Help

Client Privacy

You are on Page 1 of this book.

Use your "Page Down" button to start reading.

Use Ctrl S To Save Book

Use Ctrl F To Search Book

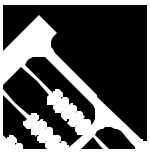
Use the scroll button at right to fast forward to any page.

More Pages

CONTENTS

INSURANCE AGENTS AND CLIENT PRIVACY

AGENT DISCLOSURES AND CLIENT PRIVACY



INTRODUCTION

Protecting a client's privacy is an ethical responsibility and an area of increasing liability for insurance agents. The concern by clients is that highly personal health and financial information you collect in the process of selling insurance will get in the hands of groups who might use this data to exploit them. As a result, new legislation has passed that requires certain disclosures be made to your clients whenever non-public (personal) data is being shared with other parties. Also, they must be given the opportunity to restrict its use.

Why Is Client Privacy An Issue Today?

There are many reasons. First and foremost is the fact that the sharing of information has become complicated. The United States is in the midst of a revolution in information technology. Gone are days of a customer's financial and health records being locked in a file room at the rear of the office. New electronic distribution channels of providing and servicing insurance products and health care have created exposure of personal financial information and health histories. And, the way we get our health care is changing from one-on-one, patient/doctor relationships, to large, integrated health networks where many levels of employees have access to records. In a sense, a new by-product of trying to control health-care and insurance costs using technology and centralization has resulted in a profound potential for abuse of privacy.

In a nutshell, today, entire networks distribute and / or disclose the data you collect on your clients with a variety of affiliates and third parties; all the while, putting you and other agents in the path of tighter and more responsible privacy rules.

Information Sharing Problems

Some have a problem understanding why the sharing of client information is a problem. After all, wouldn't it be to the client's benefit for a central database to itemize a history of medications and comprehensive medical records? For example, what if you were involved in a car accident far from home and unconscious by the time you arrived at the local hospital? The emergency room doctor might conceivably access a special computer link; plug-in your social security number and instantly learn about your specific allergies, medical conditions and medications. Life-saving therapies might be administered faster and costly re-testing for certain information might be avoided. Sounds great, right?

Unfortunately, not everyone will use this kind of information as it was intended. For example, what if the same medical records were retrieved by a prospective employer. Could he use the health and financial information in making a decision not to hire you? Insurers themselves have been accused of privacy invasion when they use personal financial information, like FICO scores (a system to determine a consumer's credit worthiness), to raise insurance premiums or rank insurability based on the types of credit cards, catalogs or cars a prospect owns and uses.

Also, consider cases where records have fallen into the wrong hands. Are the consequences of exploiting personal information sufficient to deter someone from the temptation? Think it doesn't happen? Think again. In Nevada, for example, a woman purchased a used computer and discovered that it still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy database included names, addresses,

social security numbers, and a list of all the medicines the customers had purchased. What happens to the data on your old computers? In another case, a 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. Or, how about a 1999 incident in which the health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut.

In all these instances, client privacy could be breached. In response, legislation has passed to address the better handling of client privacy; especially by making the "caretakers" of this information more responsible. As you might guess, insurers, financial institutions and health care corporations have been at the head of the responsibility list since they wield incredible influence over detailed records related to age, health, finances and lifestyle.

Agent Responsibility

Agents are also involved in the privacy debate because under the definition of this privacy legislation, you are referred to as a "financial institution" or "covered entity". As such, you must comply with sweeping and complex rules and standards under HIPAA, the Gramm-Leach-Bliley Act, the Federal Medical Privacy Rule, and possibly the new Patriot Act.

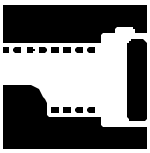
To complicate matters more, your individual state may pass privacy legislation that exceeds or conflicts with these requirements. So, you may fall under "double" standards. For example, the privacy rules under HIPAA state that items such as a person's name, address, social security number and payment history are protected "health information" subject to an ***opt-in standard***. Therefore, HIPAA would prohibit any sharing of this information with a third party unless an express release is signed by your client. Many states, however, would consider these same items as "financial information" subject to ***opt-out standards*** where the sharing of client information is allowed until he "opts-out".

Can you see where disputes might surface? And, the penalties for a mistake or not complying can be stiff, ranging from $100 to $25,000 per incident; and, even prison terms of up to one year. Failure to provide a required notice is also a violation of agency rules subject to enforcement by your State Department of Insurance, and enforcement action under federal and state unfair trade practices rules. In addition, an individual whose information has been shared in violation of the rules may bring their own, private civil action against you.

For these reasons and more, this course will attempt to provide as much information as possible to help you comply with the many client privacy requirements. First we will give you a thorough understanding of ***Privacy Issues*** and the reason they are important in today's business world. Next we will explore the two major areas where these matters effect your business most: ***Protecting Financial Information Privacy*** and ***Protecting Health Information Privacy.*** Finally, we have devoted two sections to ***Agent Disclosure Issues*** to answer specific questions on how insurance agents might comply with new privacy rules.

Keep in mind when reading this course, that even though you see a lot of legislative activity today, privacy laws in the United States are truly in their infancy. Experts say we are years behind most European countries. More rules can be expected.

Always consult proper counsel such as an attorney or your carrier before using any information from this course in personal or client matters.



UNDERSTANDING PRIVACY ISSUES

The Importance of Privacy

The reasoning behind the enacting of state and national privacy rules includes the assertion that privacy is a fundamental right of the citizenry. It is considered as essential to individual and collective freedom. All fifty states recognize a common law or statutory right to privacy. A few states include the right to privacy in their respective constitutions.

From the founding of the United States, privacy has played a fundamental role in the structure and content of America's laws. As stated in the Federal Register: December 28, 2000, Volume 65, Number 250:

"Throughout our nation's history, we have placed the rights of the individual at the forefront of our democracy. In the Declaration of Independence, we asserted the "unalienable right" to "life, liberty and the pursuit of happiness." Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." By referring to the need for security of "persons" as well as "papers and effects" the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of "persons" is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in "papers and effects" underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an "unreasonable" search of the papers and effects."

The United States Supreme Court recognized two different kinds of interests within a constitutionally protected "zone of privacy" in a New York case, Whalen v. Roe, 429 U.S. 589 (1977). In this case, a New York statute that created a database of persons who obtained drugs that were available both lawfully and unlawfully. One of the interests said to be protected in the zone of privacy is "the individual interest in avoiding disclosure of personal matters."

However, an individual's right to privacy in information about himself is not considered an absolute right under United States law. For example, the right to privacy does not prevent the reporting of communicable diseases to public health agencies, or stop law enforcement from obtaining information as long as due process is observed.

It is largely held that each individual has some rights to control personal and sensitive information about himself. In particular, medical and health information may be among the most sensitive type of information. People do not want their medical and health information to be publicly available, where anyone from neighbors, relatives, employers and the government could review it.

Mental health information may be the most sensitive type of medical or health information. Mental health treatment may include records of reflections of a patient's most intimate thoughts, words and emotions. The Supreme Court held in Jaffee v. Redmond, 116 S. Ct. 1923 (1996),

that statements made to a therapist during a counseling sessions were protected against civil discovery under the Federal Rules of Evidence. Within its opinion, the Court noted that some form of psychotherapist-patient privilege has been adopted by all fifty states. The Supreme Court stated that it "serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance."

The Right of Privacy

Privacy has become a prominent issue in every part of the American and international economy in the last few years. Legislators have been introducing many privacy bills. Laws already in place are being reinforced with new regulations and deadlines. The process of underwriting and gathering client information go hand in hand. The Internet, consolidation in financial services, and the electronic transfer of medical and financial client data have sparked new privacy concerns. Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently written Constitutions such as South Africa and Hungary's include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe. Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of privacy in early Hebrew culture, Classical Greece and ancient China. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following areas:

- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches
- **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space

Insurance Risk Appraisal

No one is more affected by the consumer's privacy concerns than the insurers. Insurance is based on the concept of a group of people sharing the risks and the costs of unexpected events. ***Risk appraisal*** helps the company determine the appropriate cost to cover one's risk profile—or his "fair share." It prevents him from having to pay the same as someone with a less favorable risk profile. Risk appraisal is necessary to allow the company to offer coverage at an affordable price, and in some cases, to offer coverage at all. However, nothing can be accomplished in the risk appraisal arena without the use of personal financial and health information supplied by consumers. It is to the advantage of BOTH that this information be collected with as little restriction as possible and protected with best efforts.

Think about it. A world without risk appraisal would mean everyone would pay the same price. Even if a consumer would be considered a "good risk," he would end up paying more than the appropriate amount for his risk level. That is because he and every other policy owner would have to absorb the extra risk and costs associated with those who have less favorable risk profiles. These extra costs would drive up the cost of insurance for everyone. Risk appraisal is especially important to the policy owner because it protects the value of his insurance. It ensures that the underwriter will only issue appropriate amounts of insurance, at the appropriate price, to people who fall within established guidelines. It also ensures that the underwriter's risk appraisal guidelines and goals remain consistent over time. Risk appraisal safeguards against compromising the value of customers' insurance and the financial stability of the company. A thorough risk appraisal process helps the consumer in several ways.

- **Lower Cost** – He is often able to purchase a policy as a member of the most favorable risk group, which means the best price—he pays only his fair share.
- **Locked-in Risk Classification** - Once the risk classification has been determined for one's policy, it cannot be changed due to deterioration in his health.
- **Quality Coverage** - A thorough risk appraisal process is a hallmark of a strong company. One can be confident he is receiving the finest-quality coverage for his money.
- **Non-Cancelable Coverage** - Once a policy is issued, the company cannot cancel it due to a deterioration of your health. By participating in the risk appraisal process, and supplying accurate information, he can secure insurance coverage that can be with him for the rest of his life.
- **Early Warning** - The risk appraisal process might alert one to potential or existing health problems that he otherwise may not have known about.

The risk appraisal process allows the underwriter to determine the state of the client's health, his financial situation and, if necessary, whether his job and hobbies impact his application. It is critical for insurers to ask for and collect information from the client about himself. The underwriter treats all of this information as personal and sensitive. And, just as the client has a responsibility to provide the underwriter with this information, the underwriter also has a responsibility to ensure that it is handled carefully and with confidentiality. The professional underwriter has established procedures in every step of the application and risk appraisal processes to help maintain the consumer's privacy. He is committed to maintaining the confidentiality of all of the information that he receives from his clients.

Understanding Consumer Concerns

The most important compliance issue for the insurance industry over the next ten years will most likely be privacy. The quest for greater privacy is a natural reaction to the information age. Privacy is a basic human right that is being reasserted. Consumers are demanding a choice in how information is used. The National Association of Insurance Commissioners believes that consumers are concerned about all types of marketing activities. They are concerned about activities related to their financial or health information.

The Internet holds tremendous potential for reducing healthcare costs and opening the door for patients to take a more active role in the administration of their healthcare. The same systems, which streamline the processing of healthcare information and afford easy, timely access to personal health information, also open new doors to the misuse of sensitive information. It is not hard to see how personal health information given to a physician or other healthcare provider, would be sought by insurers, employers or even advertisers. It is the doctor and patient's fears of this potential misuse that is the Achilles Heel of online healthcare services. Unfortunately, countless abuses of personal information by e-commerce companies have created an environment of open distrust of online services.

Privacy advocates' numbers have exploded in the past two years in response to corporate abuses. The fact that corporate America openly spends hundreds of millions to lobby against new privacy legislation adds to consumer distrust. But, privacy concerns in the world of e-commerce pale in comparison to a patient's perception that his or her personal health information could be revealed to someone without consent. The damage that could occur from misuse could be devastating to an individual, causing great personal harm. No wonder indeed, that doctor and patient acceptance of Internet technologies will depend on the perception that information that is entrusted to the healthcare system will be protected by stringent standards.

A March 2000 report by the American Medical Association says the majority of today's health information web sites do not comply with their own stated privacy standards, and fail to protect personal health information of their visitors. As eHealth moves beyond information sites to more direct healthcare functions, privacy will become even more important. Building confidence in the online experience is critical to the future success of eHealth. Privacy failures will stifle physician and patient enthusiasm for the online health industry.

Personal Health Information

Even though the consumer is concerned about activities related to both his health and financial information, he desires a greater level of protection for his personal health information. Health records are among the most sensitive data that are acquired, used, and disclosed by the government and the private sector. Health information reveals a great deal of personal facts about individuals which may lead to stigma and discrimination when possessed and misused by government officials, employers, insurers, and by friends and family. The increasing potential for disclosure of this information within a rapidly developing national health information infrastructure, facilitated by massive computerization of records and other technological developments, presents significant risks to individual privacy.

Despite the highly sensitive nature of individual health information, protecting the privacy and security of these records has been historically de-emphasized when compared with statutory protections allotted to other types of personal information such as banking and investment

records, consumer spending information, tax information, and video rental records. There are many reasons for the de-emphasis of health information privacy, including economic and political theories. However, modern legal developments are likely to improve privacy and security protection. As we develop a national health information infrastructure, the importance of privacy and security become crucial.

Health information privacy, of course, is a two-edged sword. While it is important in respecting the autonomy and dignity of individuals, excessive amounts of privacy can impede many of the goals of the health care system. Health information creates unprecedented opportunities to benefit individuals and communities. Health care professionals can use computerized data to improve clinical care for patients. Health service researchers can better assess the quality of services. Government and health service managers can gain administrative efficiencies. Health insurers, including Medicare and Medicaid, can prevent fraud and abuse. Public health authorities can improve surveillance and epidemiological investigations within the community.

In each of these areas, overly restrictive health information privacy and security protections may thwart legitimate and important uses of identifiable health data that benefit society. Though privacy is certainly necessary, legal protection should strike a reasonable balance between individual rights and the collective goods of health information. Today, society is witnessing tremendous changes in both the collection and use of health information and in the environment in which it resides. The transition from fee-for-service health care to managed care has led to a demand for an unprecedented depth and breadth of personal information by a growing number of players. At the same time, the environment for information is moving rapidly from paper forms and files to electronic media, giving organizations a greater ability to tie formerly distinct information together and send it easily through different sources.

Personal health information can be used to hurt consumers in various ways. Consumers realize that their health information can be used against them when they are trying to qualify for a loan or mortgage. It can also be used against one when he is applying for a job, or cause termination of employment. An individual with a medical condition requires treatment with a very high-priced prescription drug. After his insurance company receives the claim for reimbursement, his doctor receives numerous calls from pharmaceutical companies trying to convince him to change the medication to a drug that their company produces. Other patients have received marketing calls for products related to their illness, even though they had not disclosed this information to anyone other than their insurance company.

Because of these consumer concerns, the National Association of Insurance Commissioners (NAIC) has decided to treat health information differently from financial information. This will be done by using an “opt-in” standard for individually identifiable health information, and by enforcing marketing restrictions. It is critical for underwriters to be thinking about the future, and making privacy compliance a significant factor in planning for the future. It is also important for them to begin developing a privacy compliance program.

Studies have shown that health web sites understand the consumer’s concern about the privacy of their personal health information. These web sites have tried to establish privacy policies, but there is inconsistency between the privacy policies, and they fall short of truly safeguarding consumers. Visitors to health web sites are seeking to manage their health better. The risks of doing this, however, are that they are not anonymous, even if they think they are, and their personal health information is probably not adequately protected. To make matters worse, health web sites disclaim liability for the actions of third parties, which negates the privacy policies.

Personal Financial Information

Banks, insurance companies, and brokerage firms operating as one are known as financial institutions. They offer benefits such as consolidated account statements and lower fees. At the same time, the ability of these companies to merge customer data from several sources and even sell it to third parties represents a real risk to one's privacy. Consumer information kept in the files of financial institutions is some of the most sensitive, personal information imaginable. In the past, there were few restrictions on a financial institution's ability to share or even sell one's personal information. Title V of GLBA gives the consumer some minimal rights to protect his financial privacy.

The GBLA requires that a financial institution give the consumer notice of three things:

- **Privacy Policy:** The financial institution must tell one the kinds of information it collects about him and how it uses that information.
- **Right to Opt-Out:** The financial institution must explain one's ability to prevent the sale of his customer data to third parties.
- **Safeguards**: Financial institutions are required to develop policies to prevent fraudulent access to confidential financial information. These policies must be disclosed to the consumer.

The deadline for financial institutions to comply with new privacy regulations under Title V of the Gramm-Leach-Bliley Act was July 1, 2001. In preparation for these new requirements, financial services professionals spent hours attending seminars, pouring over the legislation and reading clarifications from the office of the Comptroller of the Currency. The new law contains extensive federal requirements governing the disclosure of consumer information by banks and other private entities. Differing requirements created some confusion because satisfying one set of requirements does not necessarily amount to compliance with another.

Consumers continue to express concern over the availability and distribution of their personal financial information. Relieving their concerns may not be as simple as complying with the letter of the law. While consumers may have been only vaguely aware of debate in Washington leading up to the new legislation, they find it impossible to ignore one of its by-products. A typical consumer's home mailbox has been stuffed with privacy notices from banks, credit card companies, brokerage and investment firms, and other finance companies. While financial institutions have notified consumers, it's ongoing communication and education that are the key to long-term consumer confidence. Effective communication requires a certain amount of empathy, and the ability to see a situation from another point of view. Financial service companies must continue to develop their privacy policies keeping their customers at the forefront. Financial service companies should ask themselves how their customers might react to the following issue:

- the quantity of a customer's personal financial information the business collects
- how the business uses the information
- whether that information is transferred to affiliates or other parties
- which other entities receive that information
- what happens to the information once it is handed over to another party

Financial service companies that deal with a customer's nonpublic financial information should make every effort to explain their privacy policy in plain language. Failing to understand the volatility of sentiment surrounding privacy may endanger the public trust that financial institutions have worked diligently to earn and maintain. Eroding consumer trust could constrict the flow of vital credit information, and this in turn would have a negative impact, not only on financial institutions, but also on consumers. When lending institutions have an accurate and complete picture of creditworthiness, they reduce their risk in lending, which ultimately reduces the cost of credit. Consumers can shop for the best rates among many lenders who can quickly access the applicant's financial information. This increases competition among lenders and also helps to drive rates down for consumers. The ability to monitor information also helps financial institutions spot fraudulent activity, and identify unusual transactions or unacceptable risks. When fraud does occur, immediate access to information helps investigators limit loss and apprehend criminals.

Availability of consistent and accurate information has enabled investors to buy loans of similar credit quality that are packaged and sold as asset-backed securities. Access to this information allows investors to judge with more confidence the risks and potential return of their investment. The secondary mortgage market is one example of successful secondary markets that provide liquidity, spread the risk among a large pool of investors, and lower the price of loans. According to at least one estimate, the secondary loan market has lowered the price of mortgages in the U.S. by a full two percentage points in comparison to other countries.

Secondary markets for automobile loans and credit card receivables are producing similar results. Investors in pools of security backed assets hold more than 50% of all revolving credit and over 30% of all non-mortgage consumer credit, currently totaling approximately $436 billion. The advent of online financial transactions heightened consumer demands that financial service companies handle and exchange nonpublic financial information responsibly. Technology has opened the door for new, more specialized financial products and services, but in order to successfully take advantage of those opportunities, banks must reassure consumers that the bank-customer relationship -- and the expectation of privacy that is an essential part of that relationship -- will be honored as much on the Internet as it is in the branch office.

Customers enjoy the benefits and convenience that an information-based marketplace makes possible, such as fast credit approval or financial products tailored to their specific needs. In the past, consumers may have enjoyed these benefits without understanding what is required to handle nonpublic financial information responsibly. The new privacy regulations may prompt consumers to make more informed choices about how their personal financial information is used. At the same time, the rules are moving financial institutions to demonstrate they take privacy protection seriously. Education and privacy protection are both vital because consumers and financial service companies have too much to gain from a marketplace where information can be exchanged quickly, accurately and securely.

Privacy Regulations

We will discussing these regulations in detail in later sections. For now, it is important to familiarize yourself with their names and purpose since we refer to them often:

HIPPA – Administrative Simplification

The final rule for the Standards for Privacy of Individually Identifiable Health Information, known as the "Privacy Rule," implements the privacy requirements of the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Privacy Rule applies to health plans, health care clearinghouses and certain health care providers. It also includes standards regarding the rights of individuals regarding their health information, the procedures for exercising these rights and the authorized and required uses of the information.

The type of health information that is protected by the Privacy Rule is information that

- relates to a person's physical or mental health, the provision of health care, or the payment of health care;
- identifies or could be used to identify, the person who is the subject of the information;
- may be created or received by a covered entity; and
- is transmitted or maintained in any medium.

The reasoning behind the enacting of national health privacy rules includes the assertion that privacy is a fundamental right of the citizenry. It is considered as essential to individual and collective freedom.

There is clear indication that this information could impact agents. This we will discuss in a later chapter.

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) is a comprehensive law regulating the use of customer information by financial institutions. GLBA's privacy regulations went into effect on November 13, 2000. The deadline for full compliance was July 1, 2001. These provisions apply to insurance agents, brokers and companies. HIPAA and Gramm-Leach-Bliley Act are both statutes dealing with the financial privacy statue. The legislation applies to all financial institutions. These include all that are involved in:

- traditional banking activities such as lending
- investment-oriented activities such as providing investment advice or underwriting securities offerings,
- insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability or death
- providing and issuing annuities
- acting as principal, agent, or broker for these activities

The Gramm-Leach-Bliley Act (GLBA) has issued privacy regulations for all insurers. The Federal Trade Commission has given examples of businesses that could be covered with these privacy regulations. These include retailers who issue their own credit cards, real estate and personal property appraisers, tax preparers, automobile dealerships who lease automobiles, developers of financial software, career counselors providing advice for employees in the financial services industry and business that print and sell checks for consumers. Most insurers will be included within these provisions. These regulations and provisions not only apply to

health insurance, but any other line of insurance. For non-health lines of business, the GLBA may contain the only federal privacy restrictions on medical information.

The rules of the GLBA apply to any person or entity that is authorized to conduct business under state insurance codes. The GLBA establishes a federal standard of privacy of protection. Individual states may provide greater consumer privacy protection. An insurance producer that is licensed by a State's department of insurance does not have to comply with GLBA privacy notice requirements if

- he is an employee, agent or other representative of another licensed agent
- if his affiliates provide the required notices
- he does not disclose any non-public information to any person other than his employer or those affiliated with him

This agent exception relieves any agency from compliance with GLBA notification burdens if the agency limits its information sharing to insurance companies for which they are acting as agent. If the agent shares the information with anyone other than an insurance company, the agent must provide separate notices and opt out opportunities as required by the rules. If an agent, for a fee, provides any other services to any institution such as financial, investment or economic advisory services relating to an insurance product, that individual becomes the agent's customer and must be provided with all required notices about the agent's privacy policy.

The rule provides that an independent agent sharing information with multiple insurance companies in order to obtain the best price quote for a client does not need to provide notices to the client. It is the responsibility of each insurance company to comply with the notice requirements as to that client. The client will be considered a consumer of each company to whom the client's information is provided, and if the client purchases coverage from one of the companies, the client becomes the customer of that company.

However, if the agent discloses or plans to disclose that information to anyone other than the companies, the agent must send that client all required notices and provide the client with the opportunity to opt out. Each agency's operations are different, and because the law is designed to reflect all of the different types of information-sharing in the marketplace, there is no one single privacy notice agencies can use to comply with the federal law. Each agency will need to develop its own internal privacy policy and consumer privacy notice.

The agent exception benefits agencies that have *exclusive agency* relationships with an insurer, such as life insurance agents. It may be better for the agencies to be covered by that company's GLBA privacy policy. The agent exception also benefits agents that are involved in the *more traditional* types of agency activities. This would include those who do not share protected information with third parties after a sale is complete. If an agent submits an individual's application to a number of different insurance companies, that individual is not a customer until an application is accepted and the individual becomes a policyholder of the insurance company. Any agent wanting to take advantage of this exception should be sure that its appointment contracts require the insurer to be in compliance with its GLBA obligations.

Again, the impacts of this legislation are far-reaching for agents and we will discuss it in greater length in a later chapter.

The Federal Medical Privacy Rule

In April 2001, President Bush approved The Federal Medical Privacy Rule. This rule imposed a major shift in health care ethics applicable to patient consent. For the first time in our nation's history, the federal government is going to decide for each and every citizen who can access his or her personal health information, including genetic information. The concept of informed consent has been defined as a person's agreement to allow personal data to be provided for research and statistical purposes. The individual's agreement to share information has been based on full exposure to the facts the person needs to make the decision intelligently. Informed consent has described a condition appropriate only when patients have a clear choice, and have not been subject to penalties for failure to provide the data sought. The federal medical privacy rule does not meet this definition of consent.

The Patriot Act

On April 24, 2002, the Patriot Act became law. The Act, put in place after September 11, addresses terrorism and money-laundering activities. The intent is for businesses to “know their customer” by verifying their identities. As of the writing of this course, it is not known exactly how this Act will impact agents or how it is effected by Gramm-Leach-Bliley. Regulators believe that producers might be included under the law, but it is not certain how.

Additional Legislation

Other legislation that could affect your clients right to privacy include The Privacy Act (1974), The Freedom of Information Act, Federal Substance Abuse Confidentiality Requirements, Employee Retirement Income Security Act of 1974, The Family Educational Rights and Privacy Act, Federally Funded Health programs (Medicaid, Medicare, etc), Food, Drug and Cosmetic Act, Clinical Laboratory Improvement Amendments, Federal Disability Nondiscrimination Laws, Fair Credit Reporting Act and more!

As you can see, there is much you need to know about collecting and transmitting information from a prospect. This will be further discussed in later sections.

Advantages of Compliance

Simplification

The magnitude of changes mandated through privacy regulations has had a significant impact on health care organizations and insurers alike. Accomplishing this change successfully has required a process that facilitates advanced planning so that an organization can become completely accountable for the management of a patient's health care information. The smart organizations have used the task of moving towards compliance as an opportunity to improve their effectiveness. This has resulted in the benefits of administrative simplification.

Increased Security

The growing concern over increasingly malevolent hacker attacks and viruses, as well as the need to meet government privacy regulations, has many companies searching for solace in

outsourced security services. Viruses such as Code Red, the Love Bug, and Nimda have caused billions of dollars in damage to companies' systems. Researchers estimate that the Love Bug, which hit in 2000, cost businesses $8.75 billion in lost productivity and cleanup efforts. Any company that deals with proprietary customer data has to be concerned with these and other security threats. The Health Insurance Portability and Accountability Act of 1996 is pushing health-care companies to tighten the security of their patient information. The act's primary objectives are to provide better access to health insurance, limit fraud and abuse, and reduce administrative costs for health-care and insurance providers. Companies that rely heavily on the Internet need to be acutely aware of security issues. As an added protection, some corporations have hired senior security personnel to conduct an internal risk assessment. While the financial-services and health-care industries are at the forefront of heightened Internet security, others will likely follow. The price of performing a risk assessment and adding managed security services is small when compared with the cost of losing customer confidence

Disadvantages of Compliance

Even with all the emphasis on privacy issues, the American people still do not have true medical privacy. In reality, they weaken one's ability to restrict access to his medical records, and increase the federal government's power to access one's personal health information without his consent. Every doctor and other health care practitioner are required to share patients' records with the federal government without patient consent. Medical records can be disclosed for many reasons. Some of these are:

- public health surveillance and activities
- law enforcement activities
- research
- FDA monitoring
- judicial and administrative proceedings
- oversight of the health care system
- licensing
- U.S. public health officials working with foreign governments

After one's medical records are disclosed to a third party other than a business associate, the final rule no longer protects the information. There is **nothing** that prohibits the federal government, state governments, or private parties from using the patient information listed above without patient consent. This can be compiled into large databases of information. The privacy rule does not apply to information that was collected or stored in databases without consent prior to February 26, 2003.

Patients are not guaranteed the right to restrict access to their records. Health care providers may refuse to treat a patient if he will not give consent to share his medical records. Any doctor can use those records to treat other patients without one's consent. Patients will be given limited information about when and to whom their medical records were disclosed for most health care activities. There is no penalty for disclosing information in one's medical record. Consequently, patients have no rights for any kind of action even if they believe that their medical privacy has been violated. Identifiable health information such as banking of blood, sperm or body tissue is not protected by the privacy rule, because it is not considered to be health care under this rule. These items include genetic information, and lack of privacy protection in these areas could have far-reaching effects.

With the Internet, it is easy to transfer electronic medical records. The medical privacy rule promotes the development of a national health information network through standardized codes for all health care services throughout the United States. The privacy spotlight will glare on the health-care industry as providers and insurers scramble to comply with new regulations governing the confidentiality of patient data. While some fight to delay or dilute those regulations, there are some who champion even broader efforts to protect patient confidentiality. Medical experts contend that to maintain trust in the doctor-patient relationship, lawmakers must pass more-comprehensive legislation to ensure the privacy of health records. They know that an essential to that caring relationship must be a trust that health-care professionals will protect the confidentiality of patient information. Health-care providers, insurers, and transaction processors must comply with new patient-data privacy regulations included in the Health Insurance Portability and Accountability Act by June 2003.

Opt-Out, Opt-In and Client Privacy

Definition of "Opt-Out"

"Opt-out**"** is the process of having one's personal information removed from databases and lists that are often sold for marketing purposes. Personal information is collected on individuals in a variety of ways such as when they are applying for a credit card, telephone service, or entering contests. Credit bureaus also sell information for marketing purposes. If the consumer has active accounts with a brokerage house, credit card company, or insurance company, he will receive a privacy notice from these institutions. The term "financial institution" includes companies such as payday loan companies, collection agencies, and travel agents. For this reason, it is particularly important for the consumer to carefully review all preprinted notices that he receives in the mail or electronic mail messages.

Federal law now gives one some minimal rights to protect his personal financial information. The law gives him the right to prevent a company he does business with from sharing or selling certain sensitive information to non-affiliated third parties. The term "opt-out" means that *unless and until* the consumer informs his bank, credit card company, insurance company, or brokerage firm that he does not want them to share or sell his customer data to other companies, they are free to do so.

Controversies Concerning Opt-In

When this law was debated in Congress, consumer advocates argued unsuccessfully for an **opt-in** provision. This stronger standard would have prevented the sharing or sale of the customer data *unless* the consumer affirmatively consented. The opt-in standard did not prevail. Therefore the *burden is on the consumer* to protect his financial privacy.

Opt-in does not enhance consumer privacy. Since it is the consumer who makes the final and binding decision regarding the use, non-use, or misuse of his personal information under either "opt-in" or "opt-out", there is no privacy advantage to "opt-in". Neither approach provides the consumer with greater or lesser rights than the other. If this argument is valid, and both "opt-in" and "opt-out" fully reflect consumer preferences regarding the use of their personal information, then all the other arguments are invalid – sellers would receive the same amount of information under either approach. Thus, implementing "opt-in" would not impose any additional costs on either producers or consumers, as compared with implementing "opt-out". However, the choice of scheme – "opt-in" or "opt-out" – does distort consumer preferences by imposing

transaction costs on one choice or the other. After acknowledging that transaction costs cause both "opt-in" and "opt-out" schemes to reflect imperfectly the "true" privacy preferences of the consumer, the policy debate can move forward and tackle the next question. Does "opt-in" or "opt-out" reflect the true preferences of the consumer better? Presumably, transaction costs under "opt-in" lead consumers to provide less information than their true privacy preferences would suggest; conversely, transaction costs under "opt-out" lead consumers to provide too much information. The structure of the seller-producer relationship suggests one reason why "opt-in" might represent the consumer's true privacy preference better. The seller can adjust the level of transaction costs involved in "opting" in or out, whereas the consumer cannot. Since the seller has an obvious interest in collecting information, it has an incentive to make it easy and simple to opt in, under an "opt-in" system, and an incentive to make it difficult and time-consuming to opt out, under an "opt-out" system. Whatever regulations exist to make opting out easier, the seller has an incentive to push the envelope, to make opting out as difficult as possible within the letter of the law. Thus, transaction costs under an "opt-out" scheme are likely to be higher than under an "opt-in" scheme, and the outcome under "opt-out" is likely to be concomitantly farther away from the correct outcome than under "opt-in".

Opt-in reduces consumer privacy by hampering efforts to fight fraud and identity-theft. Since an "opt-in" approach reduces the amount of information available to sellers regarding the consumer's preferences, spending habits and typical behavior patterns, it hampers sellers' efforts to detect unusual purchases and alert the consumer to possible fraud. This makes it easier for criminals to assume false identities and engage in other fraudulent behavior at the expense of law-abiding consumers. Not only is this an invasion of privacy in itself, but also the rectification of the situation often requires the consumer to provide personal information about himself. This is a valid point, which, under an "opt-in" scheme, producers might wish to present to consumers in order to convince them to permit use of their personal information. Under an "opt-out" scheme, this point could be presented to consumers to deter them from exercising their "opt-out" option.

Opt-in imposes significant costs on sellers, which are then passed on to consumers. Opt-in increases the costs to a seller of expanding its range of services, because of the necessary expenditure of resources to obtain consumer permission to use the additional personal information that enables the better service. *Opt-in also increases marketing costs* because, instead of sending promotional materials to a neatly identifiable population segment that is likely to find such materials useful, the seller must send the promotional materials blindly to broader population segments. Some believe that in the "distance shopping" market through catalogs and online sales, enforcing an "opt-in" scheme will result in increased costs, which will then be passed on to consumers. The data restrictions inherent in the "opt-in" scheme would affect catalog marketing more than online marketing. This is because the interactive nature of the Internet can counteract the lack of third-party information about prospective customers. To properly understand the aggregate impact of an "opt-in" scheme on sellers, one would need to look at the reliance of other industries on catalogs, as opposed to more interactive means of marketing. One of the factors slowing the growth of e-commerce, though, is consumer hesitation over conducting business online. In a report to Congress on online privacy, the Federal Trade Commission presented surveys showing the extent to which privacy concerns hamper the growth of e-commerce. Recent survey data demonstrate that 92% of consumers are concerned and 67% are **very** concerned about the misuse of their personal information online. Concerns about privacy online reach even those not troubled by threats to privacy in the off-line world. Thus, 76% of consumers who are not generally concerned about the misuse of their personal information, fear privacy intrusions on the Internet. This apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled. Indeed, surveys

show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction. There are benefits of adopting and enforcing an "opt-in" scheme, in which consumers are assured that no one will make use of their personal information without their prior and express consent. The resulting burgeoning in e-commerce would reduce sellers' costs, by enabling them to make more extensive use of the efficiency inherent in interactive marketing tools such as the Internet. This effect may offset, and perhaps even outweigh, the increase in costs attributable to the data restriction effect.

Opt-in reduces the amount of competition in the market. By raising costs of operation, "opt-in" will drive marginally profitable companies out of the market altogether. By requiring new entrants to go through a laborious process of obtaining personal data permits from each new consumer, "opt-in" creates a barrier to entry into the market. Market incumbents, on the other hand, will benefit from an established consumer base that has already given permits. Essentially, "opt-in" helps entrench market incumbents. Since consumers are more likely to "opt-in" to companies they know and trust, such a scheme will favor large firms with established brand names over smaller firms. Competition is most reduced in the industries that rely the most on expensive means of obtaining permission, such as telephone or paper-mail, rather than on website-notices and e-mail. As e-commerce continues to grow, and technology becomes more pervasive, there is likely to be a shift from the former to the latter, and a reduction in the height of the entry barrier. A new entrant, though forced to beseech consumers for information-permission, could do so inexpensively through mass e-mailing.

Opt-in costs to sellers will be passed on disproportionately to less wealthy consumers. A study of distance shopping in the apparel market (catalogs, online purchases) reveals that inner city and rural consumers are significantly more reliant on distance shopping than the average U.S. household. These populations will be hit hardest by increased prices or decreased discounts which will result from implementation of "opt-in", as companies seek to recoup the increased costs of providing the "distance shopping" option. These are also the consumers who can least afford such price hikes.

Control of Personal Information

Now, we face the question of consumers' rights to financial privacy, an issue that was brought to the forefront by recent federal legislation, the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act. At the core of this, as well as most other privacy debates, is the issue of *control* of personal information. Who ultimately determines how personal information flows, and how it is used? Is it the individual who is the subject of the data or the company that compiles that data?

The Gramm-Leach-Bliley Act (GLB) enables financial institutions such as banks to affiliate with insurance companies and brokerage firms under one corporate roof. A major incentive for these industries to affiliate with one another is the ability to share and intermingle their customer data. Industry representatives sell their services as merged industries providing one-stop shopping for their customers, and offering benefits like consolidated statements and total relationship pricing. But there are also profound privacy implications of the federal legislation. One's financial information can now be shared with the affiliated insurance company for use in making decisions about coverage and rates. Sensitive health information held by insurance companies might be shared with affiliated banking and brokerage firms. Moreover, comprehensive data profiles can be compiled by combining the customer data of the affiliated banks, insurance companies and investment firms, creating dossiers of unprecedented depth and specificity.

The federal law does provide some small degree of control to consumers. Financial institutions are required to provide customers an "opt-out" opportunity before selling customer data to unaffiliated *third parties*. But until and unless the customer says "no" to third party sharing of their data, the bank is free to sell it. However, the law says nothing about obtaining consent for *affiliate* sharing, leaving consumers no opportunity to prevent the compilation of detailed profiles of their sensitive financial, health-related and investment data. Many consumers feel strongly that information they must supply to a financial institution to open a bank account, get a car loan, a mortgage, an insurance policy or a mutual fund should be used for that one purpose alone. The information consumers must give to financial institutions is the sort that most people would never think to share, even with close family members, let alone strangers. This includes Social Security number, income, account balances, net worth, debt level, payment history, alimony or child support payments, and bankruptcies. Also included in a consumer's file may be incidental personal information such as health status, buying patterns, political affiliations, and charitable donations.

Even if "opt-in" never becomes the law in individual states; some consumers will try to protect their privacy by following the opt-out procedures. Writing letters and filling out forms would be no easy task for a busy consumer who has, two major credit cards, several checking and savings accounts, a mortgage, a car loan, a couple of insurance policies and a brokerage account. Some experts believe that it is likely that financial institutions will obtain *implied consent* because most individuals will simply not respond to the opt-out notices. Perhaps they are too sick, too tired, too confused, or just uninformed to respond to the opt-out notices.

The issue of control does not end there. Even a well-intentioned, consumer-conscious financial institution loses control over how the information is used once it shares or sells its customer data. Industry can offer little to no assurance that information will not end up, for instance, in the hands of unscrupulous telemarketers selling fraudulent investments. The elder population is a prime target of deceptive marketing, because they are unlikely to respond to all opt-out notices. Nor do consumers have any assurance that the opt-out procedure will not increase the already rising tide of identity theft crimes, where minimal consumer information such as a name and Social Security number are sufficient to allow crooks to impersonate the innocent consumer. Opt-in is the better choice for businesses as long as the company merely wants to sell its products and services and has no interest in making money off the sale of confidential customer data.

Some companies may use the notice as a marketing opportunity. Instead of referring to the consumer's rights under the law, there may be statements at the beginning of the notice such as these: "Because we respect your privacy…" or "In order to provide you with the best services..." However, the rights described in the notices are the consumer's under federal law and companies are required by law to give the notice. The notices are a combination of one's opt-out rights under *two* federal laws -- the Financial Services Modernization Act (also known as Gramm-Leach-Bliley, or GLB, after the Congressmen who introduced it) and the Fair Credit Reporting Act (FCRA). The notice may not identify either of these laws by name, so the consumer should be able to identify the words and phrases associated with each law. An important difference is that GLB allows the consumer to opt-out of information sharing only with *non-affiliated third parties* and *not* with a company's *affiliates.* The FCRA allows him to opt-out or prevent a company from sharing "creditworthiness" information with its *affiliates.*

The Internet and Client Privacy

As more and more consumers are doing business online, the issue of privacy has quickly become one of the hottest topics. With the wealth of personal data stored on the web, privacy violations associated with e-commerce activities have created a minefield of fraud, ethics, and legal issues for insureds and insurers alike. There is a fine line between privacy and piracy, and it is called the Internet. Much of the U.S. - E.U. discussions over the European privacy laws have dealt with the Internet. The Internet is currently at the center of the earliest enforcement issues. It is the first place privacy activists will look for compliance. After all, it provides universal access to one's company's privacy policies where non-compliance may be easy to spot. The real danger for many companies is that information processes and data that are used by Web sites often originate in marketing departments, are implemented by information technicians and change frequently. Often, they do not receive the scrutiny of the company's policy, legal and business operations staffs, where compliance with privacy laws may be viewed more cautiously.

Online Communications

Online communications are communications over telephone or cable networks using computers. Examples of online communications include connecting to the Internet through an Internet Service Provider (ISP), connecting to a commercial online service such as America Online, CompuServe, or Prodigy, dialing into a computer bulletin board service (BBS). Increasingly, the differences between ISPs, the commercial services, and BBSs are blurring. The larger commercial services and many BBSs now provide Internet access. The Internet raises some unique privacy concerns. Information sent over this vast network may pass through dozens of different computer systems on the way to its destination. A different system operator known as a sysop may manage each of these systems, and each system may be capable of capturing and storing online communications. Furthermore, the online activities of Internet users can potentially be monitored, both by their own service provider and by the sysops of any sites on the Internet that they visit. ISPs, commercial services, and BBSs are managed by sysops who may have different attitudes toward online privacy. Additionally, there are a tremendous variety of activities provided by all types of online services, each of which may raise specific privacy concerns. The vast information flow created by the Internet has been driving much of the public attention to privacy. The Internet-privacy principles will have a significant impact on the insurance industry. The insurance business is moving to the Internet and the primary principles of privacy on the Internet are becoming a common denominator for businesses in any sector, on-line or off-line, and will probably serve as guidelines for litigation challenges in the future.

Level of Privacy

Often the level of privacy one can expect from an online activity will be clear from the nature of that activity. Sometimes, however, an activity that appears to be private may not be. *There are virtually no online activities or services that guarantee an absolute right of privacy.*

Public Activities

Many online activities are open to public inspection. Engaging in these types of activities does not normally create an expectation of privacy. In fact, according to federal law, it is not illegal for anyone to view or disclose an electronic communication if the communication is "readily accessible" to the public. A message that is posted to a public newsgroup or forum is available for anyone to view, copy, and store. One's name, e-mail address, and information about his

service provider are usually available for inspection as part of the message itself. Most public postings made on the Internet are archived in searchable databases.

Other public activities may allow one's message to be sent to multiple recipients. Online newsletters, for example, are usually sent to a mailing list of subscribers. If one wishes to privately reply to a message posted in an online newsletter, he should be sure that he addresses it specifically to that person's address, not to the newsletter address. Otherwise, he might find that his message has been sent to everyone on the newsletter mailing list. The consumer should not expect that his service account information would be kept private. Most services provide online "member directories" which publicly list all subscribers to the service. Some of these directories may list additional personal information. Even individuals with direct Internet accounts may be identified with commands such as "finger," which let anyone with Internet access find out who else is online. Most service providers will allow users to have their information removed from these directories upon request. Some service providers may sell their membership lists to direct marketers.

Semi-Private Activities

Often the presence of security or access safeguards on certain forums or services can lead users to believe that communications made within these services are private. For example, some bulletin board services maintain forums that are restricted to users who have a password. While communications made in these forums may initially be read only by the members with access, there is nothing preventing those members from recording the communications and later transmitting them elsewhere. One example of this kind of activity is the real-time "chat" conference, in which participants type live messages directly to the computer screens of other participants. Often the service provider describes these activities as private. However, chat line users may capture, store, and transmit these communications to others outside the chat service. Additionally, these activities are subject to the same monitoring exceptions, which apply to "private" e-mail.

Private Services

Virtually all-online services offer some sort of "private" activity, which allows subscribers to send personal e-mail messages to others. The federal Electronic Communications Privacy Act (ECPA) makes it unlawful for anyone to read or disclose the contents of an electronic communication. This law applies to e-mail messages. However, there are **three** important exceptions to the ECPA.

- The online service may view private e-mail if it suspects the sender is attempting to damage the system or harm another user. Random monitoring of e-mail is prohibited.
- The service may legally view and disclose private e-mail if either the sender or the recipient of the message consents to the inspection or disclosure. Many commercial services require a consent agreement from new members when signing up for the service.
- If an employer owns the e-mail system, the employer may inspect the contents of employee e-mail on the system. Therefore, any e-mail sent from a business location is probably not private. Several court cases have determined that employers have a right to monitor e-mail messages of their employees.

Once a sysop has intercepted e-mail for any of these lawful reasons, the sysop generally may not disclose the contents to anyone other than the addressee. Certain exceptions to this disclosure prohibition exist. These exceptions include

- when any party to the message consents to disclosure
- when disclosure is ordered by a court
- when the message appears to involve the commission of a crime (in which case disclosure is limited to the appropriate law enforcement officials)

A sysop does not violate the ECPA if the message is accidentally sent to the wrong person. The sysop may be responsible for damages caused by negligence in operating the service. Law enforcement officials may access or disclose electronic communications only after receiving a court-ordered search warrant. Only certain officials may apply for this order, and a detailed procedure is set forth in the ECPA for granting the order. These provisions are relaxed for messages that have been stored in a system for over 180 days.
The consumer's e-mail message may be handled by several different online services during delivery. The sysop of each of these systems may view e-mail under the above exceptions to the ECPA. Additionally, the message may be intercepted if either the sender or recipient consents. So even if one does not consent himself, the person he sent the e-mail to may have consented to the disclosure of the message.

Tracking and Recording Activity

Many types of online activities do not involve sending e-mail messages between parties. Internet users may retrieve information or documents from sites on the World Wide Web. Or users may simply browse these services without any other interaction. Many users expect that such activities are anonymous. *They are not*. It is possible to record many online activities including which newsgroups or files a subscriber has accessed and which web sites a subscriber has visited. This information can be collected both by a subscriber's own service provider and by the sysops of remote sites which a subscriber visits.

When one is surfing the web, many web sites deposit data about his visit, called cookies, on his hard drive When he returns to that site, the cookies data will reveal that he has been there before. The web site might offer him products or ads tailored to his interests, based on the contents of the cookies data. Records of subscriber browsing patterns, also known as ***transaction-generated information***, are a potentially valuable source of revenue for online services. This information is useful to direct marketers as a basis for developing highly targeted lists of online users with similar likes and behaviors. It may also create the potential for junk e-mail and other marketing uses. Additionally, this information may be embarrassing for users who have accessed sensitive or controversial materials online.

The practice of collecting browsing patterns is increasing. Online users should be aware that this practice poses a significant threat to online privacy. Additionally, online users should educate themselves about what information is transmitted to remote computers by the software that they use to browse remote sites. Most World Wide Web browsers invisibly provide web site operators with information about a user's service provider, and with information about the location of other web sites a user has visited. Some web browsers are programmed to transmit a user's e-mail address to each web site a user visits. Users who access the Internet from work should know that employers are increasingly monitoring the Internet sites that an employee visits. In order for law enforcement officials to gain access to subscriber transactional records,

they must obtain a court order demonstrating that the records are relevant to an ongoing criminal investigation.

Many of the commercial online services will automatically download graphics and program upgrades to the user's home computer. News reports have documented the fact that certain online services have admitted to both accidental and intentional "prying" into the memory of home computers signing on to the service. In some cases, personal files have been copied and collected by the online services. It is difficult to detect these types of intrusions. The online user should be aware of this potential privacy abuse, and investigate new services thoroughly before signing on.

Protecting Cyberspace Privacy

The consumer should be aware that at any step along the way, his online messages could be intercepted, and his activities monitored, in the world of cyberspace. One should create passwords with nonsensical combinations of upper and lower case letters, numbers and symbols. He should change his password frequently, and never write it down or give it to someone else. He should not let others watch him log in. One should never leave his computer logged in unattended. One should contact the sysop of any online service he intends to use and ask for its **privacy policy**. Most of the commercial services have written privacy policies that are provided to new subscribers. One should carefully read all messages, which appear on initial login. Many sysops notify online users in login messages that e-mail is subject to inspection. Many services require new subscribers to allow e-mail to be monitored as part of the sign-up process. All sysops should have a well defined, written policy concerning privacy. Those that do not should be avoided. When one is "surfing the web," he should look for the privacy policies posted on the web sites he visits. If he is not satisfied with the policy, or if there is no policy posted, he should not spend time on that site.

One should investigate new services before using them. He can post a question about a new service in a dependable forum or newsgroup. Bad reputations get around quickly in cyberspace, so if others have had negative experiences with a service, he should get the message. One should assume that his online communications are not private unless he uses powerful encryption. He should not send sensitive personal information (phone number, password, address, credit card number, vacation dates) by chat lines, forum postings, e-mail or in his online biography. Consumers must be cautious of "start-up" software that makes an initial connection to the service for him. Often these programs require one to provide credit card numbers, checking account numbers, Social Security numbers, or other personal information, and then upload this information automatically to the service. Also, these programs may be able to access records in one’s computer without his knowledge.

Public postings made on the Internet are often archived and saved for posterity. It is possible to search and discover the postings an individual has made to Usenet newsgroups. This information can be used to create profiles of individuals for a variety of purposes, such as employment background checks and direct marketing. Online activities leave electronic footprints for others to see both at his own service provider and at any remote sites he visits. His own service provider can determine what commands he has executed and track, which sites he visits. Web site operators can often track the activities one engages in on their site, particularly at sites, which ask him to "register" or otherwise provide personal information. Some web browsing software transmits less information to remote sites than other software. One can avoid leaving tracks when he sends e-mail messages by using anonymous remailers. If one’s online service allows him to compile a list of favorite newsgroups, or lets him range newsgroups by

priority, he should be aware that his sysop can monitor that list. He should not place controversial or sensitive newsgroups in this list if he wants to avoid being connected to particular issues. The consumer should know that if he publishes information on a personal web page, direct marketers and others may collect his address, phone number, e-mail address and other information that he provides. One should take advantage of privacy protection tools. There are several technologies, which help online users protect their privacy. Some of these are encryption, anonymous remailers and memory protection software.

Encryption

This is a method of scrambling an e-mail message or file so that it is gibberish to anyone who does not know how to unscramble it. The privacy advantage of encryption is that anything encrypted is virtually inaccessible to anyone other than the designated recipient. Thus, private information may be encrypted, and then transmitted, stored or distributed without fear that outsiders will scrutinize it. An encrypted e-mail message cannot be read by the online service sysop, or anyone else who has obtained the message legally or illegally. Therefore, any message containing private or sensitive information should be encrypted prior to communicating it online. Various strong encryption programs, such as PGP (Pretty Good Privacy) are available online. Because encryption prevents unauthorized access, law enforcement agencies have expressed concerns over the use of this technology, and Congress has considered legislation to create a "back door" to allow law enforcement officials to decipher encrypted messages. Users should be aware that the legal status of this technology is still unsettled. Moreover, federal law limits exporting certain types of encryption code or descriptive information to other countries. However, its use within the United States is not currently restricted.

Anonymous Remailers

Because it is relatively easy to determine the name and e-mail address of anyone who posts messages or sends e-mail, the practice of using anonymous remailing programs has become more common. These programs receive e-mail, strip off all identifying information, and then forward the mail to the appropriate address. There are several anonymous servers available on the Internet.

Memory Protection Software

Software security programs are now available which help prevent unauthorized access to files on the home computer. For example, one program encrypts every directory with a different password so that to access any directory one must log in first. Then, if an online service provider tries to read any private files, it would be denied access. These programs may include an audit trail that records all activity on the computer's drives.

The health care industry is currently moving toward linking institutions through a proposed information infrastructure and communications networks. Linkages would allow transfer of patient data from one care facility to another to coordinate services, and would allow collation of clinical records of each patient over time among providers and at various health sites to provide a longitudinal record, one that forms a cradle-to-grave view of a patient's health care history. Electronically connecting the health care industry by an integrated system of electronic communication networks would allow any entity within the health care system to exchange information and process transactions with any other entity in the industry. As a result of the linkage of computers, patient information will no longer be maintained, accessed, or even necessarily originate with a single institution, but will instead travel among a myriad of facilities.

Smart cards have also been proposed as a means to computerize and maintain health care information. Smart cards can function to store information, which can be accessed when a patient presents the card to a health care practitioner, and/or as an access control device, carrying out security functions to maintain a more secure and efficient access control system for health care information computer systems.

A major focus of security and confidentiality measures for these systems is preventing privacy invasion by trusted insiders. For online computer systems, security is generally provided by use of user identification names and passwords, and by menus to control access to computer system functions. Some systems also use audit trails to record significant events on a system. However, technology alone cannot completely secure a system. Organizational education, policies, and disciplinary actions supplement technical protection for confidentiality. Smart cards can serve as an access control device, providing the security functions that are normally carried out by the user.

All health care information systems, whether paper or computer, present confidentiality and privacy problems. Computerization can reduce some concerns about privacy in patient data and worsen others, but it also raises new problems. Computerization increases the quantity and availability of data and enhances the ability to link the data, raising concerns about new demands for information beyond those for which it was originally collected. The potential for abuse of privacy by trusted insiders to a system is of particular concern. In addition, special policy problems are raised by computerization. Proposed use of a unique patient identifier assigned at birth and retained throughout a patient's lifetime raises concerns among privacy advocates, who claim that if the Social Security number is used for this purpose, linkage of a wide variety of information resulting in dossier type files on individuals would be possible. Policies governing requirements for informed consent could be challenged as well, since currently patients have limited access to their health care record and may have little choice in consenting to its disclosure for certain purposes.

The Internet Revolution

The United States is in the midst of a revolution in health-care delivery and its related information technology. Some are concerned that as clinical information systems and health-care management resources are established in cyberspace, the Hippocratic foundations of patient privacy, trust and confidentiality may be sacrificed to efficient processing of medical records and insurance profiles. Though information technology may allow us to control health-care costs and understand the true implications of managing disease, that same technology may represent a very real threat to our civil liberties if it is not managed appropriately. There may even be greater concern over the ability of insurance companies and employers to gain access to comprehensive medical histories, and even to track people's information-seeking habits as they browse insurance company homepages and coverage information on the World Wide Web.

The spread of managed care from coast-to-coast is generating enormous economic pressures to simplify health-care delivery through streamlined networks and to simplify the filing of health insurance claims. Information technology will play a key role in these advances. At the same time there is great concern as to how patient privacy might be compromised as physicians, insurers and HMOs exchange information over vast Internet-based computer networks. Computerized records are now the norm, and access granted to insurance providers has meant a significant loss of physician control over detailed patient information. As brokers of health care, insurers and managed-care organizations wield incredible influence over the

dissemination of patient information, HMO providers, for example, need to know how sick their clients are in the aggregate, which requires detailed data on each client. With medical information resources so interconnected, comprehensive medical records could compromise patient privacy.

An accurate profile of a patient's mental health may be gleaned merely from a record of medications they need -- even if they pay cash to avoid informing an insurer. Pharmacy databases are often vast, and many chain pharmacies boast refill capabilities coast-to-coast. Anything that is on a database somewhere can be found. If a patient were taking medication specific for schizophrenia, for example, any pharmacist in the country who has access to these databases would know. The same is true for drugs specific to the treatment of HIV infection, or any other drug.

Centralized Databases

Just as pharmacy databases are useful for itemizing a patient's history of medications, comprehensive medical records in centralized databases now store complete medical histories that could have a major impact on the efficient and cost-effective delivery of health care. If a person is involved in a car accident in a rural area far from home, and brought unconscious to a nearby hospital, the emergency room doctors obtain his complete medical record through a special computer link. With the push of a button, they learn about any allergies, medical conditions and medications the person may have. Life-saving therapies might be administered faster, and costly retesting for certain information might be avoided.

Physicians can say that it is in a patient's best interest to have detailed, computerized medical records. And, of course, those records would be trusted and secured and treated as carefully as their health. But we must find a way to make the whole system treat those records as confidentially as a doctor is sworn to do. Questions that need to be considered are:

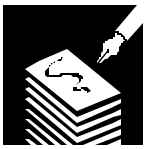
- What avenues of abuse do having a person’s complete medical record in a centralized database open up?
- Could a complete medical record get into a prospective employer's hands?
- Would prospective insurers balk at information regarding precautionary medical tests that may be decades old?

Clients of private insurers fear that insurers will provide personal health information to financial service providers, employers and marketing groups. They fear that employers will use health information when making hiring decisions.

In the near future, consumers may rely on the Web even to shop for health-care plans. Insurance companies have Web pages with detailed benefit information and various coverage scenarios for people to explore. They also have the ability, through what is known as a "cookies.txt" file, to track the people who visit their Web sites and even to evaluate their information-seeking habits. Cookies files are like off-ramps on the information superhighway that record where a browser has visited.

With these new systems, consumers will be able to examine a number of potential health-care plans from perspectives unique to their circumstances. But as consumers are learning about their health- care options, the providers of this information will have the reciprocal opportunity to learn more about the interests and needs of their individual clients. Patrons of on-line systems should never forget that, while they are reading information on their screens, the provider of that

information may be learning as much about them as they are about the provider. Ultimately, the office of the medical practitioner will have to operate under the same laws governing most other office environments. Technology should never compromise the trusted relationship between patients and physicians.



PROTECTING FINANCIAL INFORMATION PRIVACY

What Is Financial Information?

This is information that you or your insurer retains that individually identifies a prospect or policyholder. Most privacy rules refer to it as ***nonpublic financial information*** since it is information that one would NOT typically find through public sources like a phone book or government record that is open to anyone. You collect this kind of information from applications as well as other transactions and claims. It also includes information a company gets from consumer reports (such as FICO credit scores, etc) and by tracking people who have used a company or agency website. It can include things like income, credit history, premium payment history, phone numbers, addresses, social security numbers, e-mail addresses, passwords, etc.

Most nonpublic financial information under privacy rules is considered to fall under ***opt-out standards***. This means that you or your company are typically able to share it with affiliated parties as long as you disclose in a privacy policy that you intend to do so, and, you give them the opportunity to "opt-out" or disallow any sharing of information.

Health information, similar to what you ask on applications, is not usually considered to be financial information. And, of course, it has its own privacy and disclosure requirements, which we will discuss in a later section. Most health information is protected by ***opt-in standards***, meaning you or your company are obligated not to share this information without first obtaining express authorization or consent from your client beforehand.

What can be tricky is that some privacy rules, such as HIPAA, identify certain financial information; like a person's name, address, social security number and payment history, as protected individually identifiable health information subject to an "opt-in" standard. And, as such, it requires an individual's express consent or a specific exception before it is released. The privacy requirements of the Gramm-Leach-Bliley Act, however, consider this same information to be financial in nature and subject to "opt-out" standards. More on solutions to this will be discussed later.

The Financial Services Modernization Act (Gramm-Leach-Bliley Act)

The Financial Services Modernization Act more commonly known as the Gramm-Leach-Bliley Act, or GLBA has widespread implications regarding what companies, including insurers, can and cannot do with the financial information collected from customers. The language was made broad to include nontraditional financial services. These include Internet service providers whose services allow users to conduct financial transactions online, such as buying stock. For any company that comes under the jurisdiction of the GLB Act, the front-end costs of compliance are minimal, say experts. Even so, experts believe that the designated enforcement agencies -- the Federal Reserve Bank, Federal Deposit Insurance Corp. and Federal Trade Commission -- will find many out of compliance. Many new companies are nontraditional financial players, unused to being identified as such. For example, any store collecting data

from a consumer who is applying for a store credit card is not usually classified as a ***financial institution***. Under GLBA, they are and so are you!

While commercial incentives can play a strong and dominant role in the overuse or misuse of personal and financial data on the Internet, the government, too, can be an unwitting abuser. Access to public records is a lot more affordable and easier for the average citizen if the data is on the Internet. Property records, which include street addresses and owners' names, are also likely prospects for a city or county government to make available on its Web site.

Financial Institutions

Effective July 1, 2001, The Gramm-Leach-Bliley Act mandates that financial institutions (also referred to as "covered entities" in various states) establish appropriate safeguards to insure the confidentiality of customer records and nonpublic personal information. The law defines a financial institution for privacy purposes as any institution that is engaged in financial activities or activities that are incidental to financial activities. This would include banks, thrifts, credit unions, broker-dealers, mutual funds, insurance companies and agents, finance companies, mortgage brokers and lenders, notification filers, check cashers, pawnshops, collection agencies, sale of checks, credit repair, and any other non-bank entities offering financial products.

The legislation now allows banks, insurance companies, and brokerage firms to operate as one. In other words, banks can sell insurance products and insurance companies can sell banking services. The combined companies are now called financial institutions. They offer benefits such as consolidated account statements and lower fees. At the same time, the ability of these companies to merge customer data from several sources and even sell it to third parties represents a real risk to one's privacy.

Under the new law, each financial institution must have a ***privacy policy*** and disclose it to its customers at the time the customer relationship is established, and at least once a year thereafter. Institutions must provide, at least on an annual basis, clear and conspicuous notice of their policies and procedures for protecting the consumer's nonpublic personal information. Institutions also must give customers an opportunity to "opt-out" before disclosing nonpublic information to an unaffiliated third party. According to the legislation, the financial institutions may share nearly any information with companies that they are affiliated with. The GLBA is considered a notice statute rather than a restriction statute. It is telling institutions that they must give notice to their clients that they may be sharing information.

The GLBA does not apply to companies or individuals obtaining products or services for business purposes. It applies to personal information about individuals who obtain financial services or products for themselves or their family. The privacy regulations apply to information concerning bank accounts and securities listings. It also protects a broad range of non-public personal information. This includes information:

- obtained during a transaction involving a financial product or service between a financial institution and a consumer
- given by a consumer to a financial institution to obtain a financial product or service
- gained in any way by the financial institution in the process of providing a financial product or service to a consumer

Remember, any personal information that is obtained by a financial institution in connection with providing a financial product or service to a consumer is defined as “financial information”.

Privacy Notices

By July 1, 2001, the consumer should have received a privacy notice from every financial institution where he has an ongoing customer relationship. Financial institutions must send such notices annually thereafter. If one has more than one account with any company, he will probably not receive a notice for each account. He may receive notices from companies where he was not even aware that he had an existing relationship. One will receive a written notice in the mail or by electronic mail if he normally does business online. The notice, whether received in the mail or online, must be clear and conspicuous. In order for it to be effective, one must *agree* to receive the notice by electronic means and must *acknowledge* having received it. Verbal notice alone is not enough. Nor is it enough for a company to post a notice at its office.

The law does not require that the consumer receive a separate notice of the privacy policy, his right to opt-out, or the policy regarding safeguarding confidential information. There is no standard form, so the notice may come in a variety of ways. The exact format is left to the discretion of the company. The law requires only that the notice be "clear and conspicuous" and "designed to call attention to the nature and significance of the information contained" in the notice. Notices may, for example, be mailed along with one’s account statements. His privacy notice may also be included with other notices he is required to receive, for instance, in a mutual fund prospectus. If he does not want his financial institution to share or sell his confidential information, the burden is on him to recognize the notice and follow the opt-out instructions.

Privacy Policies

The consumer may ask a financial institution that he is thinking of doing business with for a copy of its privacy policy. He is only *entitled* to the notice if he is either an existing customer or at the time he establishes a customer relationship with a financial institution. After that, he is entitled to receive a notice annually. A customer relationship means a continuing relationship. One has only a consumer relationship if he has an isolated transaction with a financial institution. One example would be an ATM withdrawal. A consumer is entitled to notice of the financial institution's privacy policy only if it intends to disclose information to nonaffiliated third parties.

Joint Accounts

If two friends/relatives share an account, it is best that **both** of them opt-out to prevent information from being shared or sold. A financial institution cannot *require* that both of them opt-out. If only one of them decides to opt-out, he should ask for separate notices. Then, only information that relates to the one who did not opt-out can be disclosed. The company’s policy regarding joint accounts should be included it its privacy notice to the consumer.

Closed Accounts

Initial and annual notices must inform the consumer of the policies regarding disclosures of information from closed accounts. Financial institutions are not required to send one an "opt-out" notice if his account is closed. However, if he has an existing account for which he has returned the notice saying he does not want his information disclosed, his opt-out election would continue even after he closed the account. If at a later time he decides to open another account

with that bank or other company, he will receive another initial "opt-out" notice, which will apply only to data about his new account. He may choose to "opt-out" of the second account, but his decision with regard to the first account will not change unless he changes it.

"Opt-Out" Choices

The consumer is entitled to a '***reasonable time"*** to respond before his personal data can be disclosed. Usually thirty days is considered "reasonable." If the privacy notice says that one has thirty days to respond, he must return the notice so that it reaches the company *within* 30 days after it was sent to him. When he agrees to accept notice on the Internet, he must respond to the notice *within* thirty days after he acknowledges that he received it, if thirty days is the amount of time he is given to respond. If he has an isolated transaction, which means he has only a "consumer relationship" with a financial institution, he may be required to decide whether to opt-out at the time of the transaction. For example, if an ATM screen posts a privacy policy and opt-out notice, he must elect at that time whether he wants to opt-out. Failure to do so would mean that the financial institution could share or sell his personal data any time after that.

His right to opt-out is continuing. If he fails to return the initial opt-out notice or an annual opt-out notice, his financial institution may sell or share his personal data after a "reasonable" time, usually thirty days. If he later decides that he wants to keep his financial institution from disclosing his personal data, he always has the right to opt-out, but most likely the information is already disclosed. The financial institution is required to give the consumer a "reasonable" means to exercise his opt-out rights. Requiring him to write individual letters is not considered "reasonable" if that is the only way he can opt-out. A formal response may be included with the notice such as a form with check-off boxes or a simple reply form. However, financial institutions are not required to provide pre-paid postage. An e-mail or web site form may be used if one's request is processed via the Internet. A toll-free telephone number may also be used for customers to call and opt-out. One must opt-out using the procedure his bank or other financial company establishes, as long as it is reasonable. The burden is on the consumer to follow the procedures set out by his financial institution.

Disclosed Information

The law and regulations require only that the consumer get notice of the *categories* of information the financial institution collects and the *categories* of information that may be sold or shared with a third party. The notice must give specific examples of the kinds of information included in each category, but this is by no means a complete list of the data that may be disclosed. The privacy notice may tell the consumer that his financial institution collects and may disclose information obtained from him from account applications and give examples such as his name, address, Social Security number, assets and income. One should assume from such a statement that any other information he provides on an account application could be collected and disclosed. Depending on the nature of the application, other information might include former addresses, debt level, mortgage payments, income other than salary such as child support payments, and much more.

GLB and federal regulations *only* keep financial institutions from disclosing one's account number or access code to a third-party nonaffiliated company to use in telemarketing or direct mail marketing. This means that a financial institution can sell one's personal data to a telemarketer, for example, but it cannot sell the means by which his account can be accessed. Unless the consumer opts-out, sensitive information such as details about his health and

treatments, may be disclosed to a third-party nonaffiliated company. He will receive notice of only the category of information that will be disclosed.

Even though the Department of Health and Human Services has adopted rules that apply only to health-related institutions, the consumer has little control over whether medical information captured by financial institutions is shared with an affiliate company. If one pays a medical bill by credit card or check, that information will be recorded and perhaps shared with third parties. One may have greater rights to protect health information under the laws of his state. A state may have a law that makes it a crime for an insurance company to sell information to a financial institution for the purpose of granting credit. The information flow in this case is only restricted one way. This law does not cover information that flows from a financial institution to an insurance company. State regulations about insurance may also give one more rights to medical privacy. A financial institution may receive information directly from the consumer when he fills out an application for a new account. Information about him may also be compiled based upon records of transactions with that company or its affiliates. This may include information about how he uses his credit card, his account balances, late payments, what he buys, and where he shops.

Information may also be collected from nonaffiliated third parties, consumer reporting agencies, or public records. Some financial institutions increase their files about a consumer with information purchased from companies that collect data from consumer surveys, product registration cards, public records, and Census tracts. Such data is used to market products and services to the consumer that the company believes are compatible with his interests. The consumer should consider the amount and kinds of information he supplies to a financial institution that may sell insurance, bank products, and securities. Then he should combine this with the information available from other sources, and he will realize that virtually any detail of financial affairs, health status, spending habits, lifestyle purchases, political affiliations, religious contributions, and more can be collected by his financial institution. Unless he formally objects, it can be shared, sold, rented, or otherwise disclosed with few exceptions.

The privacy notice that one receives from financial institutions does not have to tell him the names of any specific companies or organizations that may buy or receive his personal information. Only the *categories* of companies have to be disclosed to him. His bank may sell his personal information to financial services providers such as an insurance company that is not affiliated with his bank. Other *categories* of nonaffiliated companies that could receive one's information might be non-financial service providers such as retailers, direct marketers, or nonprofit organizations. A company that is an affiliate of his bank may include a credit card company, a brokerage company, a mortgage company, an insurance company and an automobile financing company.

The consumer's opt-out will only prevent disclosure to third party nonaffiliated companies described in the preceding paragraph. A company can still share his information with service providers such as outside companies that print checks. Another exception is that disclosures can be made, without the consumer's knowledge or consent, to outside companies that have entered into a joint marketing agreement with his company. One cannot opt-out of information sharing made with service providers or joint marketers.

Under GLB, a company can share the consumer's personal information with its affiliates. However, the notice he receives is also likely to explain his right to opt-out under the Fair Credit Reporting Act (FCRA). This law gives him the right to prevent a company from sharing information about his credit worthiness and information from his applications with an *affiliate*. His

transaction and experience information can still be shared with affiliates without his consent, according to the FCRA.

Under federal rules, a credit-reporting agency (CRA) cannot sell so-called **credit header** information to third parties. Credit header information includes one's name, address, phone number, age and Social Security number unless his bank has given him the right to opt-out. Credit reporting agencies have filed lawsuits over this issue, claiming they should not be restricted in selling such data. The consumer is free to tell the company that he objects to *any* use of his personal information even if it is permitted by law.

Law Suits Against Financial Institutions

GLB does not contain what is called a private right of action. So the consumer *cannot* go to court and sue for violations of his privacy rights just under that statute. However, under some state laws one might be able to claim that the company's violation of GLB violated other rights he has. The consumer can complain to one of the seven federal agencies that has jurisdiction over financial institutions under GLB. These agencies are identified below along with a description of the kinds of financial institution each oversees. Each agency has enforcement authority under GLB for the area of financial services it regulates. Enforcement authority means that one can complain to the agency, the agency may investigate his complaint, and may bring a court action or administrative case against the company. The agency cannot represent the consumer and cannot give him legal advice on his particular complaint.

Protecting Personal Financial Privacy

The single most important thing the consumer can do to protect his financial privacy is to carefully read all information that comes from a financial institution. He should study the institution's privacy policy. If it causes him concern, he should return the opt-out notice within the specified time. One has very little ability to prevent a financial services company from sharing his customer data with its affiliated companies. The privacy provisions of GLB only pertain to unaffiliated third parties. One cannot prevent his bank from sharing his customer data with its affiliated insurance company or brokerage firm. If the consumer is concerned about affiliate sharing and the ability of these "financial supermarkets" to compile extensive information about him, he must take extra care to conduct his banking with one corporation, keep his insurance accounts with another unaffiliated corporation, and his investments with yet another. Many people have responded to polls and expressed their concerns about their privacy. Opt-out gives the consumer some control over how his personal information is used. Banks and other financial companies may revise and *strengthen* their privacy policies if enough people show their concern for privacy by opting-out.

Federal Agencies

There are seven federal agencies that enforce the privacy provisions of the GLBA.

Federal Deposit Insurance Corporation (FDIC) ~ The FDIC insures consumer deposits made in banks and savings associations. To insure financial soundness and compliance with consumer protection rules, the FDIC, often in coordination with other federal banking agencies, conducts examinations of the institutions included within its jurisdiction. *Board of Governors of the Federal Reserve (Federal Reserve)* ~ The Federal Reserve is the nation's central bank. It sets monetary policy and regulates bank institutions. *Office of Thrift Supervision (OTS)* ~ The OTS is an agency of the U.S. Department of Treasury. OTS regulates state-chartered thrift institutions

such as savings banks and savings and loan associations. *Office of Comptroller of the Currency (OCC)* ~ The OCC is an agency of the U.S. Department of Treasury. This agency charters, regulates and supervises all national banks as well as the federal branches of foreign banks. *National Credit Union Administration (NCUA)* ~ The NCUA regulates and conducts examinations of federal credit unions, which are nonprofit, cooperative financial institutions owned and run by members. *Securities and Exchange Commission (SEC)* ~ The SEC oversees the nation's equity markets which include stock exchanges, broker-dealers, associated persons of broker- dealers, and investment advisors. *Federal Trade Commission (FTC)* ~ The FTC investigates consumer protection and consumer fraud matters that are not specifically within the jurisdiction of another federal agency such as the SEC. The FTC's consumer protection jurisdiction includes debt collection, credit reports, lending, telemarketing, credit repair services and much more.

Recently, the National Association of Insurance Commissioners has adopted the "Standards for Safeguarding Customer Information" model regulation which seeks to satisfy requirements of the GLBA giving insurance regulators the responsibility of making sure that insurance companies safeguard consumers' private information.

More On Gramm-Leach-Bliley

The Gramm-Leach-Bliley Act was passed in 1999 and regulates the ability of financial institutions to disclose "nonpublic personal information" about consumers to non-affiliated third parties. It also requires financial institutions to provide customers with their privacy policies and practices with respect to nonpublic personal information. ***Financial institutions*** are defined under the Act as including institutions engaged in the financial activities of bank hold companies, which may include the business of insuring. Health insurers, however, were not placed under the jurisdiction of any of the seven agencies to which Congress gave the duty to oversee the requirements of the Gramm-Leach-Bliley Act. Rather, the Act gave states the incentive to adopt their own insurance authorities to enforce rules as applicable to health insurers.

The Gramm-Leach-Bliley Act is also known as the *Financial Services Modernization Act*. This Act is broad in scope and regulates many aspects of financial transactions. Title V of this Act includes some specific privacy provisions applicable to insurance transactions. This Act applies to insurers, as discussed above, as well as other types of financial institutions.

Under Title V, Subtitle A, Section 501, the Act states that *each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.*

The specific requirements related to this obligation as put forth in the Act include that appropriate standards must be followed:

- *to insure the security and confidentiality of customer records and information*
- *to protect against anticipated threats or hazards to the security or integrity of such records*
- *to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.*

These appropriate standards are to be established by the appropriate authorities over the various types of financial institutions. Generally, the respective state insurance commissioner's office and state statutes are in authority over insurers doing business in each state.

Section 502 of Title V of the Act includes provisions regarding disclosure of personal information. A financial institution may not disclose to any nonaffiliated third party any nonpublic personal information unless:

- a consumer notice is provided that informs the consumer that such information may be disclosed to a third party;
- the consumer is given the opportunity before information is disclosed, to direct that the such information may not be disclosed to a third party; and
- the consumer is given an explanation of the method that may be used to direct that such information not be disclosed

This section also prohibits a nonaffiliated third party that receives nonpublic personal information from disclosing such information to any other nonaffiliated third party of the financial institution, unless such disclosure would be lawful if made directly from the financial institution to that other party.

Excepted from these disclosure rules is disclosure of nonpublic personal information
(1) *as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with--*

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;
(3)

(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein;

(B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(C) for required institutional risk control, or for resolving customer disputes or inquiries;

(D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;
(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, United States Code, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;
(6)

(A)to a consumer reporting agency in accordance with the Fair Credit Reporting Act, or

(B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

Under Section 503 of Title V of the Act, the financial institution is required to provide a *clear and conspicuous* disclosure to the customer regarding the institution's policies and practices with respect to:

- disclosure of nonpublic personal information to affiliates and nonaffiliated third parties;
- disclosure of nonpublic personal information of people who are no longer customers of the financial institution; and
- protection of nonpublic personal information of consumers.

The disclosure must include:

- the policies and practices used by the institution for disclosing nonpublic personal information to nonaffiliated third parties;
- the categories of persons to whom information may be disclosed as required by the Act;
- the policies and practices used regarding disclosing nonpublic personal information of people who are no longer customers of the institution;
- the categories of nonpublic personal information that are collected by the financial institution;
- the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information; and
- other disclosures as required under the Fair Credit Reporting Act.

Enforcement under the Act for any person engaged in providing insurance is placed under the applicable State insurance authority of the State.

Under Section 521 of Title V of the Act includes provisions related to privacy protection for customer information of financial institutions. This Section prohibits obtaining customer information by false pretenses:

(1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution;
(2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or
(3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

This prohibition does not generally apply to law enforcement agencies when obtaining customer information of a financial institution in connection with the performance of the official duties of the agency. It also does not apply to insurance institutions or any officer, employee, or agency of an insurance institution, from information *as part of an insurance investigation into criminal activity, fraud, material misrepresentation, or material nondisclosure that is authorized for such institution under State law, regulation, interpretation, or order.*

Section 523 provides for a fine or imprisonment, or both for anyone who knowingly and intentionally violates, or knowingly and intentionally attempts to violate Section 521 of this Act.

Fair Credit Reporting Act

The Fair Credit Reporting Act regulates credit and consumer reports. This Act was originally enacted in 1970 and has been amended by other legislation since that time.

The Act regulates consumer reports and investigative consumer reports. Under the act a consumer report is defined as follows:

(1) In general. The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for

(A) credit or insurance to be used primarily for personal, family, or household purposes;
(B) employment purposes; or
(C) any other purpose authorized under section 604 [§ 1681b].

(2) Exclusions. The term "consumer report" does not include

(A) any
(i) report containing information solely as to transactions or experiences between the consumer and the person making the report;
(ii) communication of that information among persons related by common ownership or affiliated by corporate control; or
(iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons;
(B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;
(C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosures to the consumer required under section 615 [§ 1681m]; or
(D) a communication described in subsection (o).

The Act also defines ***"investigative consumer reports",*** which the insurance industry generally refers to as "inspection reports:"

The term "investigative consumer report" means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a

creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

Permissible Purposes of Consumer Reports

Under the Fair Credit Reporting Act, consumer reports may only be furnished for certain purposes by consumer reporting agencies. One of these permissible purposes is furnishing a report to a person the consumer reporting agency has reason to believe intends to use in connection with the underwriting of insurance.

Furnishing Consumer Reports

Under the Fair Credit Reporting Act, a consumer reporting agency may only issue a consumer report that is not initiated by a consumer request if the consumer authorizes the agency to provide the report or the transaction for which the consumer report is used is considered a "firm offer of insurance." If a consumer report is issued because the transaction is a "firm offer of insurance" and is not authorized by the consumer, the report may only furnish the name and address of the consumer, an identifier used solely to verify the identify of the consumer and other information pertaining to the consumer that does not provide the relationship of experience of the consumer with a particular creditor or other entity.

Items That May Not Be Included In Consumer Reports

Consumer reports initiated by the consumer or authorized by the consumer may not generally include:

- bankruptcy that occurred more than ten years before the report;
- civil suits, civil judgments and records of arrest that were recorded by the greater of seven years before the report of the governing statute of limitations has expired;
- paid tax liens that were paid more than seven years before the report;
- accounts placed for collection or charged to profit or loss more than seven years before the report; and
- any adverse information, other than records of convictions of crimes, that occurred more than seven years before the report.

Disclosing Investigative Consumer Reports

In order to have an investigative report prepared, it must be clearly and accurately disclosed to the consumer than an investigative consumer report, that includes information about the consumer's character, general reputation, personal characteristics, and mode of living, may be made. The disclosure to the consumer must:

- be in writing;
- be mailed or delivered to the consumer not more than three days after the date the report was requested; and
- include a statement that the consumer has the right to request information about the nature and scope of the investigation.

If the consumer requests information about the nature and scope of the investigation, the person who caused the report to be prepared must comply with the consumer's request in writing not later than five days after the request was received.

Disclosures to Consumers

The Fair Credit Reporting Act and related legislation also requires that reporting agencies, upon request from the consumer, disclose:

- all information in the consumer's file at the time of the request, other than credit scores or similar risk predictors;
- sources of information, other than information used solely for an investigative consumer report which must be available if needed for the discovery process in an applicable court case;
- the identity of each person who procured a consumer report generally in the last one year period only; and
- dates, original payees and amounts of any checks upon which is based any adverse characterization of the consumer.

A consumer reporting agency must also include a "Summary of Rights" with the disclosure to the consumer. A Summary of Rights includes:

- a brief description of the Fair Credit Reporting Act and all consumer rights within it;
- an explanation of how a consumer may exercise rights under the Fair Credit Reporting Act;
- a list of Federal agencies responsible for the enforcement of the provisions in the Act, including addresses and phone numbers;
- a statement that the consumer may have additional rights under State law; and
- a statement that a consumer reporting agency is not required to remove accurate derogatory information from a consumer's file that is in compliance with the Act.

Disputed Information

If a consumer disputes the information from a consumer reporting agency, the consumer reporting agency must reinvestigate the information free of charge. The consumer reporting agency must then record the current status of the disputed information or delete inaccurate information, generally within thirty days from the date the consumer reporting agency receives the notice of dispute from the consumer. In some cases, the consumer reporting agency can deny reinvestigation because it determines the request is frivolous or irrelevant.

If information in a consumer's file is found to be inaccurate or unverifiable, the consumer reporting agency must promptly delete the item or modify it as applicable.

Special Restrictions On Investigative Consumer Reports

If a consumer reporting agency prepares a subsequent investigative consumer report on the same consumer, it cannot include any adverse information in the report, other than matters of public record, unless the adverse information has been verified during the process of making the subsequent report, or the adverse information was received within three months prior to the date the subsequent report is furnished.

Requirements For Uses Of Consumer Reports

The insurance company is a user of consumer reports and is subject to certain rules found in the Fair Credit Reporting Agency and related legislation. Under these rules, if adverse actions are taken on the basis of information found in consumer reports, the insurer must:

- provide to the consumer oral, written, or electronic notice of the adverse action;
- provide to the consumer orally, in writing or electronically the name, address and phone number of the consumer reporting agency that furnished the report along with a statement that the consumer reporting agency is unable to provide the consumer with the specific reasons the adverse action was taken; and
- provide to the consumer oral, written or electronic notice of the consumer's rights to obtain a free copy of the report and to dispute the accuracy or completeness of information.

Duties of Users Making Insurance Solicitations On The Basis of Information Contained in Consumer Files

Anyone who uses a consumer report in connection with an insurance transaction not initiated by the consumer and that is a "firm offer of insurance" must include with the solicitation:

- a written statement that information in the consumer report was used in connection with the transaction, that the consumer received the offer of insurance because the consumer satisfies the criteria of insurability for the offer;
- a statement that, if applicable, the insurance may not be extended if the consumer does not meet the criteria of insurability; and
- a statement that the consumer has the right to prohibit information contained in the consumer's file with any consumer reporting agency from being used in any credit or insurance transaction not initiated by the consumer.

The person who makes an offer of insurance based on a consumer report must also maintain on file the criteria used to select the consumer to receive the offer, all criteria bearing on credit worthiness or insurability that are used to select consumers for the offer, and any requirement for the furnishing of collateral as a condition of insurability for three years after the offer was made.

PROTECTING HEALTH INFORMATION PRIVACY

Importance of Medical Records

Health information and the medical record reveal some of the most intimate aspects of an individual's life. In addition to diagnostic and testing information, the medical record includes the details of a person's family history, genetic testing, history of diseases and treatments, history of drug use, sexual orientation and practices, and testing for sexually transmitted diseases. Subjective remarks about a patient's demeanor, character, and mental state are sometimes a part of the record.

The medical record is also the primary source for much of the health care information sought by parties outside the direct health care delivery relationship. These data are important because health care information can influence decisions about an individual's access to credit, admission to educational institutions, and his or her ability to secure employment and obtain insurance. Inaccuracies in the information, or its improper disclosure, can deny an individual access to these basic necessities of life, and can threaten an individual's personal and financial well being.

At the same time, accurate and comprehensive health care information is critical to the quality of health care delivery, and to the physician-patient relationship. Many believe that the efficacy of the health care relationship depends on the patient understanding that the information recorded by a physician will not be disclosed. Without these assurances, many patients might refuse to provide physicians with certain types of information needed to render appropriate care.

Informational Privacy Rights

Definitions of privacy and confidentiality rights have largely depended upon the definitions of a medical record and decisions about who owns it. A general definition of a medical record is any data that are collected and used to diagnose or treat a patient's health problems. State statutes, case law and federal laws regulate the ownership and use of patient medical records and data. Some statutes and common law doctrines apply to any medical records stored in any medium; others appear to have no application to electronically stored records. Still others apply only to records created and maintained by certain types of providers.

Those laws which do exist seek to protect individual privacy by limiting or prohibiting the disclosure of information which may identify an individual or which may publicly disclose private facts about an individual. The applicable federal laws, such as the Privacy Act, largely regulate permissible uses by government agencies and employees, or uses of certain narrowly defined types of medical information. Very few state laws have universal applicability, concentrating instead on certain types of information such as HIV test results or certain types of providers. Under most state laws, the originator or creator of a medical record generally owns the record. This ownership, however, is almost universally subject to a patient's interests in the information contained within the record. In other words, the patient has the right (though not always absolute) to limit or otherwise define the disclosure. He may compel the dissemination of the information or he may require that the information not be disclosed, subject to many exceptions.

In the clinical data management (CDM) environment, where no single entity creates the record, it is unclear with whom the record's ownership rests. It is also unclear, as non-treatment related data are included in patient records and as derivative records are created, just what constitutes the patient's medical record. The bundle of privacy rights is based upon ethical, common law and statutory requirements - all of which protect one's autonomy or privacy in one's medical information. It is helpful to understand these rights as what some commentators have termed "information privacy rights."

Physician-Patient Confidentiality

The physician-patient relationship is confidential. Were that not the case, patients would be reluctant to divulge information necessary to the diagnosis and treatment of their problems. The physician's duty to keep information private and confidential derives from ancient physician oaths, presently unchanged at their core, and from more recent legal recognition that an individual has a right to keep those things private that he desires to be kept private. Most states' physician licensure statutes mandate that, except as the law otherwise requires and unless directly related to the treatment and care of an individual patient or consented to by the patient, a physician must keep all client confidences. Pennsylvania, for example, provides that a physician may be subject to disciplinary procedures for "revealing identifiable facts, obtained as the result of a physician-patient relationship, without the prior consent of the patient, except as authorized or required by statute." Courts in an increasing number of states have held hospitals to this same obligation, pursuant to a fiduciary or contractual duty to the patient, or as provided in a statute.

Confidentiality is the sine qua non of the physician-patient relationship. Rules of physician-patient confidentiality and other related doctrines protect one's privacy. Confidentiality is a significant mechanism by which a patient's right to privacy is maintained and respected. Privacy protection, however, is not absolute. Privacy may be conditioned upon the public's right to know, or the government's legitimate interest in, certain information. It may be waived or consented to by the patient. A waiver or consent must be the product of a decision made after being informed of the risks and benefits of such disclosure.

Privacy, confidentiality and informed consent doctrines are nothing new to health care or to medical records managers. CDM systems, however, create new or magnify existing legal issues. From at least the 1970s through the present, groups such as the Privacy Protection Study Commission have studied privacy protections in electronic health records systems. They have also advocated various safeguards that are instructive to CDM system planners. For example, the American Medical Association’s (AMA) Current Opinions require the "utmost effort and care" to protect the confidentiality of computerized medical records. Among the AMA's guidelines are requirements that both the patient and physician be advised about the very existence of computerized medical databases. In addition, the AMA requires that this information be communicated to the patient and physician before the physician releases the information to the database. Most importantly, the AMA characterizes fully disclosure to the patient of this information as necessary to obtaining the patient's fully informed consent to treatment.

CDM systems should define and insure security. Security, as defined by the National Information Infrastructure Task Force is the totality of safeguards in a computer-based information system. Methods should protect both the system and the information contained within it from unauthorized access and misuse, and accidental damage. It consists of hardware, software, personnel policies, information management policies, and disaster preparedness. The

most effective CDM system will design safeguards, which ensure that information privacy rights are respected. Methods of achieving this can include:

- Establishing institutional and employment policies which outline permissible and non-permissible uses of patient data and establish mechanisms for reviewing and enforcing these policies
- Executing User Agreements which specify users' obligations regarding system access and the collection, use and dissemination of patient data
- Using public-key encryption of information so that information is safeguarded and the originator of data can be identified
- Re-designing patient consent forms and releases which allow patients to consent to the release and use of information which can be readily associated with the patient and is used for diagnosis, treatment, utilization review, quality assurance and reimbursement
- Establishing mechanisms for patient access to all of the information collected identifying that patient and institute methods which allow patients to correct erroneous information
- Blocking user access, through varying security levels of access codes, to data fields or records which the user is not authorized to access pursuant to the patient consent
- Using patient identifiers other than the patient's social security number to ensure that users (authorized or unauthorized) cannot access and collate records they weren't intended to access

As health care delivery systems integrate and managed care pervades the marketplace, the ability to collect, interpret and disseminate health care data becomes a very critical challenge of cost-efficient, quality, outcome-driven health care delivery. Clinical data management (CDM) systems enable health care organizations, employers and payers, through a core central data repository, to better manage and deliver care to patients, employees and insureds. CDM system planners must find the highest common denominator, in terms of privacy protection, in order to comply with differing and often contradictory statutory and regulatory requirements.

Medical Records and Client Privacy

Individual health and medical data can be collected, collated, stored, analyzed and distributed in unprecedented quantities and put to diverse uses. Payers can tap patient data for claims payment. They use it for utilization review, underwriting and coverage decisions. Employers use health data to reduce their health care and workers compensation costs, as well as to identify employees who may be costly in the future. Health care providers use the data for research, to collect reimbursement, coordinate diagnosis and treatment, conduct quality assurance and monitor other providers. Clinical data repositories and management systems will likely reduce health care costs and improve patient care. Clinical data management (CDM) systems and increasing automation of the electronic medical record (EMR) also present significant patient privacy and confidentiality issues, among others, which executives and planners must recognize. Understanding these issues insures that CDM and EMR systems are effective without exposing its hosts and users to liability.

National Patient Record Privacy

Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use

and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. On December 20, 2000, President Clinton presented the final version of medical privacy regulations drafted by the Department of Health and Human Services (HHS). The regulations are the first federal privacy protections for medical information and will apply to both paper and electronic health records. The Department of Health and Human Services began drafting the regulations when Congress failed to pass federal legislation concerning medical privacy on August 21 of 1999.

In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by comments received from the public. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for thirty days. After that comment period, President Bush and Secretary Thompson allowed the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes during the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. On July 6, 2001, HHS issued its first set of guidance to answer common questions and clarify confusion about the final rule's provisions. As required by the HIPAA law, most covered entities have two full years - until April 14, 2003 - to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions such as electronic billing and funds transfers electronically. All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule. Under the final rule, patients will have significant new rights to understand and control how their health information is used:

- Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.
- Patients will be able to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients.
- Health care providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment, and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.

- People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes. Health information covered by the rule generally may not be used for purposes not related to health care - such as disclosures to employers to make personnel decisions, or to financial institutions - without explicit authorization from the individual. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

Safeguard Standards

The final rule establishes the privacy safeguard standards that covered institutions must meet, but it also gives covered institutions the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Covered entities generally will have to:

Adopt written privacy procedures. These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.

*Train employees and designate a privacy officer***.** Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

Establish accountability for medical records use and release. In HIPAA, Congress provided penalties for covered entities that misuse personal health information. Those penalties include:

- Civil penalties ~ Health plans providers and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated.

- Federal criminal penalties ~ Under HIPAA, Congress also established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Balance public responsibility with privacy protections. In limited circumstances, the final rule permits - but does not require - covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities. These permitted disclosures include:

- emergency circumstances
- identification of the body of a deceased person
- the cause of death

- public health needs
- research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- oversight of the health care system
- judicial and administrative proceedings
- limited law enforcement activities
- activities related to national defense and security

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

Provide protection for psychotherapy notes. Psychotherapy notes used only by a psychotherapist are held to a higher standard of protection because they are not part of the medical record and are never intended to be shared with anyone else. All other personal health information is considered to be sensitive and protected consistently under this rule.

Make equivalent requirements for government entities. The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

The Medical Information Bureau

The bureau is a non-profit organization made up of most of the insurance companies in the country. The purpose of the MIB is not to be an industry "big brother" collecting all kinds of information on insurance applicants and "black booking" them for life if something bad happens. The true purpose of the MIB is to simply protect insurance companies from significant missing information or misinformation in regards to life insurance underwriting.

MIB codes consist of information on health or underwriting problems, the source of the information, the date the code was reported, and the approximate date of the actual information. The codes do not contain any information on which insurance company reported the code, or what underwriting action that insurance company took. There is no "decline" or "rated" code. It really makes no difference if someone with a history of a heart attack in 1980 applies to a conservative company and gets declined, or applies to a liberal company and gets standard coverage. Either way, a code to the MIB would be reported stating that this client had heart history in 1980 found in an APS.

The Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act, known as HIPAA. The Act is broad in scope, addressing many facets of health insurance, including employer sponsored group health plans, long-term care plans, Medical Savings Accounts, health insurance plans for self-employed individuals, accelerated death benefits, and more. The subject of this section is "Administrative Simplification," part of HIPAA's provisions, and the "Privacy Rule" created pursuant to it.

Administrative Simplification is found in Sections 261-264 of HIPAA. Within its provisions, Congress directs the Secretary of Health and Human Services (the Secretary) to adopt standards for transactions so that information may be exchanged electronically among health plans and providers. These provisions also require the entities covered by them to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, and to protect against threats to the security of the information and any unauthorized uses and disclosures. The entities are also required to enforce compliance among its officers and workforce. The provisions also require the Secretary to issue standards with respect to the privacy of individually identifiable health information.

The few lines in HIPAA addressing these activities have spawned many requirements for health plans, health care providers and many of the entities that work with them. Those entities covered by the provisions, known as "covered entities," must now publish privacy notices, obtain consent or authorization for many uses and discourses of health information, and are subject to compliance review by the Department of Health and Human Services. They must also put into place training and procedures to implement the requirements of the law, create forms and notices and other documents, and create and maintain systems to keep health information secure and private. Entities must keep records of their compliance with the Administrative Simplification requirements and be ready to provide an accounting to individuals and the federal regulators.

Below, we will examine the Administrative Simplification law, the Privacy Rule and other federal privacy regulations affecting insurers. First we will look at the Administrative Simplification provisions, and the reasoning the federal government has stated is behind many of its key provisions. Next we will examine the "Privacy Rule," issued by the Department of Health and Human Services, and which puts forth the privacy standards from the Secretary required under Administrative Simplification. Other federal privacy regulations follow including the Guidance for the Privacy Rule issued by the Department of Health and Human Services.

Administrative Simplification

The final rule for the Standards for Privacy of Individually Identifiable Health Information, known as the "Privacy Rule," implements the privacy requirements of the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Privacy Rule applies to health plans, health care clearinghouses and certain health care providers. It also includes standards regarding the rights of individuals regarding their health information, the procedures for exercising these rights and the authorized and required uses of the information.

This chapter will consider the HIPAA provisions, found in Sections 261-264, known as "Administrative Simplification." It will also provide some insight to the reasoning behind the enactment of this section of HIPAA. .

Purpose of Administrative Simplification in HIPAA

The Administrative Simplification Regulations found in HIPAA have the following purposes:

1. to protect and enhance the rights of consumers by providing access to their health information and controlling the inappropriate use of that information;
2. to improve the quality of health care by restoring trust in the health care system among consumers, health care professionals and others committed to the delivery of care; and
3. to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

Electronic Transmission of Personal Information

The Administrative Simplification provisions of HIPAA specifically address electronic information. As will be discussed later, the protection of all individually identifiable health information became the subject of the Privacy Rule, but the genesis of the regulations laid in the concerns about the ease with which large amounts of private information may be stored, transmitted and accessed through electronic information systems. As the Federal Register, in the same issue cited earlier, notes, "Until recently health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, however, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information." It goes on to state: "This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve

the quality of care delivered in the U.S. The National Research Council recently reported that 'the Internet has great potential to improve Americans health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals.' See 'Networking Health: Prescriptions for the Internet,' National Academy of Sciences (2000)."

The transformation to an electronic system from a paper system has reduced or eliminated many of the financial and operational barriers that in the past had served as a natural wall of protection around the privacy of personal records. Allowing easy access, easy duplication, and easy communication of information that in the past may have been difficult to access and assemble, cumbersome and expensive to copy, and time-consuming to communicate has broken down the old protective walls. Today, because information flows freely and easily in a swift and broad river of communication, purposeful privacy protection regulation has become, according to the federal government, essential.

The advent of effective electronic transmission of data also provides marketing and entrepreneurial opportunities. Some of these opportunities will make good use of information and may help both individuals and society. Other opportunities may have the potential to harm, especially if individually identifiable information is used maliciously, such as for identity theft. In order to create the perfect "target market," businesses may attempt to utilize sensitive information in a manner that may lead to embarrassment or worse for individuals within the data they access. Therefore, Administrative Simplification includes the establishment of marketing standards, regulating what marketing uses are prohibited and the allowable uses of health information for marketing purposes.

Another reason for federally regulated privacy laws is that the electronic age has made information easily accessible all across the nation. This information may benefit those in other communities and states, if it can be shared in ways that protects the privacy rights of individuals. By relying on individual states to implement such rules, it may be difficult for those who may utilize information for the benefit of many to comply with conflicting laws among the states in which it seeks to access information. For this reason, Congress passed federal regulations to govern the protection of sensitive health information.

The Current Health Care System

The electronic transmission of data is only one facet of the change in America's health care system over the past few decades. In the past, health care was provided largely through one-on-one interactions between patients and their physician or their clinic. Today, the popularity of managed care has spawned large integrated health care delivery networks. These networks collect, process and share patient information in order to provide treatment. These activities also result in increasing numbers of people having access to health information. Besides the workforce within the entity providing health care, the workforce of entities who perform certain duties for the health care provider, such as billing, also have access. Employers also often perform certain duties related to health plans they offer, such as front-end processing of enrollment forms and claim forms, and therefore employer workforces may also have access to health information. Other entities with access to health information may include pharmacies, clinical laboratories, life and health insurance companies, self-insured employers and medical information bureaus.

Prior to the passage of Administrative Simplification, there were no rules governing how health information was used by secondary and tertiary users. For example, a pharmacy could receive

health information in order to determine whether an insurance plan should cover a prescription, and then use that information to market other products to the patient.

The Federal Register: December 28, 2000, Volume 65, Number 250 also listed recent breaches of privacy in order to demonstrate the need for privacy regulation:

- *"A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).*

- *A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).*

- *An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10,1996).*

- *The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).*

- *A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).*

- *A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy database included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).*

- *A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).*

- *In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).*

- *A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997)."*

The ever-growing volume of health information, accessible by increasing numbers of people, is another reason Congress authorized passage of the Administrative Simplification provisions under HIPAA.

Privacy and Effective Health Care

Protecting the privacy of health information not only avoids misuse, unauthorized use, embarrassment and harm, but may also contribute to the providing of more effective health care. A cornerstone of providing effective medical care is a complete understanding of a patient's condition. If a patient is concerned about the ways in which his or her health information may be used, the patient is more likely to conceal intimate details of their health history. Patients must trust their physician or other health care provider enough to provide them

with a full picture of their health, symptoms and medical history, and other details of their lives. If a patient does not provide full and accurate information, a provider may prescribe a treatment plan that is completely inappropriate for a patient.

Accurate health information is also important for public health activities. Complete and accurate information is needed by public health agencies and all those involved in public health efforts in order to identify public health trends and evaluate public health programs and plans. The insurance industry also needs accurate information to enable proper underwriting, claims processing, and identification of fraud. Scientists need accurate information to conduct research. Protecting the disclosure and use of health information should provide a higher likelihood that all these entities will not be given inaccurate or incomplete health information from individuals who fear it will be used in improper or inappropriate ways.

Harmful Uses of Health Information

The Federal Register also cited several instances where health information was used in an explicitly harmful manner:

- *"A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the National Law Journal, May 30,1994.*

- *A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See Estate of Behringer v. Medical Center at Princeton, 249 N.J. Super.597.*

- *A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See New York Times, October 10, 1992, Section 1, page 25.*

- *A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998)"*

Examples of uses of health information in harmful ways such as these are another reason Congress passed Administrative Simplification.

Social Security Act -- Part C--Administrative Simplification

The first portion of the Administrative Simplification provisions, §1171, provides the definitions of important terms within the law:

DEFINITIONS
SEC. 1171. [42 U.S.C. 1320d] For purposes of this part:
(1) CODE SET.--The term "code set" means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.
(2) HEALTH CARE CLEARINGHOUSE.--The term "health care clearinghouse" means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

(3) HEALTH CARE PROVIDER.--The term "health care provider" includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

(4) HEALTH INFORMATION.--The term "health information" means any information, whether oral or recorded in any form or medium, that--

(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(5) HEALTH PLAN.--The term "health plan" means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan--

(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

(ii) is administered by an entity other than the employer who established and maintains the plan.

(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

(D) Part A or part B of the Medicare program under title XVIII.

(E) The Medicaid program under title XIX.

(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

(I) The health care program for active military personnel under title 10, United States Code.

(J) The veterans health care program under chapter 17 of title 38, United States Code.

(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term "individually identifiable health information" means any information, including demographic information collected from an individual, that--

(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(7) STANDARD.--The term "standard", when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.
(8) STANDARD SETTING ORGANIZATION.--The term "standard setting organization" means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

Section 1172 of the Law applies the standard under Part C, Administrative Simplification, to health plans, health care clearinghouses and health care providers who transmit health information in connection with transactions referred to in § 1173(a)(1). This section also includes procedural requirements for the adoption of standards.

GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS
SEC. 1172. [42 U.S.C. 1320d-1]
(a) APPLICABILITY.--Any standard adopted under this part shall apply, in whole or in part, to the following persons:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).
(b) REDUCTION OF COSTS.--Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.
(c) ROLE OF STANDARD SETTING ORGANIZATIONS.--
(1) IN GENERAL.--Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.
(2) SPECIAL RULES.--
(A) DIFFERENT STANDARDS.--The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if--
(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and
(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, United States Code.
(B) NO STANDARD BY STANDARD SETTING ORGANIZATION.--If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part--
(i) paragraph (1) shall not apply; and
(ii) subsection (f) shall apply.
(3) CONSULTATION REQUIREMENT.--
(A) IN GENERAL.--A standard may not be adopted under this part unless--
(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard.

(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following:

(i) The National Uniform Billing Committee.

(ii) The National Uniform Claim Committee.

(iii) The Workgroup for Electronic Data Interchange.

(iv) The American Dental Association.

(d) IMPLEMENTATION SPECIFICATIONS.--The Secretary shall establish specifications for implementing each of the standards adopted under this part.

(e) PROTECTION OF TRADE SECRETS.--Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

(f) ASSISTANCE TO THE SECRETARY.--In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) APPLICATION TO MODIFICATIONS OF STANDARDS.--This section shall apply to a modification to a standard (including an addition to a standard) adopted under section 1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

Section 1173 requires the Secretary of the Department of Health and Human Services to adopt standards for transactions to enable health information to be exchanged electronically. Section 1173(a)(1) identifies the transactions covered by these laws, including other transactions determined appropriate by the Secretary. This Section also requires the Secretary to adopt specific stands for unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Section 1173(d) is the portion of the Law that particularly requires the covered entities to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information and to ensure compliance with Administrative Simplification by the entity's officers and workforce.

STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

SEC. 1173. [42 U.S.C. 1320d-2]

(a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.--

(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

(A) the financial and administrative transactions described in paragraph (2); and

(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

(2) TRANSACTIONS.--The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

(A) Health claims or equivalent encounter information.

(B) Health claims attachments.

(C) Enrollment and disenrollment in a health plan.

(D) Eligibility for a health plan.
(E) Health care payment and remittance advice.
(F) Health plan premium payments.
(G) First report of injury.
(H) Health claim status.
(I) Referral certification and authorization.

(3) ACCOMMODATION OF SPECIFIC PROVIDERS.--The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) UNIQUE HEALTH IDENTIFIERS.--

(1) IN GENERAL.--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

(2) USE OF IDENTIFIERS.--The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) CODE SETS.--

(1) IN GENERAL.--The Secretary shall adopt standards that--

(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

(B) establish code sets for such data elements if no code sets for the data elements have been developed.

(2) DISTRIBUTION.--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

***(d) SECURITY STANDARDS FOR HEALTH INFORMATION.*—[Bolding Added]**

(1) SECURITY STANDARDS.--The Secretary shall adopt security standards that--

(A) take into account--

(i) the technical capabilities of record systems used to maintain health information;

(ii) the costs of security measures;

(iii) the need for training persons who have access to health information;

(iv) the value of audit trails in computerized record systems; and

(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated--

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) ELECTRONIC SIGNATURE.--

(1) STANDARDS.--The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS.--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

Section 1174 requires the Secretary to establish standards by specified dates, depending upon the transaction type. The final rule for these transaction standards, known as the Transaction Rule, was not promulgated until August 17, 2000, after the specified date. About 17,000 comments were received in response to the proposed rule, and the Department of Health and Human Services attempted to address the concerns within them and to build a consensus in the industry regarding the standards.

TIMETABLES FOR ADOPTION OF STANDARDS

SEC. 1174. [42 U.S.C. 1320d-3] (a) INITIAL STANDARDS.--The Secretary shall carry out section 1173 not later than 18 months after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after such date.

(b) ADDITIONS AND MODIFICATIONS TO STANDARDS.--

(1) IN GENERAL.--Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1173, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

(2) SPECIAL RULES.--

(A) FIRST 12-MONTH PERIOD.--Except with respect to additions and modifications to code sets under subparagraph (B), the Secretary may not adopt any modification to a standard adopted under this part during the 12-month period beginning on the date the standard is initially adopted, unless the Secretary determines that the modification is necessary in order to permit compliance with the standard.

(B) ADDITIONS AND MODIFICATIONS TO CODE SETS.--

(i) IN GENERAL.--The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

(ii) ADDITIONAL RULES.--If a code set is modified under this subsection, the modified code set shall include instructions on how data elements of health information that were encoded prior to the modification may be converted or translated so as to preserve the informational value of the data elements that existed before the modification. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption and cost of complying with such modification.

Section 1175 also deals with the Transaction Rules and prohibits health plans from refusing to process or to delay the process of transactions presented in standard format. It also establishes a timetable for compliance.

Civil penalties are established in § 1176 for violations of Part C.

GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS
SEC. 1176. [42 U.S.C. 1320d-5]
(a) GENERAL PENALTY.--
(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.
(b) LIMITATIONS.--
(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may not be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177.
(2) NONCOMPLIANCE NOT DISCOVERED.--A penalty may not be imposed under subsection (a) with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.
(3) FAILURES DUE TO REASONABLE CAUSE.--
(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--
(i) the failure to comply was due to reasonable cause and not to willful neglect; and
(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.
(B) EXTENSION OF PERIOD.--
(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.
(ii) ASSISTANCE.--If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary.
(4) REDUCTION.--In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) that is not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

Section 1177 establishes penalties for knowingly using a unique health identifier, or obtaining or disclosing individually identifiable health information for violating Part C.

WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION
SEC. 1177. [42 U.S.C. 1320d-6]
(a) OFFENSE.--A person who knowingly and in violation of this part--
(1) uses or causes to be used a unique health identifier;
(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

(b) PENALTIES.--A person described in subsection (a) shall--

(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

Section 1178 provides that the requirements of Part C, and any standards or implementation specifications adopted under Part C, preempt contrary state law. If state laws (1) are necessary, as determined by the Secretary, for certain purposes set forth in the statute, (2) address controlled substances, as determined by the Secretary, or (3) are contrary to federal law and are more stringent than federal law, they are not preempted.

EFFECT ON STATE LAW

SEC. 1178. [42 U.S.C. 1320d-7]

(a) GENERAL EFFECT.--

(1) GENERAL RULE.--Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

(2) EXCEPTIONS.--A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall not supersede a contrary provision of State law, if the provision of State law--

(A) is a provision the Secretary determines--

(i) is necessary--

(I) to prevent fraud and abuse;

(II) to ensure appropriate State regulation of insurance and health plans;

(III) for State reporting on health care delivery or costs; or

(IV) for other purposes; or

(ii) addresses controlled substances; or

(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

(b) PUBLIC HEALTH.--Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

(c) STATE REGULATORY REPORTING.--Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

Section 1179 states that the provisions set forth in the provisions do not apply to financial institutions when “authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.”

Section 264 is another provision in HIPAA that address the Administrative Simplification provisions. It requires the Secretary to issue standards with respect to the privacy of individually identifiable health information.

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.
(a) IN GENERAL.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.
(*b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:*

--The rights that an individual who is a subject of individually identifiable health information should have.
--The procedures that should be established for the exercise of such rights.
--The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--
IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).
PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.
(d) CONSULTATION.--In carrying out this section, the Secretary of Health and Human Services shall consult with--

1. *the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and*

2. *the Attorney General.*

The Privacy Rule

Summary of the Privacy Rule

The final regulations required under Administrative Simplification were effective on April 14, 2001. The regulations are commonly known as the “Privacy Rule.” The entities covered by the Privacy Rule include health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. Health plans include HMOs, health insurers, and group health plans including employee welfare benefit plans. Health care clearinghouses are entities that process health information going from a health-care provider to a payer. The type of information protected under these rules include all medical

records and other individually identifiable health information and used for disclosed by a covered entity in any form, whether it electronically, on paper, or orally.

The Privacy Rule applies equally to the private sector and the public sector. Generally, if laws in force in the states are stricter than the federal laws and regulations, the state laws apply.

The type of health information that is protected by the Privacy Rule is information that

1. relates to a person's physical or mental health, the provision of health care, or the payment of health care;
2. identifies or could be used to identify, the person who is the subject of the information;
3. may be created or received by a covered entity; and
4. is transmitted or maintained in any medium.

The Privacy Rule represents the first time federal rules regarding the protection of privacy of health information and guarantee patient access to such information have been created. States have enacted privacy regulations regarding the protection of health information, but state regulations generally apply only to certain types of conditions, such as mental illness, AIDS and HIV, cancer or other specified condition. The federal rules are much broader than those found in most state's laws.

Through the Privacy Rule, patients now have the right to access their own medical records. In the past, patients did not have the ability to review their records as a right and it was possible that they would be denied access to their own information. Providers and health plans are now required to provide patients with a clear written explanation of how the patients' information may be used and disclosed. In order for health care providers to share information about a patient for treatment, payment, or health care operations the provider must obtain patient consent. Specific separate authorization must also be obtained for non-routine disclosures and most non-health care purposes. Patients also have the right to request restrictions on the use and disclosure of their health information.

In addition to patients having access to their own health information, the patient also has the right to obtain documentation of who else has had access to their information. In addition, individuals have the right to request amendments or corrections to health information that is incorrect or incomplete. Certain exceptions apply to the patient's right to access their information, such as when access would endanger the life or safety of an individual.

The Privacy Rule makes clear that an individual's health information may only be used for health purposes. Any use of information not related to health care must be explicitly authorized by the individual. In addition, disclosure of health information must be limited to the minimum necessary to fulfill the purpose of the disclosure.

Each entity covered by the Privacy Rule must adopt written privacy procedures. These procedures must include who has access to protected information, how it will be used within the

covered entity, and when and how the information may be disclosed. In addition, covered entities must train employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

Under the Administrative Simplification provisions of HIPAA, common penalties have been established, for those who violate these rules and misuse personal health information. Civil penalties may apply to health plans, providers and clearing houses that violate the privacy standards. Civil penalties are $100 per violation, up to a $25,000 per person, per year for each requirement or prohibition violated. Federal criminal penalties may also apply to those who knowingly violate patient privacy. Criminal penalties may be up to $50,000.00 and up to 1 year in prison for obtaining or disclosing protected health information, and up to $100,000 and up to five years in prison for obtaining protected health information under false pretenses, and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use the information for commercial advantage, personal gain or malicious harm.

The Privacy Rule does allow covered health organizations and persons to continue certain disclosures without individual authorization for specific public responsibilities. The circumstances under which such disclosures are permitted include:

- Emergency circumstances
- Identification of the body of a deceased person or the cause of death
- Public health needs
- Research in certain circumstances such as when a waiver of authorization is approved by a privacy board or Institutional Review Board
- Oversight of the health care system
- Judicial and administrative proceedings
- Limited law enforcement activities
- Activities related to national defense and security

Psychotherapy notes are protected under special rules due to their sensitive nature. These notes, which are used only by a psychotherapist, are not part of the medical record and are never intended to be shared with anyone else. Written disclosures are generally required, and health plans may not condition enrollment or eligibility for benefits of the patient providing an authorization for the use and disclosure of psychotherapy notes.

Obtaining Consent

Certain activities require the consent of an individual under Administrative Simplification and the Privacy Rule.

Treatment, Payment or Health Care Operations

Prior to using or disclosing protected health information to carry out treatment, payment or health care operations, a health-care provider must generally obtain a patient's consent. A health care provider may condition treatment upon the patient providing a consent form. Health plans may condition enrollment on provision of consent by an individual.

Directories

If information is to be provided to directories, such as a hospital's patient directory, or to next of kin and or other persons, the patient must be given notice prior to the information being disclosed and must have the opportunity to opt out of this use of information.

Marketing and Fund-Raising

If information will be used for marketing and fund-raising, the covered entity must give patients the opportunity to opt out of further disclosures during the initial contact with the individual.

Notice of Privacy Practices

Health plans and health care providers must provide written notice of their privacy practices, including a description of an individual's rights regarding protected health information. The notice must also include anticipated uses and disclosures of this information that may be made without the patient's written authorization.

Law Enforcement Officials

In certain circumstances health information may be disclosed to law enforcement officials without consent. For example, health information may be disclosed pursuant to a warrant, subpoena, or order issued by a judicial officer, pursuant to a grand jury subpoena, or pursuant to an administrative subpoena or summons, civil investigative demand or similar certification if a three-part test is met: 1) the information is relevant 2) the request is specific and 3) de-identified information cannot reasonably be used.

Research

Researchers may be provided protected information if the researchers' protocol has been reviewed and approved by in Institutional Review Board or a privacy board.

State Law and the Administrative Simplification Regulations

Under § 160.201 – 160.204 of the Privacy Rule, the circumstances under which state law may be preempted by the Rule are explained. Generally, if a standard, requirement or implementation of the regulation is "contrary" to a state law, the federal regulation preempts state law. "Contrary" is defined in the regulations to mean:

> *(1) A covered entity would find it impossible to comply with both the State and federal requirements; or*
> *(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.*

(The "Act" referred to in *(2)* above is the Social Security Act, and Pub. L 104-191 is HIPAA. Part C of the Social Security Act is where most of the Administrative Simplification law is found.)

There are exceptions to this general rule regarding the preemption of state law. The state must submit to the Secretary of Health and Human Services a request for a law to be excepted from

preemption, and the Secretary must generally evaluate the request based on whether the state law:

- is necessary to prevent fraud or abuse in the provision of or payment of health care,
- to ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery or costs, or
- to serve a compelling need related to public health, safety or welfare; or has the principal purpose of the regulation of the manufacture, registration, distribution, dispensing or other control of a controlled substance.

The Secretary may also find that the state law is "more stringent" than the Act requires, and therefore the state law will not be preempted. "More stringent is defined in the regulations as:
…a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

- *Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or*
- *To the individual who is the subject of the individually identifiable health information*

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that is authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually indentifiable health information about a use, a disclosure, rights and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

State law may also be excepted from preemption if the state's law, and related procedures as applicable, provide for the reporting of disease or injury, child abuse, birth, or death, or for conducting public health surveillance, investigation, or intervention. Another reason state law may be excepted from preemption is if the state law requires a health plan to report, or to provide access to, information for the purpose of management or financial audits, program monitoring and evaluation, or licensing or certification of facilities or individuals.

Complaints and Compliance Reviews

If an individual believes that a covered entity is not complying with the regulations of the Act, the individual may file a complaint with the Secretary. The complaint must be in writing, either on paper or electronically. The contents of the complaint must include the name of the entity that is believed to be in noncompliance and a description of the acts or omissions the entity has committed that are believed to be in violation. Complaints must generally be filed within 180 days of when the complainant knew, or should have known, that the act or omission was committed. Once a complaint is received, the Secretary may investigate, including reviewing pertinent policies, procedures or practices of the covered entity who is the subject of the complaint.

Besides investigating complaints, the Secretary may conduct compliance reviews of covered entities. The purpose of these reviews is to determine whether the entity is complying with the regulations.

If an entity is the subject of a complaint investigation or compliance review, the entity must:

- provide records and compliance reports to the Secretary,
- cooperate with complaint investigations and compliance reviews,
- permit access to information, including its facilities, books, records, accounts and other sources of information pertinent to the investigation or review.

Use and Disclosure

§ 164.500-534 of the Final Regulations address the Privacy of Individually Identifiable Health Information, based on Section 264 of HIPAA. These regulations also apply to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form as defined under the Act.

General Rules Regarding the Use and Disclosure of Protected Health Information

A covered entity may generally use or disclose protected health information in the following ways:

- to disclose or use protected health information to the individual;
- in accordance with the consent and authorization requirements found in the regulations; and
- if consent is not required, to carry out treatment, payment or health care operations.

The "Minimum Necessary" Standard

Generally, when a covered entity is using or disclosing protected health information, or is requesting protected health information from another covered entity, the covered entity must make reasonable efforts to limit the protected health information to the "minimum necessary" to accomplish the intended purpose for using, disclosing or requesting the information.

The minimum necessary rule does not apply to disclosures to a health care provider for treatment or requests by a health care provider for treatment. It also does not apply to disclosures to the individual, or disclosures made to the Secretary pertaining to a complaint against a covered entity. Disclosures required by law, such as when a public health authority

must collect information for the purpose of preventing or controlling disease, injury, and so on, are also not subject to the minimum necessary standard.

The Use and Disclosure of De-Identified Protected Health Information Standard – Business Associates

A covered entity may use protected health information to create information that is not individually identifiable health information. It may also disclose protected health information to a "business associate" for the purpose of creating de-identified health information. Under the regulations, a "business associate" is defined as a person who:

(1)(i) On behalf of such covered entity or of an organized health care arrangement…in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by [the regulations]; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation… management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph(1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Once information has been de-identified, it is considered to be protected health information if a code or other means of record identification is disclosed that causes the information to become individually identifiable.

Disclosure to Business Associates Standard

A covered entity may generally disclose health information to a business associate, and may allow a business associate to create or receive protected health information on the entity's behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. The "satisfactory assurance" must be in a written contract or agreement between the covered entity and the business associate.

Specifications of Business Associate Contracts

The contract between a covered entity and a business associate:

- must establish the permitted and required uses and disclosures of such information by the business associate
- may permit the business associate to use and disclose protected health information for the management and administration of the business associate, or to carry out legal responsibilities of the business associate
- may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity
- must provide that the business associate will not use or further disclose the information except as permitted or required by the contract or by law
- must provide that the business associate will use appropriate safeguards to ensure that protected information will not be used or disclosed other than as allowed by the contract
- must provide that the business associate will report to the covered entity any use or disclosure that is not allowed by the contract of which it becomes aware
- must provide that information provided to any of its agents, including subcontractors, is covered by the same restrictions and condition as those applying to the business associate
- must provide that the business associate will provide protected health information to the individual under the rules of the regulations
- must provide that any amendments allowable under the law be incorporated into protected health information by the business associate
- must provide the information necessary for the accounting of disclosures of protected health information by the business associate be done in accordance with the law
- must provide that the business associate make its internal practices, books and records relating to the use and disclosure of protected health information available to the Secretary for purposes of determining the covered entity's compliance with the regulations
- must provide that at the termination of the contract between the business associate and the covered entity that, if feasible, all protected health information be returned or destroyed, or if not feasible, provide for further protections and limitations on the use and disclosure of the information
- must provide that the covered entity will terminate the contract if the business associate has violated a material term of the contract

Deceased Individual Standard and Personal Representatives

In the case of protected information of a deceased individual, the personal representative, such as an executor or administrator of the deceased's estate, may be treated as the individual for the purposes of the Administrative Simplification regulations.

If an individual is authorized to act on behalf of an adult or an emancipated minor in making decisions about health care, such an individual may also be treated as a personal representative, i.e., as the individual, for the purposes of the regulations.

The final regulations also address the issue of parents, guardians or other person the issue of parents, guardian, or other person acting *in loco parentis* acting as a personal representative for an unemancipated minor. State laws differ regarding whether parents or guardians must be notified and/or given authorization in order for a minor to receive health care services. The final federal regulations recognize these differences by stating that if an unemancipated minor is able to legally consent to health care services without the consent of the parent or guardian, the parent or guardian may not act as personal representative and thereby receive protected health information about the minor. But, if the parent or guardian has authority to act on behalf of a minor and give or deny authorization for health care services, the covered entity must treat the parent or guardian as a personal representative and disclose applicable protected health

information about the minor to the parent or guardian, unless the parent, guardian, or other individual acting *in loco parentis* consents to an agreement of privacy regarding health information between the minor and the health care provider.

A covered entity has some room for discretion regarding the disclosure of information to a personal representative. If a covered entity has a "reasonable belief" that:

- an individual has been or may be subjected to domestic violence, abuse or neglect by a personal representative;
- that treating an individual as a personal representative could endanger the individual who is the subject of the health care or the protected information; or
- it is not in the best interest of the individual to treat the person as the individual's personal representative, based on the exercise of professional judgment by the covered entity, the covered entity may choose not to treat the person as the individual's personal representative.

Disclosures by Whistleblowers

A "whistleblower" is an employee or other member of the workforce of a covered entity, or a business associate who informs authorities of a real or apparent violation of the law or professional or clinical standards by the covered entity. A whistleblower may disclose what would otherwise be considered protected health information if the whistleblower believes in good faith that the covered entity has engaged in conduct that is unlawful, or otherwise violates professional or clinical standards, or that the care, service, or conditions provided by the covered entity potentially endangers patients, workers or the public. The whistleblower may disclose such information to a health oversight agency or public health authority authorized by law to investigate or oversee such allegations of misconduct, or may inform an attorney retained for the purpose of determining legal options for the whistleblower.

Disclosures By Workforce Members Who Are Victims Of A Crime

If a member of a covered entity's workforce is a victim of a crime, the member may disclose what would otherwise be protected health information to a law enforcement official, as long as the information disclosed is regarding the suspected perpetrator of the crime, and is limited to information used to identify a suspect, fugitive, material witness or missing person, including:

- name and address;
- date and place of birth;
- social security number;
- ABO blood type and RH factor;
- type of injury;
- date and time of treatment;
- date and time of death, if applicable; and
- a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

Requirements for Group Health Plans

Generally, in order for a group health plan to disclose protected health information to a plan sponsor, or to permit disclosure to a sponsor, the group health plan documents must restrict the use and disclosure of such information, in accordance with the law and regulations.

A group health plan, or a health insurance issuer, or an HMO may disclose summary health information to the plan sponsor if the sponsor requests the information for the purpose of obtaining premium bids from health plans, or for modifying, amending or terminating a group health plan.

"Summary health information" is defined in the final regulations to mean: *information, that may be individually identifiable health information; and*

> *(1)That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and*
> *(2) From which the information described at §164.514(b)(2)(i)* [see below] *has been deleted, except that the geographic information described in 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.*

The information described in §164.514(b)(2)(i), cited above, includes, generally:

- names
- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code [§164.514(b)(2)(i)(B)]
- all elements of dates directly related to an individual, e.g. birth date, admission date, discharge date, date of death, etc.
- telephone numbers
- fax numbers
- electronic mail addresses
- social security numbers
- medical record numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identifiers
- device identifiers and serial numbers
- URLs
- IP address numbers
- biometric identifiers, including finger and voice prints
- full face photographic images, and
- any other unique identifying number, characteristic or code

Plan Document Requirements

Plan documents of a group health plan must incorporate provisions:

- to establish the permitted and required uses and disclosures of the information by the plan sponsor, in accordance with the regulations
- that require that the plan sponsor agree to the following before protected health information will be disclosed by the group health plan:
  - the sponsor will not use or further disclose information other than as permitted or required by the plan, or as required by law

- the sponsor will ensure that any agents, including subcontractors, will abide by the same restrictions and conditions pertaining to protected health information as the sponsor
- the sponsor will not use or disclose protected information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan
- the sponsor will report to the group health plan any use or disclosure of the information of which it becomes aware that is not allowed by the plan
- the sponsor will make available information needed to investigate a complaint or is needed for a compliance review
- the sponsor will incorporate any amended protected health information in accordance with the regulations
- the sponsor will make information available that is needed in order for the accounting of disclosures as required under the law
- the sponsor will make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance with the regulations by the group health plan
- the sponsor will destroy or return protected health information that is no longer needed, if feasible, and if not feasible, to limit its further uses and disclosure

In addition, the group health plan must provide for "adequate separation" between the group health plan and the plan sponsor. To accomplish this "separation," according to the Privacy Rule, the plan documents must:

- describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, and any employee or person who receives protected health information relating to payments under, health care operations of, or other matters pertaining to the group health plan
- restrict access to and use by employees to the plan administration functions for which the sponsor is responsible
- provide an effective mechanism to deal with noncompliance under the regulations by the sponsor's employees or workforce members

Consent for Uses or Disclosures To Carry Out Treatment, Payment or Health Care Operations

Generally, a health care provider must obtain the individual's consent prior to using or disclosing protected health information to carry out treatment, payment or health care operations. If a health care provider has an "indirect treatment relationship" with an individual, the health care provider does not need to obtain consent before using or disclosing protected health information for these purposes. An indirect treatment relationship is defined under the regulations to mean:

a relationship between an individual and a health care provider in which:

> *(1) The health care provider delivers health care to the individual based on the order of another health care provider; and*
> *(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual."*

A health care provider with an indirect treatment relation acts based on the consent or authorization obtained by the provider with a direct treatment relationship with the individual.

A covered health care provider may also use or disclose protected health information without prior consent in emergency situations, if the provider attempts to obtain consent as soon as is reasonably possible. Also, if a covered health care provider is required by law to provide treatment to an individual and attempts to obtain consent but is unable to obtain the consent, the health care provider may use or disclose protected health information to carry out the treatment, payment or health care operations.

A covered health care provider may also use or disclose protected health information without consent in order to carry out treatment, payment or health care operations if the provider attempted to obtain the consent but is unable to obtain the consent, the health care provider may use or disclose protected health information to carry out the treatment, payment or health care operations. A covered health care provider may also use or disclose protected health information without consent in order to carry out treatment, payment or health care operations if the provider attempted to obtain the consent but is unable to due to substantial barriers to communicating with the individual, and the provider determines that the individual's consent to receive treatment is inferred from the circumstances.

In circumstances where a health care provider is unable to obtain consent, but follows the regulations pertaining to these circumstances and carries out treatment, payment or health care operations, the provider must keep documentation regarding attempts to obtain consent, and the reason or reasons that consent was not obtained.

A covered health care provider may require consent as a condition to provide treatment, or as a condition to enroll an individual in a health plan.

The consent for use and disclosure of protected health information may be combined with other types of legal permission from the individual as long as the consent is visually and organizationally separate from other written legal permission and is separately signed and dated by the individual. A covered entity must document and retain signed consents.

Revocation of Consent

An individual may revoke a consent for use and disclosure of protected health information at any time. The revocation must be in writing.

Consent Content Requirements

In order to comply with the final regulations, consents must:

- be in plain language
- inform the individual that protected health information may be used and disclosed to carry out treatment, payment or health care operations
- inform the individual that he or she is able to request a complete description of the privacy practices of the covered entity and that the individual has the right to receive the notice prior to signing the consent form
- inform the individual, if the covered entity has retained the right to change privacy practices, that the practices may change and that the individual may obtain a revised notice regarding privacy practices

- state that the individual has the right to request that the entity restrict how protected health information is used or disclosed, that the covered entity is not required to agree to requested restrictions, and if the entity does agree, that the restriction is binding on the covered entity
- state that the individual has the right to revoke the consent in writing
- require that the individual sign and date the consent

Authorizations

Authorizations differ from consents in that a consent gives health care providers with a direct treatment relationship with a patient, permission to use and disclose all protected health information for treatment, payment or health care operations, while authorizations give permission to covered entities to use specified protected health information for specific purposes, generally other than for treatment, payment or health care operations, and also may give permission for the entity to disclose protected health information to a third party. Authorizations are more specific than consent forms and include an expiration date.

Generally, authorizations must be obtained to disclose any information not covered under the consent rules, meaning most disclosures or uses other than use or disclosure of protected health information to carry out treatment, payment or health care operations by a health care provider with which the individual has a direct treatment relationship.

Psychotherapy Notes and Authorizations

Generally, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except for:

- use by the originator of the psychotherapy notes for treatment
- use or disclosure by the covered entity in training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve skills
- use for determining compliance, by the originator of the psychotherapy notes or to investigate a complaint
- use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual

Authorization Contents

A valid authorization must include:

- a description of the information to be used or disclosed
- the name or other specific identification of the person or class of persons authorized to use or disclose the information
- the name or other specific identification of the person or class of persons to whom the covered entity may make the requested use or disclosure
- an expiration date or expiration event after which the authorization is no longer valid
- a statement that the individual has the right to revoke the authorization
- a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and is no longer protected under the privacy regulations
- signature of the individual and date

Unlike consents, generally, a covered entity may not condition provision of treatment, payment, enrollment in a health plan or eligibility on providing an authorization, except under the circumstances listed below. An authorization may be required by an entity:

- for research-related treatment
- for use in determining the eligibility of an individual for a health plan or for determining underwriting or risk ratings, prior to the individual enrolling in the health plan
- if necessary for determining payment of a claim
- if the provision of health care is for the purpose of creating protected health information for disclosure to a third party

If an authorization is requested by a covered entity, in order for another covered entity to disclose protected health information to the requesting covered entity to carry out treatment, payment or health care operations, the requestor must include in an authorization form the normal elements of an authorization, as well as the following items:

- a description of each purpose of the requested disclosure
- a statement that, other than the allowable exceptions for requiring an authorization for treatment, payment or enrollment, the entity will not condition other services on the receipt of authorization, and
- a statement that the individual may refuse to sign the authorization

The covered entity must also provide the individual a copy of a signed authorization.

Authorization for Use and Disclosure of Protected Information for Research

Authorizations used to gain approval to use and disclose information for research must contain the information that an authorization normally requires, plus:

- a description of the extent to which the information will be used or disclosed to carry out treatment, payment or health care operations
- a description of any uses that go beyond those that do not require consent or authorization
- reference to any applicable consents from or privacy notices to the individual

Uses and Disclosures Not Requiring Authorization of Consent, But Requiring the Opportunity to Agree or Object

Certain uses and disclosures of protected health information are allowed without a formal consent or authorization, as long as the individual is informed in advance of the use or disclosure and has the opportunity to agree or object. The process of informing the individual and obtaining agreement or objection may be oral.

As long as an individual does not object, the following information may be used for a facility directory:

- the individual's name
- the individual's location in the facility
- the individual's condition described in a manner that does not give specific medical information
- the individual's religious affiliation

This information may be disclosed to members of the clergy. This information, except for religious affiliation, may also be disclosed to anyone who asks for the individual by name.

Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

Certain protected health information may be disclosed to a family member, other relative, a close personal friend of the individual, or other person identified by the individual. Information directly relevant to the person's involvement with the individual's care or payment related to the individual's health care, is allowed to be disclosed or used.

If the individual is present and able to make health care decisions, the covered entity must obtain the individual's agreement, give the individual the opportunity to object, or use professional judgment to determine that the individual does not object, before disclosing the information to the family member or other person. If the individual is not present, or is incapable of providing agreement, or when an emergency situation exists, the covered entity may use its professional judgment to determine whether the disclosure is in the best interests of the individual, and if so, disclose only the protected health information directly relevant to the person's involvement with the individual's health care. The covered entity may also allow the person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays and other similar forms of protected health information.

Use and Disclosure for Disaster Relief Purposes

A covered entity may use or disclose protected health information to a public or private entity that assists in disaster relief efforts for the purpose of coordinating with such entities any of the permitted uses and disclosures of health information.

Uses and Disclosures For Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required

Certain uses and disclosures of protected health information may be made without consent, authorization or giving the individual an opportunity to agree or object. These are uses and disclosures:

- required by law
- for public health activities for the purpose of preventing or controlling disease, injury or disability
- for a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect
- to a person required to report adverse events, product defects or problems, or biological product deviations to the Food and Drug Administration
- to a person required to track product by the Food and Drug Administration
- to enable product recalls, repairs, or replacements under the Food and Drug Administration
- to conduct post-marketing surveillance to comply with requirements or under the direction of the Food and Drug Administration
- to a person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is required by law to notify the person
- to an employer about an employee of a covered entity who is a member of the workforce of the employer or who provides health care to the individual at the request of the employer to

conduct an evaluation relating to surveillance of the workplace, or to evaluate whether the individual has a work-related illness or injury,

- to an employer about an employee if the protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medial surveillance
- to an employer about an employee if the employer needs the information to comply with workers compensation or other similar laws
- to an employer about an employee if the covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided or by posting the notice in a prominent place at the location where the health care is provided

Disclosures About Victims of Abuse, Neglect or Domestic Violence

A covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, authorized by law to receive reports of abuse, neglect or domestic violence:

- if the individual agrees to the disclosure
- if the disclosure is expressly required by statute or regulation the covered entity believes the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
- if the individual is unable to agree to the disclosure due to incapacity, and a law enforcement or other authorized public official represents that the protected health information is not intended to be used against the individual and that an immediate enforcement activity depends upon the disclosure and would be materially and adversely affected by waiting until the individual is able to agree to the disclosure

Generally, if a covered entity determines that a disclosure about an individual who is a victim of abuse will be made, the covered entity must inform the individual that a report has been made. However, if the covered entity believes informing the individual would place the individual at risk of serious harm, the covered entity is not required to inform the individual.

Uses and Disclosures for Health Oversight Activities

Protected health information may be disclosed to a health oversight agency for oversight activities authorized by law, such as audits, civil, administrative or criminal investigations, inspections, licensure or disciplinary actions, and criminal proceedings. Generally, the disclosures allowed under these rules must be for activities necessary for oversight of the health care system, government benefit programs for which health information is relevant to beneficiary eligibility, entities subject to government regulatory programs that require health information to determine compliance with program standards, or entities subject to civil rights laws that require health information to determine compliance.

Disclosures for Judicial and Administrative Proceedings

If a court or administrative tribunal orders a covered entity to disclose protected health information as expressed in the order or if a covered entity receives a subpoena, discover request, or other lawful process, it may disclose protected health information if the party seeking the information provides a written statement and supporting documentation that:

- it has made a good faith attempt to provide written notice to an individual
- the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal
- no unresolved objections against the disclosure or use were filed within the designated time frame

The covered entity may also disclose protected health information in this situation if the requestor secures a "qualified protective order." A qualified protective order is an order of a court or of an administrative tribunal that prohibits the parties from using or disclosing the protected health information other than for the purpose for which it was requested and requires the return or destruction of the protected health information at the end of the proceedings.

Disclosure for Law Enforcement Purposes

A covered entity may generally disclose protected health information as required by law including laws that require the reporting of certain types of wounds or other physical injuries. It may also disclose protected health information in compliance with a court order, warrant, subpoena or summons, or a grand jury subpoena.

As long as an administrative request, or similar process authorized by law asks for information that is relevant and material to a legitimate law enforcement inquiry, is specific and limited in scope to the purpose for which the information is sought, and de-identified information could not be utilized for the purpose, a covered entity may disclose protected health information pursuant to such a request.

In response to a request from a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, a covered entity may generally disclose:

- name and address
- date and place of birth
- social security number
- ABO blood type and RH factor
- type of injury
- date and time of treatment
- date and time of death, if applicable
- description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, facial hair, scars and tattoos

Permitted Disclosures Regarding Victims Of A Crime

If an individual is or suspected to be a victim of a crime, a covered entity may generally disclose protected health information if the individual agrees to the disclosure. Protected health information about such an individual may also be disclosed to a law enforcement official if agreement from the individual may not be obtained due to incapacity or emergency, as long as, based on representations by the law officer:

- the information is needed to determine whether a violation of law by a person other than the victim has occurred
- the information is not intended to be used against the victim

- the law enforcement activity would be materially and adversely affected by waiting for agreement from the individual
- the disclosure is in the best interests of the individual as determined by the professional judgment of the covered entity

If a covered entity suspects that an individual's death may have resulted from criminal conduct, it may disclose protected information to a law enforcement officer to alert them of the circumstances of the death. It also may disclose protected health information to a law enforcement officer if it believes in good faith that criminal conduct occurred on its premises.

If a covered health care provider is giving care in response to a medical emergency off the premises of the provider, it may disclose protected health information to a law enforcement officer that is necessary to alert the officer of the commission and nature of a crime, the location of or victims of the crime, or the identity, description and location of the perpetrator of the crime.

Uses and Disclosures About Decedents

A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other authorized duties under the law. It may also disclose information to funeral directors, as allowed by law, so that the funeral directors are able to carry out their duties.

A covered entity may also disclose protected information to an organ procurement organization or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes or tissues in order to facilitate transplantation.

Uses and Disclosures for Research Purposes

A covered entity may use or disclose protected health information for research as long as the entity has had an approved waiver of authorization as required under the law. This is discussed in greater deal in the final chapter of this course.

Uses and Disclosures to Avert A Serious Threat to Health or Safety

If a covered entity believes the use or disclosure of protected health information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, it may disclose it to a person reasonably able to prevent or lessen the threat. It may also disclose protected health information if it believes the information is necessary for law enforcement authorities to identify or apprehend an individual because the individual admitted participating in a violent crime that the covered entity believes may have caused serious harm to a victim, or if it appears that the individual escaped from a correctional institution or lawful custody. However, if the individual is under counseling or therapy treatment by the entity when the individual admitted participating in a crime, the entity may not generally disclose the information.

Standard Disclosures for Workers' Compensation

A covered entity may disclose protected health information as necessary to comply with laws relating to workers' compensation or similar programs.

Other Requirements Relating To Uses and Disclosures of Protected Health Information

A covered entity must identify the people or class of people in its workforce who need access to protected health information to carry out their duties. The category or categories of protected health information that needs to be accessed must also be documented for each identified person or class, as well as the conditions appropriate to such access. The covered entity must also make reasonable efforts to limit the access to protected health information by the persons or class of persons.

For any disclosure that is made routinely, the covered entity must implement policies and procedures to limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For other disclosures, the covered entity must abide by the following rules:

a) develop criteria designed to limit the protected health information to that necessary to accomplish the purpose for the disclosure – the minimum necessary
b) review each disclosure in light of the criteria established

Minimum Necessary Representations

In some cases, a covered entity may not have to ascertain on its own when a disclosure meets the "minimum necessary" standard. If a disclosure is made to public officials in accordance with the regulations and the public official reasonably represents that the requested information is the minimum necessary, the covered entity may rely on that representation. In addition, if a covered entity receives a disclosure request from another covered entity, meeting the minimum necessary standard is the responsibility of the requesting entity. And, if a professional who is a member of a covered entity's workforce or who provides professional services to the entity requests protected health information and reasonably represents that it is the minimum necessary, the entity may rely on the professional's representation.

A covered entity may not request, disclose or use an entire medical record, unless it is specifically justified as reasonably necessary to accomplish the purpose of the request, disclosure or use.

Uses and Disclosures of Protected Health Information for Marketing

A covered entity does not have to obtain authorization when it uses or discloses protected health information to make a marketing communication to an individual in a face-to-face encounter, or concerning products or services of nominal value. An authorization is not needed when a covered entity markets health-related products and services of the covered entity or of a third party through a communication and the communication:

- identifies the covered entity making the communication
- discloses prominently that the entity has received or will receive remuneration, if applicable
- contains instructions describing how the individual may opt out of receiving future communications, unless the communication is a general communication device, such as a newsletter, that is distributed to a broad cross-section of patients, enrollees, or other group

The entity must also make a reasonable effort to ensure that those who decide to opt out of receiving future communications are not sent communications.

Target Marketing

If a covered entity uses protected health information to target a communication to individuals based on their health status or condition, the covered entity must make a determination prior to communicating about a product or service marketed to the target market that the product or service may be beneficial to the health of those in the target group. The communication must also explain why the individual was targeted and how the product or service relates to the health of the individual.

Verification Requirements

Prior to any disclosure of protected health information, the covered entity must verify the identity of a person requesting protected health information and the authority of the person to have access to protected health information, unless the identity is already known to the entity. The covered entity must also obtain any documentation, statements or representations, whether oral or written, from the requestor, when required under the regulations.

Notice of Privacy Practices For Protected Health Information

An individual enrolled in a group health plan has a right to a notice of privacy practices from the entity that directly provides health benefits, whether a group health plan, a health insurance issuer or HMO. If a group health plan provides benefits through a contract with a health insurer or HMO, creates or receives protected health information and summary health information or information regarding whether the individual is participating in the group health plan, or who has enrolled or disenrolled, must maintain a privacy plan notice and provide it upon request to anyone who requests it.

Notice Contents

The privacy notice must be written in plain language. It must include the following statement as a header or otherwise prominently displayed:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The notice must also contain:

- a description of the types of uses and disclosures that the entity is permitted to make for treatment, payment and health care operations, including at least one example for each purpose
- a description of each of the other purposes the entity is permitted to use or disclose without the individual's written consent or authorization
- a statement that other uses and disclosures will only be made with the individual's written authorization, and that the individual may revoke such an authorization
- if applicable, a statement that the entity may contact the individual with appointment reminders, treatment alternatives or other health-related benefits and services

- if applicable, a statement that the entity may contact the individual to raise funds for the covered entity
- if applicable, a statement that a group health plan, or a health insurer or an HMO may disclose protected health information to the plan sponsor
- a statement of the individual's right to request restrictions on certain uses and disclosures of protected heath information, that the entity is not required to agree to a requested restriction, and a brief description of how the individual may exercise this right
- a statement of the individual's right to receive confidential communications at other locations or by alternate means, as authorized under the regulations, and a brief description of how the individual may exercise this right
- a statement of the individual's right to inspect and copy protected health information, and a brief description of how the individual may exercise this right
- a statement of the individual's right to amend protected health information, and a brief description of how the individual may exercise this right
- a statement of the individual's right to receive an accounting of disclosures of protected health information, and a brief description of how to exercise this right
- a statement of the individual's right to obtain a paper copy of the notice upon request to the covered entity, and a brief description of how to exercise this right
- a statement that the covered entity is required by law to maintain the privacy of protected health information and to provide notice to individuals of the entity's duties and privacy practices under the law regarding protected health information
- a statement that the covered entity is required to abide by the terms of the notice currently in effect
- if applicable, a statement that the entity reserves the right to change the terms of the notice and to make new privacy provisions effective for all the protected health information it maintains, and a description of how individuals will be provided with any such new notice
- a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a description of how the individual may file a complaint, and a statement that the individual will not be retaliated against for filing a complaint
- the name, title or telephone number of the person or office to contact regarding complaints
- the effective date of the notice, not earlier than the date it is published

Provision of Notice

Health plans must provide notice no later than the compliance date, which is thirty-six months after the final rule is published in the Federal Register for small health plans, and twenty-four months after it is published for other health plans, to all individuals covered by the plan. Thereafter, health plans must provide notice at time of enrollment to new enrollees and within sixty days of material revision to individual covered by the plan. In addition, at least once every three years the health plan must notify individuals covered by the plan of the availability of the notice and how to obtain the notice.

A covered health care provider that has a direct treatment relationship with an individual must provide notice no later than the date of the first service delivery after the compliance date for the covered health provider, which is twenty-four months after the final rule is published in the Federal Register. If the provider has a physical service location, the notice must be available at the location for individuals to request to take with them and the notice must be posted in a clear and prominent location where it may be reasonably expected that individuals seeking service will be able to read it.

If a covered entity maintains a web site that provides information about the entity's customer services or benefits, it must post the notice on the web site and make the notice available electronically through the web site.

Notice may be provided via e-mail if the individual agrees to receive it in this manner. If the entity knows that an e-mail transmission has failed, it must provide a paper notice to the individual. If the first service to an individual is made electronically, the notice must be made automatically and contemporaneously at that time to the individual. Individuals who receive notices electronically must have the right to receive notices by paper as well.

Notice Revisions

If a notice is materially revised, the covered entity must promptly revise and distribute the revised notice to the individuals to whom it must make notice.

Right of Individuals to Request Restrictions of Use and Disclosures

An individual has the right to request that the covered entity restrict, beyond the normal privacy practices found in the notice, the uses or disclosures of protected health information regarding:

- the carrying out of treatment, payment or health care operations, and
- allowable disclosures to family members and others for the purpose of facilitating the carrying out of the individual's health care, treatment or payment operations.

The covered entity is not required to agree to a restriction.

If a covered entity agrees to such a restriction, it may not violate it while it is in effect, other than for emergency situations. If, in an emergency situation, the covered entity must disclose protected health information to a health care provider, the covered entity must request that the provider not further disclose or use the protected health information.

Restrictions may not apply to disclosures:

- to the individual
- as required under law, such as to investigate a complaint
- for legal use in a facility directory
- for public health activities as authorized under the regulations
- regarding victims of abuse, neglect or domestic violence as authorized under the regulations
- for authorized use by a health oversight agency
- for authorized use for judicial and administrative proceedings
- for law enforcement purposes, as authorized under the regulations
- for research purposes, in accordance with the regulations
- to avert a serious threat to health or safety
- for specialized government functions, as defined in the regulations
- for compliance with workers' compensation and similar laws

A restriction may be terminated by the individual in writing or by the individual orally, if the oral agreement is documented. The covered entity may also terminate a restriction by informing the individual in writing.

Confidential Communication Requirements

A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health care provider by alternate means or alternative locations. A health care provider may not require an explanation from the individual as to the reason for the request as a condition of providing communications on a confidential basis.

On the other hand, a covered health plan may require that a request to receive communications at an alternate location or by alternate means contain a statement that disclosure of all or part of the information could endanger the individual.

Access To Protected Health Information By Individuals

Individuals have the right to receive protected health information about themselves, except:

- psychotherapy notes
- information gathered in anticipation of or for use in a civil, criminal or administrative action or proceeding
- protected health information subject to the Clinical Laboratory Improvements Amendment, so that access to the individual is prohibited by law
- inmates, if obtaining the information would jeopardize the health, safety, security or rehabilitation of the individual or of other inmates, or the safety of an officer, employee or other person in the correctional institution
- information obtained in the course of research, when the individual has consented to participate in research that includes treatment and has been informed that the right of access will be reinstated upon the completion of research
- certain records held by government agencies and protected under the Privacy Act, 5 USC §552a
- if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information

Besides these circumstances defined under the regulations as reasons for denial of access by the individual, there are other circumstances under which a covered entity may deny an individual access to protected health information. These include when:

- a licensed health care professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person
- the protected health information makes reference to another person and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to that person
- the requestor is a personal representative of the individual and the licensed health care professional determines that access is reasonably likely to cause substantial harm to the individual or another person.

If the covered entity denies access for one of these reasons, it must allow the individual the right to review the denial of access. The review is conducted by a licensed health care professional designated by the covered entity as a reviewing official and who did not participate in the original decision to deny.

Providing Access

If a covered entity provides the individual access to the requested information, it must provide a copy, or allow an inspection, or both. It must provide the information in the form or format requested, if it is readily producible in that format. If the information may not be readily produced in the format requested, the entity must supply it in a readable hard copy format, or other format agreed to by both the entity and the individual.

Summary information or an explanation may be provided in response to a request for access, as long as the individual agrees in advance to the summary or explanation. If any fees are involved, the individual must agree in advance to the fees.

The covered entity must respond to a request for access within thirty days of receipt of the request. It must also arrange for a convenient time and place for the individual to inspect the records, if applicable.

Any fee for providing access may include only the cost of:

- copying, including cost of supplies and labor
- postage, if the information is to be mailed at the request of the individual
- preparing an explanation or summary of protected health information , if applicable

If a covered entity denies access to all or part of the requested information, the covered entity must:

- make other requested information accessible, if possible
- provide a written denial within thirty days after receipt of the request that includes:
- the basis for the denial
- if applicable, a statement that the individual may request a review of the denial
- a description of how the individual may complain to the covered entity or the Secretary, and a description of the name or title, and telephone number of the contact person with which to lodge a complaint

If the covered entity does not keep the protected health information that is the subject of the individual's request, but knows where it is maintained, the covered entity must inform the individual where to direct the request for access.

A covered entity must document the designated record sets that are subject to access by individuals, and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Amendment of Protected Health Information

An individual has the right to have a covered entity amend protected health information or a record in a designated record set. The covered entity must allow an individual to request amendment. It may require that the request be made in writing and that the individual provide a reason to support the request, as long as the individual was notified in advance of these requirements.

Requests for amendments must be acted upon within sixty days after receipt of the request. If the entity accepts the amendment, it must, at a minimum, identify the records in the designated record set that are affected by the amendment and append them or provide a link to the location of the amendment. It must also inform the individual that the amendment is accepted and obtain the individual's agreement to inform persons that the covered entity knows have the protected health information and that may have relied on, or could rely on, the information to the detriment of the individual. Future disclosures must include the appended material, or an accurate summary of the information.

If the covered entity denies the amendment, it must provide a written denial that:

- provides the reason for the denial, the individual's right to submit a written statement in disagreement with the denial, and the process for filing such a statement
- states that if the individual does not file a statement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the applicable protected health information
- provides a description of the process for the individual to complain to the entity or the Secretary, and provide the name or title and telephone number of the contact person or office to be contacted for complaint purposes.

If the individual submits a written statement of disagreement, the covered entity may prepare a written rebuttal to it. If a rebuttal is prepared, it must provide a copy to the individual who submitted the statement of disagreement. When applicable, the covered entity must link the affected records with the individual's request for amendment, denial of the request, statement of disagreement and rebuttal statement.

If a covered entity is notified by another covered entity of an amendment to the protected health information, the covered entity must amend its records accordingly.

Accounting of Disclosures of Protected Health Information

An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date the accounting is requested. The accounting may generally exclude disclosures:

- to carry out treatment, payment and health care operations
- to individuals of disclosures made to them
- for a facility directory or to a person involved in the individual's care
- for national security or intelligence purposes
- to correctional institutions or law enforcement officials

The accounting must include, for each disclosure:

- the date of the disclosure
- the name of the entity or person who received the protected health information and, if known, their address
- a brief description of protected health information disclosed
- a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's written authorization, or a copy of the written request for disclosure

If a covered entity is unable to provide the accounting within sixty days of the receipt of the request, it may extend the time period by up to thirty days if the entity notifies the individual in writing of the reasons for the delay, along with the date the accounting will be provided.

The first accounting requested in a twelve-month period must be done at no charge. A reasonable, cost-based fee may be charged for subsequent requests in the same twelve-month period by the same individual. The individual must be notified of the fee and given the opportunity to withdraw or modify the request subject to the fee.

Standard Training

A covered entity must train all members of its workforce on the policies and procedures regarding protected health information, as necessary for the members of the workforce to carry out their function. The training must be provided by no later than the covered entity's compliance date. New members of the workplace must be trained within a reasonable period of time after joining the workforce. If a member of the workforce has a job or function change that affects his or her responsibilities regarding protected health information, training must occur as soon as is reasonably possible.

Safeguards

A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. It must be protected from intentional or unintentional use or disclosure that is in violation of standards, implementation specifications or regulations.

Compliance

A covered entity must provide a process for individuals to make complaints about the covered entity's policies and procedures. It must also document all complaints received, along with their disposition, if any.

Sanctions

The covered entity must create and apply appropriate sanctions against members of its workforce who do not comply with its privacy policies and procedures developed in accordance with the regulations. Sanctions that are applied under this rule must be documented.

Retaliation

A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of any right under the regulations, including filing a complaint, testifying in an investigation, or opposing any act or practice that is unlawful under the regulations or exercising any other rights.

Changes of Privacy Practices and Notices

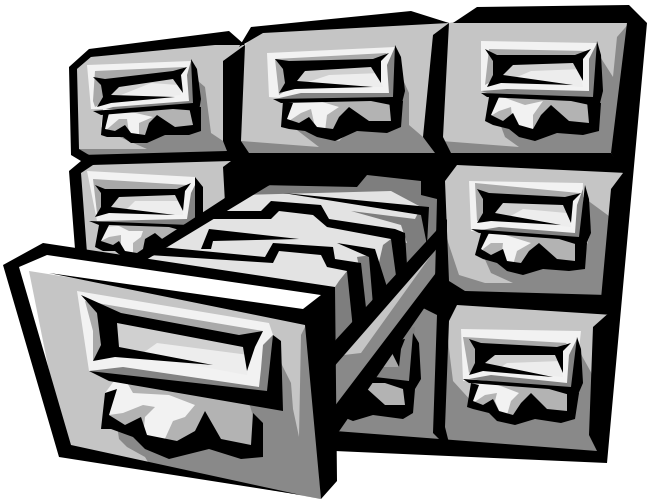
If a covered entity has included in the privacy practices notice the right to make changes to its privacy practices, it may make lawful changes. If material changes are made, the entity must revise the notice and make it available to those individuals it affects.

Federal Privacy Regulation

Congress has passed many laws that regulate privacy. In this chapter, various federal laws that interact with the Privacy Rule and others that address protection of an individual's privacy will be summarized.

The Privacy Act

The Privacy Act of 1974, found in 5 U.S.C. 552a, regulates the disclosure of records contained in a system of records maintained by a federal agency. The Act generally prohibits the disclosure of such records without the written request or consent of the individual. The exceptions to the requirement of request or consent include permitting agencies to disclose information if the disclosure qualifies as a "routine use" under the Act, and the use is published in the Federal Register.



The Act applies to all federal agencies and certain federal contractors who operate systems of records subject to the Privacy Act on the behalf of federal agencies. Some of the agencies and contractors covered by the Privacy Act are also covered by the Privacy Rule. Such agencies and contractors must comply with all applicable federal statutes and legislation, whether found in the Privacy Act, the Privacy Rule or elsewhere.

The Freedom of Information Act

The Freedom of Information Act, found in 5 U.S.C. 552, regulates the public disclosure of many types of information in the possession of the federal government. It allows public disclosure of this information, upon the request of any person, subject to nine exemptions and three exclusions. Personnel, medical and similar files may be withheld from disclosure, for example, if the disclosure would constitute a clearly unwarranted invasion of personal privacy.

Disclosures allowed under the Freedom of Information Act are referred to in §164.512(a) of the Privacy Rule which permits uses or disclosures required by law if the disclosures meet the relevant requirements of the law. However, the federal agency must generally use the exemption for personnel, medical and similar files to prohibit the disclosure, if the disclosure would violate the Privacy Rule. The federal agencies must evaluate requests for disclosure on a case-by-case basis to determine whether a disclosure would violate the Privacy Rule.

Federal Substance Abuse Confidentiality Requirements

The Federal Confidentiality of Substance Abuse Patient Records Statute, Section 543 of The Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2, regulate confidentiality requirements for patient records that are maintained in connection with the performance of any federally-assisted specialized alcohol or drug abuse program. Health care providers may be subject to the Substance Abuse Statute and the Privacy Rule. These

providers should not find that these two sets of laws are in conflict with one another, but may both be complied with.

The Substance Abuse Statute and related laws do not allow disclosure, without patient authorization, disclosures for law enforcement, judicial and administrative proceeds, public health, health oversight, directory assistance, and other purposes allowed under the Privacy Rule. However, since the Privacy Rule does not mandate that disclosure be made for these purposes, the health provider is able to deny such disclosures when the health care provider would be in violation of the Substance Abuse Statutes.

The Privacy Rule requires that, generally, an individual must be given access to his or her own health information. The Substance Abuse Statutes allow this information to be disclosed, so an entity covered by both rules is able to disclose such information, and be in compliance with both sets of laws. The Substance Abuse Statues also allow for disclosures in case of medical emergencies, to the Food and Drug Administration, for research, for audit and evaluation activities and in response to certain court orders. Under the Privacy Rule, such disclosures are required. Therefore, entities subject to both sets of laws and that must allow such disclosures under the Privacy Rule are still in compliance with the Substance Abuse Statutes.

The Substance Abuse Regulations require notice to patients of the substance abuse confidentiality requirements and provides for written consent for disclosure. The Privacy Rule also requires notice and, generally, consent. An entity subject to both sets of laws may create notices and consent forms that meet the provisions of them both.

Employee Retirement Income Security Act of 1974

The Employee Retirement Income Security Act of 1974, commonly known as ERISA, regulates pension and welfare employee benefit plans established by private employers, unions, or both, to provide benefits to their workers and dependents. ERISA defines “employee welfare benefit plans” as those that provide “through the purchase of insurance or otherwise…medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, or death.” In 1996, the Health Insurance Portability And Accountability Act (HIPAA) amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurers. ERISA plans are generally covered under the HIPAA regulations for “health plans.”

Under ERISA, §514(a), found in 29 U.S.C. 114(a), state laws relating to employee benefit plans are preempted by ERISA, unless the state laws are stricter than those found under ERISA, other than state laws that regulate insurance. In addition, ERISA plans are not deemed to be an insurer for the purpose of regulating such plans under state insurance laws.

The Family Educational Rights and Privacy Act

Another federal law that involves privacy is the Family Educational Rights and Privacy Act, or FERPA, found in 20 U.S.C. 1232g. FERPA provides parents of students and students who are 18 or older (known under the Act as “eligible students”) with privacy protection for records of students maintained by federally funded educational agencies or institutions or agencies acting for these educational agencies. The education records covered by FERPA are exempted from the definition of “protected health information.” For example, health information of individual students under the age of 18 created by a nurse in a public school and that is subject to FERPA

is an "education record," not "protected health information." FERPA address how education records should be protected.

Another exclusion under the definition of "protected health information" within the FERPA regulation are records (1) of students who are 18 years or older or are attending post-secondary educational institutions, (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity, (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student. Any use of these records under FERPA other than by persons providing treatment to students turns them into "education records," and makes them subject to FERPA protections. However, if a school does not receive federal funds, it is not regulated by FERPA, so its records may be "protected health information."

Federally Funded Health Programs

Federally funded health programs include programs such as health programs for military personnel and veterans, and programs such as Medicare and Medicaid. Under HIPAA, "health plans" include the following federally conducted, regulated or funded programs:

- Group plans under ERISA that either have 50 or more participants or are administered by an entity other than the employer who established and maintains the plan;
- federally qualified health maintenance organizations;
- Medicare;
- Medicaid;
- Medicare supplemental policies;
- the health care program for active military personnel;
- the health care program for veterans;
- the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS);
- the Indian health service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.;
- and the Federal Employees Health Benefits Program.

Besides these programs specifically listed under HIPAA, there are other federally conducted, regulated or funded programs that do not come within the statutory definition of "health plan," but the statute may nonetheless apply when the federal entity or federally regulated or funded entity provides health services. In such a circumstance the entity qualifies as a "health care provider," and is therefore subject to the Privacy Rule.

Food, Drug, and Cosmetic Act

The Food, Drug, and Cosmetic Act, found in 21 U.S.C. 301, et seq., provides the responsibilities of the Food and Drug Administration with regard to monitoring the safety and effectiveness of drugs and devices. The agency's responsibilities include obtaining reports about adverse events, tracking medical devices, and engaging in other post marketing surveillance. These reports often contain protected health information, and the health information may be regulated by the Privacy Rule.

The Privacy Rule specifically allows covered entities to disclose protected health information to a person subject to the jurisdiction of the Food and Drug Administration for specified purposes.

These specified purposes may include reporting adverse events, tracking medical devices, or engaging in other post marketing surveillance.

Clinical Laboratory Improvement Amendments

The Clinical Laboratory Improvement Amendments, or CLIA, found in 42 U.S.C. 263a, and its accompanying regulations, found in 42 CFR part 493, regulates clinical laboratories and the standards regarding the testing of human specimens. Under this law, clinical laboratories are required to disclose test results or reports to authorized persons only, as defined by state law. An authorized person under the federal law is defined as the person who orders the test. Individual states may have different definitions of who qualifies an "authorized person."

The person ordering the test may be a health care provider, rather than the individual who is the subject of the protected health information. This means that the law may prohibit a clinical laboratory from providing the individual who is the subject of the test or report with access to their protected health information. The Privacy Rule, therefore does not require covered entities maintaining protected health information subject to CLIA to provide individuals with a right of access or a right to inspect and obtain a copy of this information if this right would be prohibited by CLIA. However, if the state with authority over the covered entity uses a different definition of "authorized person" as it applies to CLIA, and includes the individual in this definition, the Privacy Rule does not exempt such a covered entity from the requirement to provide individuals with right of access or a right to inspect and obtain a copy of this information.

Other Mandatory Federal or State Laws

The Privacy Rule exempts certain types of disclosures and uses from the normal authorization requirements. The Privacy Rule permits covered entities to make disclosures required by law, and many federal laws require covered entities to provide specific information to specific entities in specific circumstances.

The Social Security Act, including Medicare and Medicaid provisions, the Family and Medical Leave Act, the Public Health Service Act, Department of Transportation regulations, the Environmental Protection Act and its accompanying regulations, the National Labor Relations Act, the Federal Aviation Administration, and the Federal Highway Administration rules, may contain provisions that require covered entities or others to use or disclose protected health information for specific purposes.

A covered entity must determine whether a disclosure is required under a federal law that applies to the disclosure if the disclosure is normally prohibited under the Privacy Rule. If the disclosure is mandatory, the entity may disclose the information under the Privacy Rule, §164.512(a). If the disclosure is permitted by the applicable federal laws, but not mandatory, then the covered entity must determine if the disclosure falls under one of the permissible disclosures under the Privacy Rule. If the disclosure is not permissible without an authorization, the covered entity must obtain an authorization from the individual, or must de-identify the information before it may be disclosed.

If a federal law other than the Privacy Rule prohibits a covered entity from using or disclosing information, but the Privacy Rule allows the use or disclosure, the covered entity must comply with the other federal law and not use or disclose the information.

Federal Disability Nondiscrimination Laws

The two primary federal disability nondiscrimination laws are the Americans with Disabilities Act, or ADA, 42 U.S.C. 12101 et seq., and the Rehabilitation Act of 1973, 29 U.S.C. 701 et seq. Other federal laws also prohibit discrimination on the basis of disability, and these federal laws include privacy protection provisions.

Section 2 of ADA explains the reasons behind this Act.

SEC. 2. FINDINGS AND PURPOSES. 42USC 12101.
(a) Findings. The Congress finds that

(1) some 43,000,000 Americans have one or more physical or mental disabilities, and this number is increasing as the population as a whole is growing older;
(2) historically, society has tended to isolate and segregate individuals with disabilities, and, despite some improvements, such forms of discrimination against individuals with disabilities continue to be a serious and pervasive social problem;
(3) discrimination against individuals with disabilities persists in such critical areas as employment, housing, public accommodations, education, transportation, communication, recreation, institutionalization, health services, voting, and access to public services;
(4) unlike individuals who have experienced discrimination on the basis of race, color, sex, national origin, religion, or age, individuals who have experienced discrimination on the basis of disability have often had no legal recourse to redress such discrimination;
(5) individuals with disabilities continually encounter various forms of discrimination, including outright intentional exclusion, the discriminatory effects of architectural, transportation, and communication barriers, overprotective rules and policies, failure to make modifications to existing facilities and practices, exclusionary qualification standards and criteria, segregation, and relegation to lesser services, programs, activities, benefits, jobs, or other opportunities;
(6) census data, national polls, and other studies have documented that people with disabilities, as a group, occupy an inferior status in our society, and are severely disadvantaged socially, vocationally, economically, and educationally;
(7) individuals with disabilities are a discrete and insular minority who have been faced with restrictions and limitations, subjected to a history of purposeful unequal treatment, and relegated to a position of political powerlessness in our society, based on characteristics that are beyond the control of such individuals and resulting from stereotypic assumptions not truly indicative of the individual ability of such individuals to participate in, and contribute to, society;
(8) the Nations proper goals regarding individuals with disabilities are to assure equality of opportunity, full participation, independent living, and economic self- sufficiency for such individuals; and
(9) the continuing existence of unfair and unnecessary discrimination and prejudice denies people with disabilities the opportunity to compete on an equal basis and to pursue those opportunities for which our free society is justifiably famous, and costs the United States billions of dollars in unnecessary expenses resulting from dependency and nonproductivity.

(b) Purpose. It is the purpose of this Act

(1) to provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities;
(2) to provide clear, strong, consistent, enforceable standards addressing discrimination against individuals with disabilities;
(3) to ensure that the Federal Government plays a central role in enforcing the standards established in this Act on behalf of individuals with disabilities; and

(4) to invoke the sweep of congressional authority, including the power to enforce the fourteenth amendment and to regulate commerce, in order to address the major areas of discrimination faced day- to- day by people with disabilities.

Section 3 of the Act defines disability as:

- *a physical or mental impairment that substantially limits one or more of the major life activities of such individual;*
- *a record of such an impairment; or*
- *being regarded as having such an impairment.*

Section 501 of the Americans With Disabilities Act addresses insurance and disability:

(*c) Insurance. Titles I through IV of this Act shall not be construed to prohibit or restrict*

(1) an insurer, hospital or medical service company, health maintenance organization, or any agent, or entity that administers benefit plans, or similar organizations from underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or
(2) a person or organization covered by this Act from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that are based on underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or
(3) a person or organization covered by this Act from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that is not subject to State laws that regulate insurance.

Federal disability nondiscrimination laws such as ADA cover two categories of entities that may also be affected by the Privacy Rule: employers and entities receiving federal financial assistance.

Employers are not covered entities under the Privacy Rule. They are, however, subject to federal disability nondiscrimination laws and are required to protect the confidentiality of all medical information concerning their applicants and employees. ADA expressly covers employers of 15 or more employees, employment agencies, labor organizations, and joint labor-management committees under its employment provisions. The confidentiality obligations of such employers include treating applicant and employee medical information as confidential medical records. Transmission of health information by an employer to a covered entity, such as a group health plan, is subject to ADA confidentiality restrictions. ADA has been interpreted to permit an employer to use medical information for insurance purposes and "is not intended to disrupt the current regulatory structure for self-insured employers…or current industry practices in sales, underwriting, pricing, administrative and other services, claims and similar insurance related activities based on classification of risks as regulated by the states" [from the ADA Enforcement Guidelines]. Transmission of health information to a covered entity by an employer falls under "use of medical information for insurance purposes." Disclosure of medical information by the group health plan may also be considered use of information for insurance purposes.

Entities that receive federal financial assistance and may also be covered entities under the Privacy Rule are subject to §504 of the Rehabilitation Act (29 U.S.C. 794). Each federal agency promulgates regulations that apply to entities that receive financial assistance from that agency.

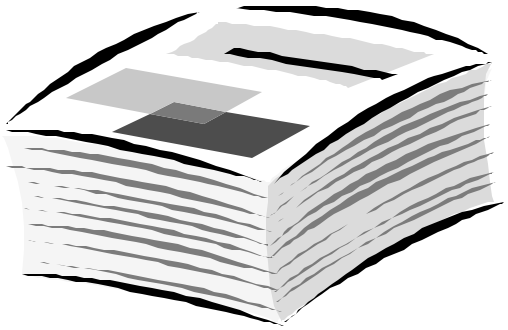
These regulations may include privacy protection provisions that limit the disclosure of medical information about persons who apply to or participate in a federal financially assisted program or activity. For example, the Department of Labor's Section 504 regulation requires entities that receive funds that conduct employment-related programs to maintain confidentiality regarding any information about the medical condition or history of applicants to or participants in the program or activity. The information is required to be kept separate from other information about the applicant or participant and may only be provided to certain specified individuals under certain limited circumstances.

Recipients of federal financial assistance from the Department of Health and Human Services, such as hospitals, are also subject to the ADA's employment nondiscrimination standards. Therefore, they must maintain confidentiality regarding the medical condition or history of both applicants and employees.

Final Regulation Guidelines

Standards For Privacy Of Individually Identifiable Health Information

A Guidance was issued July 6, 2001, promulgated by the Department of Health and Human Services, to provide direction for the implementation of the "Standards for Privacy of Individually Identifiable Health Information," commonly known as the "Privacy Rule."



In response to the question " What does this regulation do?" the Guidance states that the Privacy Rule became effective on April 4, 2001 and that the Privacy Rule creates for the first time national standards to protect individuals' medical records and other personal health information. The Guidance summarizes the Privacy Rule as follows:

- *It gives patients more control over their health information.*
- *It sets the boundaries on the use and release of health records.*
- *It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.*
- *It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients ' privacy rights.*
- *And it strikes a balance when public responsibility requires disclosure of some forms of data- for example, to protect public health.*

The Guidance also includes a summary of how the rule affects patients. It states that the rule enables patients to find out how their personal health information may be used and what disclosures of their information have been made, that it limits release of information about the patient to the minimum reasonably needed for the purpose of the disclosure, and gives patients the right to examine and obtain a copy of their own health records as well as to request corrections.

In the Guidance, the reasons the regulation is needed are also addressed. The Guidance indicates that Congress mandated the establishment of standards for the privacy of individually

identifiable information when it enacted the Health Insurance Portability And Accountability Act of 1996. Congress acted because prior to HIPAA and the establishment of these standards, personal health information was regulated by a variety of federal and state laws. Under these laws it was possible for personal health information to be distributed for reasons that have nothing to do with a patient's medical treatment or health care reimbursement. For example, the Guidance notes that prior to the enactment of this Rule, patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card, or to an employer who may use it in making personnel decisions.

The next question addressed in the Guidance is, "What does this regulation require the average provider or health plan to do?" the Guidance names five activities that are required under the rule. These are:

- Providing information to patients about their privacy rights and how their information can be used
- Adopting clear privacy procedures for its practice, hospital, or plan
- Training employees so that they understand the privacy procedures
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them

The Guidance points out that providers and plans differ in size and need and therefore the Privacy Rule gives flexibility to providers and plans to create their own privacy procedures.

In response to the question "Who must comply with these new privacy standards?" the Guidance states that the Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. These entities are called "covered entities" in the Guidance, as they are in the Privacy Rule

The next question answered in the Guidance is "When will covered entities have to meet these standards?" The Guidance states that most covered entities have two full years from the date that the regulation took effect to come into compliance and small health plans have three full years to come into compliance.

The Guidance then addresses the question "Do you expect to make any changes to this rule before the compliance date?" The Guidance suggests that it will issue proposed modifications to correct any unintended negative the facts of the Privacy Rules on health care quality or on access to such care.

The next question in the Guidance asks, "What changes might you be making in the final rule?" The Guidance lists four examples of standards for which it will propose changes. These are:

- *Phoned-In Prescriptions – A change will permit pharmacists to fill prescriptions phoned in by patient's doctor before obtaining the patient's written consent.*
- *Referral Appointments – A change will permit direct treatment providers receiving a first time patient referral to schedule appointments, surgery, or other procedures before obtaining the patient's signed consent.*
- *Allowable Communications – A change will increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high*

quality health care, including routine oral communications with family members, treatment discussions with staff involved in coordination of patient care, and using patient names to locate them in waiting areas.

- *Minimum Necessary Scope – A change will increase covered entities' confidence that certain common practices, such as use of sign-up sheets and X-ray light boards, and maintenance of patients' medical charts at bedside, are not prohibited under the rule.*

The Guidance also states that the Department of Health and Human Services (HHS) may reevaluate the Privacy Rule to make sure that parents have appropriate access to information about the health and well being of their children.

The final question in the introductory section of the Guidance asks "How will you make any changes?" The Guidance states that any changes must be made in accordance with the administrative procedures Act. HHS will publish its rule changes in the Federal Register through a notice of proposed rulemaking and will invite comment from the public after these comments are reviewed and addressed, HHS will issue a final rule that will implement the appropriate modifications. The Guidance also points out that Congress specifically authorized HHS to make modifications as appropriate in the first year after the final rule's impact is known in order to insure the Privacy Rule could be properly implemented.

Consent

45 CFR § 164.506

Background

According to the Guidance, the basis for the Consent rules is that health care providers routinely obtain a patient's consent for disclosure of information to insurance companies or for other purposes. The Privacy Rule establishes a uniform standard regarding obtaining consent for use and disclosure of a patient's health information to carry out treatment, payment or health operations.

As noted in the Guidance, general provisions of the Consent rules include:

- The requirement of patient consent before a covered health provider with a direct treatment relationship with a patient may use or disclose protected health information for purposes of treatment, payment or health care operations.
- Permitting certain uses and disclosures for treatment, payment or health care operations such as in an emergency, when a provider is required by law to treat the individual, or when there are substantial communication barriers.
- Permitting the use and disclosure of protected health information for purposes of treatment, payment, or health care operations by health care providers, health plans, and health care clearinghouses with an indirect treatment relationship without obtaining a patient's consent.
- Allowing the health care provider to refuse to treat a patient if the patient refuses to consent to the use or disclosure of their protected health information to carry out treatment, payment, or health care operations.
- Requiring that written consent need only be obtained by a provider one time.
- Using a consent document that is brief and written in general terms. The consent document must be written in plain language, inform the individual that information may be used and disclosed for treatment, payment, or health care operations, and must state the patient's

rights to review the provider's privacy notice, to request restrictions and to revoke consent, and must be dated and signed by the individual or his or her representative.

Individual rights found in the Consent Rules include the following:

- An individual may revoke consent in writing.
- An individual may request restrictions on uses are disclosures of health information for treatment, payment, or health care operations. The covered entity does not have to agree to the restriction requested.
- An individual must be given notice of the covered entity's privacy practices and may review the notice prior to signing the consent.

Administrative issues found in the Consent Rules include that:

- signed consents must be retained for six years from the date it was last in effect.
- one joint consent may be obtained by certain integrated covered entities for use by multiple entities.
- if a covered entity obtained consents and also receives an authorization, the covered entity must disclose information in accordance with the more restrictive document, unless the covered entity resolve's the conflict with the individual.

Frequently Asked Questions

For each of the Rules discussed in the Guidance, the Guidance includes answers to frequently asked questions regarding the Rules. The answers provide guidance to the covered entities and the public regarding how the rules should be applied. Below is a summary of the responses to the frequently asked questions regarding the Consent Rules.

Are health plans or clearinghouses required to obtain an individual's consent to use or disclose protected health information to carry out treatment, payment or health care operations?
No. Health plans and clearinghouses may use and disclose protected health information without obtaining consent for the purpose of carrying out treatment, payment, or health care operations. However, they may obtain consent if they choose to, and if so, must obtain consent in accordance with the Consent Rules.

Can a pharmacist use protected health information to fill a prescription telephoned in by a patient's physician if the patient is a new patient to the pharmacy and has not yet provided written consent to the pharmacy?
Currently, this activity is not permitted under the Privacy Rule. The Secretary of HHS is aware that this provision in the rules may impede a pharmacist's normal activities, and will propose modifications to the rule to address this problem.

Can direct treatment providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures before obtaining the patient's written consent?

The Privacy Rule, as written, would require consent prior to any of these routine activities. This poses a problem if the first contact with a provider is not in person. The Secretary of HHS is aware of this problem, and will propose modifications to address it.

Will the consent requirement restrict the ability of providers to consult with other providers about a patient's condition?

No. The provider with a direct treatment relationship with the patient must obtain consent to provide treatment to the patient. Consulting with other providers about a patient's condition falls under the definition of treatment. As long as the provider being consulted does not have a direct treatment relationship with the patient, it does not need to obtain consent from the patient.

Does a pharmacist have to obtain a consent under the Privacy Rule in order to provide advice about over-the-counter medicines to customers?

As long as the pharmacist does not keep records of protected health information for such a situation, the pharmacist does not have to obtain the customer's consent to provide this advice. The pharmacist may not otherwise disclose or use the protected health information.

Can a patient have a friend or family member pick up a prescription for her?

Yes. The pharmacist may use professional judgment and experience to make a reasonable inference that it is in the patient's best interest to allow a person, other than the patient, to pick up a prescription. The patient does not have to provide the pharmacist with names of such persons in advance. The Guidance provides the example that a friend or relative picking up a specific prescription is evidence that that individual is involved in the patient's care.

The rule provides an exception to the prior consent requirement for "emergency treatment situations." How will a provider know when the situation is an "emergency treatment situation" and, therefore, is exempt from the Privacy Rules prior consent requirement?

The provider must determine whether obtaining a consent would interfere with the timely delivery of necessary health care, using professional judgment. If so, the provider may use protected health information in order to carry out treatment, payment or health care operations. The provider must also attempt to obtain consent as soon as is reasonably possible after the care has been provided.

Does the exception to the consent requirement regarding substantial barriers to communication with the individual affect requirements under Title VI of the Civil Rights Act of 1964 or the Americans with Disabilities Act?

No. The fact that the Privacy Rule provides an exception to consent due to substantial barriers to communication does not affect covered entities' obligations under these laws.

What is the difference between "consent" and "authorization" under the Privacy Rule?

A **consent** is a general document that gives health care providers having a direct treatment relationship with a patient, the permission to use and disclose all protected health information for treatment, payment and health care operations. It gives permission to a provider, and no other person. Consents do not need to specify the particular use or disclosure of information, and may be used by the provider to cover all uses and disclosures of information for treatment, payment and health care operations. A provider may use consents as a condition of treatment.

An **authorization** is a more customized document giving covered entities permission to use or disclose protected health information for specific purposes, generally other than for treatment, payment or health care operations. Treatment may not be conditioned upon an individual providing authorization. Authorizations have an expiration date.

Examples cited in the Guidance of when authorizations would be needed include selling a patient mailing list, disclosing information to an employer for employment decisions, and disclosing information for eligibility for life insurance.

Would a covered entity ever need an authorization rather than a consent for uses or disclosures of protected health information for treatment, payment, or health care operations?

Yes, there are circumstances when authorization would be required for treatment, payment or health care operations. Authorization is required to disclose protected health information in psychotherapy notes for treatment by persons other than the originator of the notes, for payment or health care operations purposes, other than uses and disclosures specifically excepted in the Privacy Rules. Another circumstance would be when a health plan seeks payment for a particular service from a second health plan, such as in the coordination of benefits or secondary payer situation, and needs protected health information from a physician who provided health care services to an individual. The provider, who was given consent, has generally already been paid in such a circumstance, and the transaction is between two health plans. The plan should use an authorization to request the disclosure from the physician, rather than a consent.

Will health care providers be required to determine whether another covered entity has a more restrictive consent form before disclosing information to that entity for treatment, payment, or health care operations purposes?

No. A consent permits only the covered entity that obtains the consent to use or disclose protected health information for its own treatment, payment or health care operations. One covered entity is not bound by the terms of consents provided to another covered entity, unless a joint consent has been used, or the entities are affiliated entities using the same consent.

What is the interaction between "consent" and "notice''?

The consent refers to the notice, and informs the individual that the individual has the right to review the notice before signing the consent.

May consent for use or disclosure of protected health information be provided electronically?

Yes, as long as the consent meets all the requirements under the Privacy Rule, and the consent is signed by the individual.

Must a covered entity verify signature on a consent form if the individual is not present when he signs it?

No.

May consent be obtained by a health care provider only one time if there is a single connected course of treatment involving multiple visits?

Yes. Even if the course of treatment is not a single connected course, a provider is required to obtain consent only one time. A new consent is required only if the patient has revoked a consent between treatments.

If an individual consents to the use or disclosure of protected health information for treatment, payment, or health care operations purposes, or obtains a health care service, and then revokes consent before the provider bills for such service, is the provider precluded from billing for such service?

No. If service has been provided after obtaining consent, the provider may bill for the service even if consent is revoked immediately after the service has been provided. A revocation is not effective to the extent that the health care provider has acted in reliance on the consent.

If covered providers that are affiliated or part of an organized health care arrangement are located in different states with different laws regarding uses and disclosures of health information (e.g., a chain of pharmacies) do they need to obtain a consent in each state the patient obtains treatment?

No. The consent only needs to be obtained by a covered entity, or by affiliated entities, one time. State laws may impose additional requirements for consent forms.

Must a revocation of a consent be in writing?

Yes.

Minimum Necessary

45 CFR §§ 154.502(b), 164.514(d)

General Requirement

The Privacy Rule requires that covered entities limit the use, disclosure and requests for protected health information to the minimum necessary to accomplish the intended purposes. The minimum necessary requirement does not apply to the following:

- *Disclosures to or requests by a health care provider for treatment purposes.*
- *Disclosures to the individual who is the subject of the information.*
- *Uses or disclosures made pursuant to an authorization requested by an individual*
- *Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.*
- *Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.*
- *Uses or disclosures that are required by other law.*

A covered entity is to develop and implement policies and procedures regarding the minimum necessary standard that are appropriate for its own organization, and that reflect the entity's business practices and workforce.

Uses And Disclosures Of, And Requests For Personal Health Information

Policies and procedures for use of protected health information must identity the persons or classes of persons within the entity who need access to the information to carry out their job duties. They must also identify the categories or types of protected health information needed, and the conditions under which access is appropriate. The Guidance provides the example that hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. The policies and procedures must state when the entire medical record is necessary, including a justification.

Routine or recurring requests and disclosures may have standard protocol procedures and policies and must limit the protected health information disclosed to the minimum necessary.

Where non-routine disclosures are involved, the policies and procedures must include reasonable criteria for determining, and limiting disclosure to, only the minimum amount of protected health information needed to accomplish the purpose of the disclosure. Non-routine disclosures must be reviewed on an individual basis.

Reasonable Reliance

The Privacy Rule allows a covered entity to rely on the requestor's judgment, in certain circumstances, regarding the minimum amount of information that is needed. These circumstances include when the requestor is:

- A public official or agency for a disclosure relating to a complaint or a compliance review, as allowed for in the Privacy Rules
- Another covered entity
- A professional who is a workforce member or business associate of the covered entity that holds the information
- A researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

The covered entity always retains the discretion to make its own minimum necessary determination for disclosures, regardless of the requestor.

Frequently Asked Questions

Following is a summary of the questions and answers addressed in the Guidance concerning the minimum necessary rules.

How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

Covered entities are allowed under the Privacy Rules to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of entity's business and workforce. The minimum necessary standard is a reasonableness standard, not a strict standard.

Won't the minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health-care providers involved in treatment?

No. The disclosure of information between health care providers for treatment purposes is specifically exempted from the minimum necessary requirements.

Do the minimum necessary requirements prohibit medical residents, medical students, nursing stations, and other medical trainees from accessing patients' medical information in the course of their training?

No. The definition of "health care operations" includes "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Access to medical information for training purposes, including access to entire medical records, should be included in the policies and procedures for minimum necessary uses and disclosures.

Must minimum necessary be applied to disclosures to third parties that are authorized by an individual?

No. Most uses or disclosures authorized by an individual are exempt from the minimum necessary requirements. This includes, the Guidance states, authorizations covered entities may receive directly from third parties, such as life, disability, or casualty insurers pursuant to the patient's application for or claim under an insurance policy. The Guidance provides an example of an individual's authorization being received by a provider to disclose medical information to a life insurer for underwriting purposes. The provider is permitted to disclose the information requested without making any minimum necessary determination, as long as the authorization meets the requirements within the Privacy Rule.

Are providers required to make a minimum necessary determination to disclose to federal or state agencies, such as the Social Security Administration (SSA) or its affiliated state agencies, for individuals' applications for federal or state benefits?

No. Since these disclosures are authorized by the individual, they are exempt from the minimum necessary standards.

Does the rule strictly prohibit use, disclosure, or requests of an entire medical record? Does the rule prevent the use, disclosure, or requests of the entire medical records without case-by-case justification?

No. A covered entity may use, disclose, or request an entire medical record if the covered entity has documented its policies and procedures and they indicate that the entire medical record is the amount reasonably necessary for the purpose. Justification does not have to be provided with each distinct medical record. Where the minimum standard does not apply, no justification is needed.

In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, in order to comply with the minimum necessary requirements?

No. Covered entities are to make reasonable efforts to limit access to protected health information to only those who need access based on their roles within the entity. Although facility redesigns are not generally necessary, the entity may need to make adjustments to their facilities, such as isolating and locking file cabinets or record rooms, or providing additional security such as passwords on computers maintaining personal information.

Do the minimum necessary requirements prohibit covered entities from maintaining patient medical charts at bedside, require that covered entities shred empty prescription vials, or require that X-ray light boards be isolated?

No. Covered entities must take reasonable precautions to prevent inadvertent or unnecessary disclosures. For example, the Guidelines state that the Privacy Rule does not require that X-ray boards be totally isolated from all other functions, however, it does require that covered entities take reasonable precautions to protect X-rays from being accessible to the public.

Will doctors' and physicians' offices be allowed to continue using sign-in sheets in waiting rooms?

It was not the intent of the Department of HHS to prohibit the use of sign-in sheets.

What happens when a covered entity believes the request is seeking more than the minimum necessary protected health information?

The entity must limit its disclosure to the minimum necessary, as determined by the disclosing entity. If the situation falls under one of the circumstances where the entity is allowed to rely upon the requesting entity to determine what is the minimum necessary, the entity may do so.

Oral Communications

45 CFR §§160.103, 164.501

Background

The Privacy Rule applies to oral communications, as well as electronic, written and any other, regarding protected health information. If the Rule did not apply to oral communications, then any health information could be disclosed, as long as the disclosure was spoken.

General requirements

The general requirements regarding oral communications as stated in the Guidance are as follows:

- *Covered entities must reasonably safeguard protected health information – including oral information – from any intentional or unintentional use or disclosure that is in violation of the rule (see §164.530I(2)). They must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. "Reasonably safeguard" means that covered entities must make reasonable efforts to prevent uses and disclosures not permitted by the rule. However, we do not expect reasonable safeguards to guarantee the privacy of protected health information from any and all potential risk. In determining whether a covered entity had provided reasonable safeguards, the Department*

will take into account all the circumstances, including the potential effects on patient care and the financial and administrative burden of any safeguards.

- *Covered entities must have policies and procedures that reasonably limit access to abuse of protected health information to the minimum necessary give to the job responsibilities of the workforce and the nature of their business (see §§ 164.502(b), 164.514(d)). The minimum necessary standard does not apply to disclosures, including oral disclosures, among providers for treatment purposes.*
- *Many health care providers already make it a practice to ensure reasonable safeguards for oral information – for instance, by speaking quietly when discussing a patient's condition with family members in a waiting room or other public area, and by avoiding using patients' names in public hallways and elevators. Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.*

Frequently Asked Questions

Below is a summary of the frequently asked questions regarding oral communications found in the Guidance:

If health care providers engage in confidential conversations with other providers or with patients, have they violated the rule if there is a possibility that they could be overheard?

The Privacy Rule is not intended to prohibit providers from talking to one another or to their patients, and is not intended to prohibit providers to speak loudly to one another in a busy emergency room in order to ensure appropriate treatment.

The Guidance states that the following practices are permissible under the Rule, as long as reasonable precautions are taken to minimize the chance of inadvertent disclosures to others nearby:

- *Health care staff may orally coordinate services at hospital nursing stations.*
- *Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.*
- *A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.*
- *Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.*

Does the Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is over heard?

No. The Privacy Rule does not require that an entity have private rooms, soundproofing of rooms, encryption of wireless or other emergency medical radio communications which can be intercepted by scanners, encryption by telephone systems.

Covered entities must take reasonable measures to safeguard patient information. According to the Guidance, such reasonable safeguards include:

- *Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.*
- *Providers could add curtains or screens to areas where oral communications often occur between doctors and patients or among professionals treating the patient.*
- *In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonable use cubicle or shield-type dividers, rather than separate rooms.*

Do covered entities need to provide patients access to oral information?

No. Under the Privacy Rule, covered entities are required to provide individuals with access to protected health information about themselves contained within their "designated record sets." Oral information is not part of designated record sets as defined in the Rule.

Do covered entities have to document all oral communications?

No. The Privacy Rule does not include the requirement that covered entities document any information used or disclosed for treatment, payment or health care operations purposes, including oral communications. However, certain oral communications are required to be documented under the Rule, for example in order to meet the standard for providing a disclosure history to an individual upon request. When the Privacy Rule requires documentation, it requires it for all relevant communications, including oral communications. The Guidance provides an example of a physician disclosing information about a case of tuberculosis to a public health authority. This disclosure must be documented by the physician, whether it was done orally or in writing.

Did the Department change its position from the proposed rule by covering all oral communications in the final Privacy Rule?

No. The proposed rule would have covered information in any form or medium, as long as it had at some point been maintained or transmitted electronically. Once information had been electronic, it would have been covered, no matter in what form it was held by the entity.

For example, if a patient had e-mailed a single piece of protected health information to a clinic, and the clinic placed that information into the patient's record, that piece of information would have been under the jurisdiction of the Administrative Simplification law, but other records held by the clinic would not, possibly even records for that same patient. It would be extremely difficult for a clinic or other provider to determine which records were under the Administrative Simplification law and accompanying regulations and which were not. The Privacy Rule removed the nexus to electronic information, and covers all individually identifiable health information of a covered entity.

Business Associates

45 CFR §§ 160.103, 164.502(e), 164.514(e)

Background

Today, most health care providers and health plans do not carry out all of their health care activities and functions themselves. Rather they use various business associates to carry out

certain tasks. Under the Privacy Rule, providers and plans are allowed to give protected health information to business associates as long as they receive satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of certain disclosures. Protected health information may only be disclosed to a business associate to help the providers and plans carry out their health care functions. The business associate may not use it for its independent use.

What Is A Business Associate

The Guidance gives the following information about what a business associate is:

- *A business associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of protected health information.*
- *A business associate is not a member of the health care provider, health plan, or other covered entity's workforce.*
- *A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.*
- *The rule includes exceptions. The business associate requirements do not apply to covered entities who disclose protected health information to providers for treatment purposes – for example, information exchanges between a hospital and physicians with admitting privileges at the hospital.*

Frequently Asked Questions

Has the Secretary exceeded the statutory authority by requiring "satisfactory assurances" for disclosures to business associates?

No. HIPAA gives the Secretary authority to directly regulate health care providers, health plans, and health care clearinghouses. The Department also has explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department has the authority to require that a business associate have a contract with a covered entity in order for protected health information to be disclosed to that business associate.

Has the Secretary exceeded the HIPAA statutory authority by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?

Business associates are not subject to all the provisions of the Privacy Rule, but just a narrow set of them through the contract requirement. The Guidance points out that, for example, covered entities are not required to ask business associates to agree to appoint a privacy office, or to develop policies and procedures for use and disclosure of protected health information.

Is it reasonable for covered entities to be held liable for the privacy violations of business associates?

Covered entities are not held liable for privacy violations of business associates. Covered entities are not required to actively monitor or oversee the means by which the business

associate carries out safeguards and are not required to monitor the extent to which the business association abides by the requirements of the contract.

If a covered entity becomes aware of a pattern or practice of a business associate that constitutes a material breach or violation of the business associate's contractual obligations, the covered entity must take "reasonable steps" to cure the breach or to end the violation. If such steps are not successful, the covered entity must terminate the contract, if feasible, or if not feasible, must report the problem to the Department of HHS.

Parent And Minors

45 CFR §164.502(g)

General Requirements

A parent usually has authority to make health care decisions about a minor child and is normally considered a ***"personal representative"*** under the Privacy Rule, and so would be able to access health information about the minor child. This same provision applies to a guardian or other person acting *in loco parentis* of a minor.

In certain circumstances, a parent may not be considered a "personal representative" under the Privacy Rule, and so would not have control over the protected health information of the child. The Guidance provides the following examples of such circumstances:

- *When state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service, the parent is not the minor's personal representative under the Privacy Rule. For example, when a state law provides an adolescent the right to consent to mental health treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment. The minor may choose to involve a parent in these health care decisions without giving up his or her right to control the related health information. Of course, the minor may always have the parent continue to be his or her personal representative even in these situations.*
- *When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services. For example, courts may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself. In order to not undermine these court decisions, the parent is not the personal representative under the Privacy Rule in these circumstances.*

The Guidance also provides situations under which the Privacy Rule reflects current professional practice in determining that the parent is not the minor's personal representative and therefore would not have access to the minor's protected health information. One situation would be when a parent agrees to a confidential relationship between the minor and the physician, for example when a physician asks a parent of a 16-year old if the physician can talk with the child confidentially about a medical condition and the parent agrees, the parent would not control the protected health information that was discussed during the confidential conference. Another situation would be when a physician reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child. In such a

situation, the physician may choose not to treat the parent as the personal representative of the child.

Relation To State Law

The Privacy Rule does not preempt state laws that specifically address disclosure of health information about a minor to a parent, whether the state law authorizes or prohibits such disclosure.

Frequently Asked Questions

The Guidance addresses the following questions regarding the rules surrounding parents and minors:

Does the Privacy Rule allow parents the right to see their children's medical records?

Generally, yes. There are two exceptions, however. These are (1), when a parent agrees to a confidential relationship with the provider, and (2) when a provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, and that treating the parent as the child's representative could endanger the child.

Does the Privacy Rule provide rights for children to be treated without parental consent?

No. The Privacy Rule does not address consent to treatment, only the access to protected health information. The Privacy Rule does not preempt or change state or other laws that address consent to treatment.

If a child receives emergency medical care without a parent's consent, can a parent get all information about the child's treatment and condition?

Generally, yes. Under the Privacy Rule, the parent would still be the child's personal representative, unless the situation meets one of the two exceptions.

Health-Related Communications And Marketing

45 CFR §§ 164.501, 164.514(e)

What Is Marketing

Under the Privacy Rule, "marketing" is defined as "a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service." The Guidance provides activities that are not marketing under the Privacy Rule.

Communications That Not Marketing

A covered entity is not "marketing" when it:

- *Describes the participating providers or plans in a network. For example, a health plan is not marketing when it tells its enrollees about which doctors and hospitals are preferred providers, which are included in its network, or which providers offer a particular service.*

Similarly, a health insurer notifying enrollees of a new pharmacy that has been to accept its drug coverage is not engaging in marketing.

- *Describes the services offered by a provider or the benefits covered by a health plan. For example, informing a plan enrollee about drug formulary coverage is not marketing.*

It is also not considered "marketing" when a covered entity uses an individual's protected health information to tailor a health-related communication to that individual, as long as the communication is:

- *Part of a provider's treatment of the patient and for the purpose of furthering that treatment. For example, recommendations of specific brand-name or over-the-counter pharmaceuticals or referrals of patients to other providers is not marketing.*
- *Made in the course of managing the individual's treatment or recommending alternative treatment. For example, reminder notices for appointments, annual exams, or prescription refills are not marketing. Similarly, informing an individual who is a smoker about an effective smoking-cessation program is not marketing, even if that program is offered by someone other than the provider or plan making the recommendation.*

Limitations On Marketing Communications

A covered entity may use or disclose protected health information to create or make a marketing communication, pursuant to obtaining applicable consent, only if the marketing:

- Is a face-to-face communication, such as a patient being provided sample products during an office visit;
- Involves products or services of nominal value, such as a provider distributing pens, toothbrushes or key chains with the name of the covered entity or health care product manufacturer on it; or
- Concerns the health-related products and services of the covered entity or a third party, and it (1) identifies the covered entity making the communication so that consumers will know the source of the marketing calls or materials, (2) states that the covered entity is being compensated for making the communication, if so, (3) tells individuals how to opt out of further marketing communications as described in the Privacy Rule, and (4) explains why individuals with specific conditions or characteristics have been targeted, and if so, how the product or service relates to the health of the individual. The covered entity must have made a determination that the product or service may be of benefit to individuals with the condition or characteristic targeted by the communication.

All other marketing communications must be done pursuant to obtaining authorization from the individual to use or disclose protected health information to create or make the marketing communication.

Business Associates

Protected health information for marketing purposes may only be disclosed by a covered entity to business associates that undertake marketing activities on the behalf of the covered entity. No other disclosure for marketing is permitted under the Privacy Rule. A covered entity must obtain authorization from each person on a patient or enrollee list before it may be given away or sold.

The covered entity must obtain the business associate's agreement to use protected health information only for the covered entity's marketing activities. The covered entity may not give protected health information to a business associate for the business associate to use for its own purposes.

Frequently Asked Questions

Does this rule expand the ability of providers, plans, marketers and others to use my personal health information to market goods and services to me? Does the Privacy Rule make it easier for health care businesses to engage in a door-to-door sales and marketing efforts?

No. The Privacy Rule has more restrictive limits on the use and disclosure of protected health information marketing than exist in most states. The Guidance gives two examples of marketing that now require authorization under the Privacy Rule which would have been allowed in most states prior to the enactment of the Rule:

- *Selling protected health information to third parties for their use and re-use. Under the rule, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines.*
- *Disclosing protected health information to outsiders for the outsiders' independent marketing use. Under the rule, doctors may not provide patient lists to pharmaceutical companies for those companies' drug promotions.*

Also, the Privacy Rule places limits on marketing activities of business associates that did not exist before the Rule. For example, under the Rule, a covered entity may not give protected health information to a telemarketer, door-to-door salesperson or other hired marketer unless the marketer has agreed by contract to use the information only to market on behalf of the entity, and not for the marketer's own use, or for the use of a third party. Contracted telemarketers must identify the covered entity that is sponsoring the marketing call and must provide individuals the opportunity to opt-out of further marketing.

Can telemarketer's gain access to personal health information and call individuals to sell goods and services?

Only if the telemarketer was hired to undertake marketing by the covered entity and has contractually agreed to use the information for marketing on behalf of the covered entity, as a business associate. The individual must authorize any other use of an individual's protected health information.

How can I distinguish between activities for treatment, payment or health care operations versus marketing activities?

Marketing may occur during treatment, payment or health care operations, and the definition of "marketing" under the Privacy Rule does not require making a distinction for the purposes of determining when marketing rules apply. If the marketing communication does not fall under one of the exceptions to requiring authorization by the individual, the covered entity must obtain authorization, regardless of when the communication takes place.

Do disease management, health promotion, preventative care, and wellness programs fall under the definition of "marketing"?

Whether these activities fall under the definition of marketing depends upon the way the activities are conducted. The covered entity must examine the way these activities are undertaken, and compare this to those activities that are exempted from the definition of marketing to determine whether authorization must be obtained from participants.

Can contractors (business associates) use protected health information to market to individuals for their own business purposes?

Covered entities may not provide protected health information to a business associate for the business associate's own use unless authorization is obtained from the individuals.

Research

45 CFR §§ 164.501, 164.508(f), 164.512(i)

Background

A covered entity may always use or disclose protected health information that has been de-identified. The ***Research Rules*** in the Privacy Rule place restrictions on the use or disclosure for research purposes of protected health information that has not been de-identified. It also addresses how research subjects are informed about how their medical information will be used or disclosed and how a research subject may gain access to information about themselves when the information is held by covered entities. The Privacy Rule protects the privacy of individually identifiable health information, while ensuring that researchers continue to have access to medical information necessary to conduct important research.

Using And Disclosing Protected Health Information For Research

Certain uses and disclosures of protected health information are allowed without authorization under the Privacy Rule. Other uses and disclosures must be pursuant to authorization.

Research Use/Disclosure Without Authorization

In order to use or disclose protected health information without authorization by a research participant, the covered entity must obtain one of the following, as stated in the Guidance:

- *Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an Institutional Review Board (IRB) or a Privacy Board. This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information and it is not practicable to obtain research participants' authorization.*
- *Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.*

- *Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought.*

Protected health information for research purposes may be used or disclosed by a covered entity pursuant to a waiver of authorization by an IRB or Privacy Board as long as it has obtained documentation of all of the following:

- *A statement that the alteration or waiver of authorization was approved by an IRB or Privacy Board that was composed as stipulated by the Privacy Rule;*
- *A statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;*
- *A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the following eight criteria:*
  - *The use or disclosure of protected health information involves no more than minimal risk to the individuals;*
  - *The alteration or waiver will not adversely affect the privacy rights and the welfare of the individual;*
  - *The research could not practicably be conducted without the alteration or waiver;*
  - *The research could not practicably be conducted without access to and use of the protected health information;*
  - *The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individual, and the importance of the knowledge that may reasonably be expected to result from the research;*
  - *There is an adequate plan to protect the identifiers from improper use and disclosure;*
  - *There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and*
  - *There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.*
- *A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;*
- *A statement that the alternation or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as stipulated by the Privacy Rule; and*
- *The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.*

Research Use/Disclosure With Individual Authorization

With individual authorization, covered entities may use and disclose protected health information for research purposes. The authorization to release individual information for a research study that included treatment must include research-specific elements. For example, if the covered entity/researcher plans to bill the individual's health plan for the routine costs of care associated with the treatment, the authorization must describe the types of information that will be provided to the health plan.

Frequently Asked Questions

The Guidance addresses the following questions:

Will the rule hinder medical research by making doctors and others less willing and/or able to share information about individual patients?

The Department does not believe that the Privacy Rule will hinder medical research. Rather, it believes that patients and health plan members should be more willing to participate in research when they know information is protected. The Guidance provides an example to support this assertion that in genetic studies at the National Institutes of Health, nearly thirty-two percent of eligible people offered a test for breast cancer risk decline to take it, and of those who refuse the test, the majority cite concerns about health insurance discrimination and loss of privacy as the reason.

Does the Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing protected health information?

No. The Privacy Rule does not address the conditions a researcher may use to determine who may or may not enroll in a study. Therefore, a researcher may condition participation on the execution of an authorization.

Does the covered entity need to create an IRB or privacy board before using or disclosing protected health information for research?

No. The IRB or Privacy Board may be an independent board, or the covered entity could create the IRB or Privacy Board.

What does the Privacy Rule say about a research participant's right of access to research records or results?

The Privacy Rule gives patients the right, with few exceptions, to inspect and obtain a copy of health information about themselves maintained in a "designated record set." For example, one of the permitted exceptions is the suspending of an individual's access rights while a clinical trial is in progress, if the individual agreed to the denial of access when consenting to participate in the clinical trial.

Are the Privacy Rule's requirements regarding patient access in harmony with the Clinical Laboratory Improvement Amendments of 1988?

Yes. If clinical laboratories that are also covered health care providers are prohibited by the Clinical Laboratory Improvement Amendment to provide an individual access to information, the Privacy Rule includes an exception from the individual access rules, and does not require that individual access be provided.

THE NAIC MODEL ACTS AND EFFORTS TO PROTECT CLIENT PRIVACY

What Does NAIC Do?

The National Association of Insurance Commissioners (NAIC), founded in 1871, is an organization of the chief insurance regulatory officials of the fifty states, the District of Columbia, and the four U.S. territories. The NAIC exists to assist state insurance regulators, individually and collectively, to assure the fair and equitable treatment of insurance consumers. The NAIC's primary instruments of providing technical assistance and guidance to the states are its model laws, regulations, and guidelines. Model laws and regulations are developed by committees of regulators at the NAIC's national meetings, which take place four times a year. NAIC meetings are public and the regulators solicit comments on all drafts. Each model is referred to a parent committee for approval and ultimately to the plenary session of the NAIC for adoption. All NAIC members have the opportunity to vote on a model at the plenary session. A state may either adopt an NAIC model intact or modify it to meet the state's specific needs and conditions.

The NAIC's Regulatory Framework Task Force, whose parent committee is the Accident and Health Insurance (B) Committee, has been charged with the development of a model law addressing the confidentiality of health information. In 1993 the NAIC established the Health Plan Accountability Working Group, identified as the Task Force, to develop model acts establishing a comprehensive regulatory structure for all types of managed care entities. As part of this process, the NAIC began to examine the issues raised by the collection and reporting of health information and data, and the need to protect the confidentiality of such information. In 1993 and 1994 the working group developed a draft model act addressing the confidentiality of health information. Work on this draft, which was derived in significant part from the NAIC's existing model, the "NAIC Insurance Information and Privacy Protection Model Act," was suspended in 1995 while the working group completed five other models. This occurred because the regulators concluded that a confidentiality model could best be developed once the proposed regulatory structure for managed care health plans was complete. In the summer of 1996 the working group returned its attention to confidentiality issues and released a new draft, the "Protected Health Information Model Act." The working group also released a statement of "Principles for Model Act Addressing the Confidentiality of Health Information" to guide its drafting process. In 1997 this working group, which has been renamed the Health Information and Privacy Working Group, was charged with developing a model act addressing the confidentiality of health information.

The NAIC has three areas of concern with respect to federal legislation setting such standards. The first is the potential ***preemption of state law*** affecting individually identifiable health information. The second is ***protecting the right of insurance regulators to have access*** to individually health identifiable information to carry out their authorized regulatory functions. And the third is ***protecting the right of states to establish and enforce appropriate standards*** for insurance carriers in their collection, use, and disclosure of individually identifiable health information.

Preemption

HIPAA addresses the issue of the confidentiality of individually identifiable information explicitly. It charges the Secretary with making detailed recommendations to Congress after consulting

with the National Committee on Vital and Health Statistics. In addition Section 1173(d)(2) of the Social Security Act, as added by HIPAA, requires the Secretary to adopt and enforce security standards for health information that "ensure the integrity and confidentiality of the information" and that "protect against any reasonably anticipated...unauthorized uses or disclosures of the information...." There are existing state statutes that are relevant to both these charges. It is Congress's expressed intent that, in general, federal law or regulation not preempt these statutes.

The HIPAA establishes that any federal regulation promulgated pursuant to Section 264 shall not supersede a contrary provision of state law that "imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation." This language expresses the intent of Congress that any federal requirements with respect to individually identifiable health information established under HIPAA will constitute minimum requirements which do not prevent states from retaining or enacting additional protections.

Section 1178 of the Social Security Act, as added by HIPAA, contains exceptions that protect state laws if the Secretary determines that they are necessary for any of the purposes outlined in Section 1178(a)(2)(A). It also protects, without any Secretarial determination, a state law that "relates to the privacy of individually identifiable health information" and is therefore subject to HIPAA Section 264(c)(2). The language of Section 1178 also expresses Congressional intent that more stringent state laws affecting the privacy of individually identifiable health information, as well as certain other state laws, not be preempted.

It is very important that the states be accorded the maximum flexibility to supplement HIPAA's privacy standards if they so desire. It is important to allow more stringent state requirements for two reasons:

- A number of states have already enacted detailed provisions governing the use and disclosure of individually identifiable health information. These states laws may apply more broadly than to the individually identifiable health information transmitted in connection with the transactions described in the Social Security Act. Preempting these existing provisions would leave consumers in these states with less protection as a result of enactment of the federal law than they already have.
- In states that have not developed extensive protections for individually identifiable health information, federal preemption would create a ceiling, rather than a floor, that would deprive states of the flexibility to address specific problems in unique ways. While multistate carriers and health plans may argue for uniform privacy standards, it is not clear that uniformity is as compelling a need for consumers, particularly consumers from states that already have extensive protections.

As regulators of the insurance industry, state insurance departments have long-standing expertise in obtaining and protecting the confidentiality of highly sensitive information, which takes many forms. It includes proprietary information developed by insurance companies pertaining to their products, actuarial formulas and other business practices, and certain financial information, as well as health information about specific individuals. It is the common practice of insurance departments to obtain and evaluate confidential information in order to conduct their authorized regulatory functions. Every state has laws which authorize the insurance department to collect such information from regulated entities, but which also protect the information from further disclosure by the insurance department.

It is imperative that any federal privacy standards, either promulgated by the Secretary or adopted by Congress, not be construed by insurance carriers, health plans, or other regulated entities as prohibiting them from disclosing to state insurance regulators any individually identifiable health information that is essential for the effective regulation of these entities. Without access to individually identifiable health information, state insurance regulators would not be able to fulfill their fundamental purpose of protecting consumers.

State insurance departments typically need access to individually identifiable health information in three situations:

- to investigate a consumer complaint
- to conduct a market conduct examination of an insurance company or other regulated entity
- to conduct a financial solvency examination

Federal legislation that impeded the ability of state insurance departments to perform any of the three would greatly concern state insurance regulators.

Consumer Complaints

In investigating a consumer complaint, a state insurance department obtains a written statement from a consumer that includes an authorization to obtain that consumer's medical records from the insurance entity about whom the complaint is made. Many complaints involve a company's denial of a claim on the grounds that the service is not a covered benefit or is an experimental treatment. Without access to the consumer's medical records and the specific policy covering the consumer, the insurance department cannot determine whether the service provided was in fact a covered benefit. Access to individually identifiable information in these situations is generally not a problem because the individual who initiates the complaint is also the subject of the information and has authorized the department's access to the information in order for the complaint to be investigated.

The willingness of most complainants to authorize access to their medical records is fortunate because many state insurance departments consider their complaint process to be the single most reliable source of identifying problem carriers. In addition, through the consumer complaint process, insurance departments recover literally millions of dollars annually, and this money goes to the consumers, not to the insurance department. For example, in 1996 the Wisconsin Insurance Department completed the investigation of 8,407 complaints and recovered $2,350,000, of which $1,650,000 involved denied claims. All this money was recovered for the complainants and is completely separate from fines or penalties obtained by the Department.

Market Conduct Examinations

In a market conduct examination, the state insurance department initiates and conducts an extensive examination of an insurance carrier, including visits to the company's offices, to determine how the company is conducting its business within that state. These examinations focus on a company's marketing and sales of policies and its payment of claims, as opposed to its financial condition. To conduct a thorough market conduct examination, state insurance regulators must examine numerous records and files, including the company's register of complaints.

Most states have broad statutes authorizing the insurance commissioner's access to all relevant records and files. The regulators review individually identifiable health information to ensure that

a company is paying similar benefits for similar claims, and to investigate the complaints kept in the company's register. These examinations require regulators to review information identifying numerous consumers. Obtaining each consumer's authorization would be very time-consuming, expensive, and impracticable. Moreover, allowing the company to "sanitize" the information by concealing the name and address of the insured individual can, in certain situations, promote fraud by making it easier for a company to fabricate or alter claims.

Despite clear authority under the laws of most states to review a regulated entity's files and records, insurance departments do encounter carriers who attempt to withhold files on the grounds that they contain confidential information. These carriers use the pretext of protecting a consumer's privacy to avoid legitimate regulatory oversight of their activities. A federal law that called into question a state insurance department's authority to examine a carrier's records and files would foster evasive conduct and would not benefit consumers.

A state insurance department's authority to obtain access to individual records will become even more important as states implement and enforce new standards to regulate managed care entities. For example, the NAIC has very recently adopted five model acts, which set standards for managed care activities in five areas:

- the adequacy of the health plan's provider network, including its contracts with providers
- the health plan or carrier's grievance procedures
- its utilization review procedures
- its quality assurance activities
- its credentialing of health care professionals

To enforce the utilization review standards, the insurance department will have to examine individual records to ensure that acceptable protocols were followed with respect to specific cases. In monitoring grievance procedures, the department will have to review individual records to determine what the consumer was told, who conducted the grievance review on behalf of the carrier, and whether the procedures followed were appropriate and were in effect at the time of the consumer's grievance.

To regulate the adequacy of provider networks, the insurance department will have to identify specific subsets of the covered population to determine which enrollees need access to certain services, and whether they are obtaining that access based on their clinical records. For example, to determine whether a health plan has a sufficient number of obstetrician-gynecologists, the department will have to determine how many women of childbearing age are enrolled in the plan, and then examine their records to monitor timely access and appropriate referral, including self-referral, to these providers. None of these examinations can be effectively conducted without access to individually identifiable information.

Access to individually identifiable health information will also be critical to the efforts of state insurance departments to enforce the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For example, HIPAA prohibits health insurance carriers in the group market from establishing rules for eligibility and continued eligibility that are based on "health status-related factors" as defined in the law. It also requires guaranteed issue of individual policies to qualified individuals as defined in HIPAA. To enforce these provisions, insurance departments will have to examine individual applications and policies to ensure that certain medical information is not requested or considered in a fashion that violates HIPAA.

It would be a particular challenge to enforce the amendments to HIPAA made by the Newborns' and Mothers' Health Protection Act of 1996 and the Mental Health Parity Act of 1996 if the access of insurance departments to individually identifiable health information was limited. In order to ensure compliance with the provisions of these laws regarding access to maternal and mental health services, state insurance departments will need to review individual records containing health information to see that health carriers are permitting maternity lengths of stay to be determined in accordance with the law and are complying with the law's provisions regarding annual and lifetime limits on mental health benefits.

State insurance departments take seriously their obligation to protect the confidentiality of information that they observe and collect. Often state regulators do not copy or remove the records that they examine. For records that they do need to copy and remove, regulators will often remove identifying information. In some states, the work papers and examination papers are made confidential by law. They are not subject to subpoena or made public until the examination process is concluded. State insurance departments have also promulgated regulations articulating the expectation that their employees maintain the confidentiality of documents in the possession of the department. Some of these state laws and regulations with respect to protecting the confidentiality of information possessed by the insurance department are based on the NAIC's Model Law on Examinations and on the NAIC's Market Conduct Examiners Handbook.

Financial Solvency Examinations

In addition to market conduct examinations, state insurance departments also conduct solvency examinations to review a company's financial statements. Their purpose is to ensure that the company has sufficient assets and reserves to pay the claims that have actually been incurred and that are likely to be incurred. Like market conduct examinations, financial solvency examinations require regulators to examine claims files because the number of claims filed against a company is one factor used to determine whether a carrier has adequate reserves. Again, it is not practicable for regulators to rely on records that contain no individually identifiable information. In many cases a claim and a policy must be matched in order for the regulator to evaluate the carrier's compliance, and this necessitates using records that contain identifying information.

The investigation of consumer complaints and the conducting of both market conduct and financial solvency examinations are among the most basic and important functions of state insurance departments. They could not perform these functions for the benefit of the public without complete access to all records and files of regulated entities. In return for this access, state insurance departments have a long tradition of protecting the confidentiality of information in their possession.

Use and Disclosure of Health Information

State insurance departments protect consumers' privacy by regulating the collection, use, and disclosure of confidential information by insurance carriers and other regulated entities, such as health maintenance organizations. As mentioned above, the NAIC has already adopted an "Insurance Information and Privacy Protection Model Act,", which applies to "insurance institutions, agents or insurance support organizations" as defined in the model.

In the course of developing a comprehensive set of model acts to regulate a variety of managed care entities, the NAIC's Health Plan Accountability Working Group concluded that an additional

model specific to health information was needed to supplement the existing NAIC privacy protection model. One issue is that the current model allows for a fairly general authorization to disclose information, and this general authorization may be broader than is appropriate for health information. In addition the definitions in the existing model do not reflect the rapid changes that have occurred in the managed care industry.

The NAIC recognizes that any model it develops must be consistent with any standards promulgated by the Secretary of Health and Human Services or adopted in federal legislation pursuant to HIPAA. The NAIC's working group has been exploring many of the same issues under discussion by this Subcommittee on Privacy and Confidentiality and has received input from other interested parties, including HHS staff. These issues include:

- Defining the applicability of any model law. Should it apply to health carriers? to all insurance carriers? to other regulated entities? to both primary and secondary users of the information?
- How can "health information" be defined? How can the type of information that must be protected by the law be articulated?
- What structure should the law take with respect to a subject individual's authorization for disclosure? Should consent be required for most disclosures, or should the subject's consent be presumed for disclosures that have certain purposes, such as treatment or payment for treatment?
- What procedures should be required for a subject's access to information about himself and the opportunity to amend or supplement that information?
- Should there be any exceptions to the requirement that a subject have access to all information about him- or herself?
- How does any model law drafted for insurance carriers, health plans, and other entities regulated by the state insurance department interact with existing state and federal laws governing the behavior of providers and according special treatment for certain types of information?
- What are appropriate penalties for violation of the law? How should they be enforced?
- Is the regulatory framework appropriate for electronic transactions, which include individually identifiable health information?
- What limits should exist on a health carrier or health plan's internal use of individually identifiable information, even if that information has been lawfully obtained from the subject individual?

Many of these issues are also raised by the requirement of HIPAA, which instructs the HHS Secretary to include in her recommendations to Congress advice about rights that an individual subject should have with respect to his or her individually identifiable information, the procedures that should be established for the exercise of such rights, and the uses and disclosures of such information that should be authorized or required.

Privacy Issues Working Group

The newly reconstituted NAIC Privacy Issues Working Group had its first official meeting on July 27, 2001, in Chicago. The Working Group was formally re-established in an effort to increase dialogue among regulators and interested parties. Improved communications is critical now that most states have privacy protections in place and are moving to the next phase involving interpretation and enforcement.

One of the principal missions of the Working Group is to serve as a forum for regulators, industry and consumers to discuss questions and issues that will arise as the states interpret and enforce their privacy protections. In keeping with the states' efforts to be as uniform as possible in their approaches to privacy protection, the Working Group's goal is to agree on uniform answers to these questions if at all possible, because many of these issues will crop up in multiple states. The Working Group's analysis of particular issues and responses to questions will serve as guidance to all NAIC members.

Model Regulations

GLBA requires financial institutions, including insurance entities, to establish safeguards to protect the confidentiality, security and integrity of customer information. GLBA requires functional regulators, including state insurance regulators, to implement regulations enforcing such safeguards. At its Chicago meeting, the Working Group exposed a draft model regulation establishing such standards. The draft model regulation is being revised based on comments received subsequent to the Chicago meeting.

Privacy Notice Content Task Force

Now that the July 1, 2001, compliance date for GLBA privacy protections has come and gone, the content of financial institutions' privacy notices and the degree to which consumers are opting out from disclosure have received a great deal of attention. In an effort to make these privacy notices worthwhile for consumers and industry, and to realize the intent of Congress and the regulators who put these protections in place, the NAIC has formed a new task force to draft "plain language" model privacy notices. The Privacy Notice Content Task Force is composed of regulators, consumer representatives and industry, and will draft model language to guarantee that privacy notices are understandable, while ensuring operational uniformity and compliance with the requirements of the NAIC model privacy regulation.

Model Insurance Information and Privacy Protection Act

The National Association of Insurance Commissioners (NAIC) adopted a Model Insurance Information and Privacy Protection Act in 1979. It has been updated subsequently and is being adopted by many states in reaction to Gramm-Leach-Bliley and the Privacy Rule. This Act includes and expands upon some provisions of the Fair Credit Reporting Act as it was originally enacted, and incorporates provisions required by Gramm-Leach-Bliley. The model Act covers insurance institutions, agents, brokers, reinsurers, and organizations supporting the insurance industry. It applies to personal lines of insurance within life, health and property and casualty

insurance The purpose of the Act *is to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance support organizations*.

Under this model Act, three types of information are defined and regulated: 1) medical-record information, 2) personal information, and 3) privileged information. *Medical-record* information is information relating to an individual's physical or mental condition, medical history or medical treatment. Medical record information is also defined to be information obtained from a medical professional or medical-care institution, from the individual or the individual's spouse, parent or legal guardian. *Personal information* is information that is identified with the individual and is used to make judgments regarding the individual's character, habits, avocations, finances, occupation, general reputation, credit, health or other personal characteristics. *Privileged information* is information identified with the individual that is collected in connection with or in reasonable anticipation of an insurance claim or with or in reasonable anticipation of a civil or criminal proceeding.

Under Section 3 of the model Act, pretext interviews are discussed. A *pretext interview* is defined in the Act as an interview in which a person, attempting to obtain personal information about someone else, 1) pretends to be someone else, 2) pretends to represent a person they do not represent, 3) misrepresents the purpose of the interview, or 4) will not give his or her identity when asked. A pretext interview may only be conducted if there is a *reasonable basis for suspecting criminal activity, fraud, material misrepresentation, or material nondisclosure* in a claim situation. This reasonable basis must include *specific information available for review* by the insurance commissioner.

Under Section 4 of the model Act, insurance applicants must be given a written disclosure of the insurer's personal information collection methods, the disclosure practices of personal and privileged information, and a description of the applicant's privacy rights within the Act. Under Section 6, disclosure authorization forms are discussed. Such authorization forms must include what persons are authorized to disclose personal and privileged information and the nature of information that is disclosed to the insurer, insurance producer, or insurance support organization. Disclosure authorization forms for life, health and disability insurance are valid for thirty months under the Act and property and casualty insurance disclosure authorizations are valid for twelve months. Disclosure authorizations related to collecting claim information are valid for the claims process period.

Section 7 of the model Act discusses *investigative consumer reports*. An investigative consumer report is defined as consumer reports, or portions of consumer reports, that are based on personal interviews with the subject's neighbors, friends, associates, acquaintances or others. Information provided during these personal interviews concern the person's character, general reputation, personal characteristics or mode of living. Under the Act, investigative consumer reports may not be requested or prepared unless the subject is notified that such a report may be prepared and that he or she may receive a copy of the completed report if he or she so requests.

Section 8 provides rights to individuals to personal information an insurer, insurance producer or insurance support organization is reasonably able to locate and retrieve. The individual must make the request in writing. The insurer, insurance producer or insurance support organization must respond to the request within no more than thirty business days. The response must inform the requestor of the *nature and substance* of the personal information, include allowing the requestor to see and obtain a copy of the information either in person or through the mail,

disclose the identity of any persons to whom the information has been released, and provide an explanation of how the individual may request that information may be corrected, amended or deleted. An individual may not have access to information that is *collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding*.

Section 9 provides the process of correcting, amending or deleting information disputed by the individual. The individual must request the correction, amendment or deletion in writing. Once the insurer, insurance producer or insurance support organization researches the matter, they must correct, amend or delete the information if they find such action should be taken. If the insurer, producer or support organization determines that a correction, amendment or deletion is warranted, the individual must be notified, and the change must also be provided to any *1) person specifically designated by the individual who may have received the information in the previous two years; 2) any insurance-support organization that has systematically received such information over the preceding seven years, unless the organization no longer maintains information on the individual; and 3) any insurance support organization that supplied the information that has been changed.* If the insurer, producer or support organization does not change the information based on the individual's request because it does not believe such a change is warranted, the individual has the right to file a *concise statement* disputing the information in question, and the statement must be provided to anyone who reviews the information.

Section 10, 11 and 12 deal with the circumstance of *adverse underwriting decisions*. Under the model Act, an adverse underwriting decision is a denial of insurance, a termination of coverage, or the failure of an agent to apply for a coverage that the applicant requested. Under property and casualty insurance, *adverse underwriting decision* also includes the placing of coverage with a residual market mechanism or with an insurer specializing in substandard risks, or the charging of a higher rate on the basis of information that differs from the information provided by the applicant or policyholder. Under life, health and disability insurance, an adverse underwriting decision also includes offering to insure the applicant at a higher than standard rate.

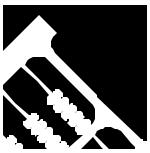
Under Section 10 of the model Act, the applicant or policyholder must be informed that he or she is able to request reasons for an adverse underwriting decision. The individual also has the right to obtain the specific information and the sources of information that support the reasons for the adverse underwriting information The individual must also be informed of his or her right to dispute the information, as was discussed above in the information related to Section 9 of the Act.

Section 11 of the model Act gives insurers, insurance producers and insurance support organizations, the right to information about an individual regarding previous adverse underwriting decisions or any previous coverage obtained through a residual market mechanism and the reasons for the adverse underwriting decision or coverage through a residual market mechanism.

Under Section 12, an insurer or insurance producer may not base an adverse underwriting decision on a prior adverse underwriting decision of another insurer, or because the applicant was placed in a residual market mechanism by another insurer. This Section also prohibits an underwriting decision to be made on information received from insurance support organizations whose *primary source of information is insurance institutions.* Rather, the insurer or producer must investigate and verify that the information is accurate before it may be used in an adverse underwriting decision.

Section 13 provides that the insurer, insurance producer or insurance support organization may only disclose personal or privileged information if the subject individual has provided written authorization to do so, or if the disclosure is for the purpose of protecting against fraud, providing required information to state regulators or other governmental bodies, providing information due to a potential sale, transfer, merger, or consolidation, or other business purposes. If information is used for a research report, identification of the individuals whose information is utilized is not allowed in the report, and the researchers must return or destroy materials used during the research process that identifies individuals. If information is disclosed for marketing purposes, it may not include medical, privileged or personal information regarding the individual's reputation, mode of living, habits. Under the model Act, individuals may stipulate that they do not want any personal information disclosed for marketing purposes.

Also under the model Act, if the insurance commissioner of the state determines that a party has violated any portion of the Act, the commissioner may issue a cease and desist order. The Act calls for a penalty of $500 for each violation, to a maximum of $10,000. If a cease and desist order is violated, a penalty of $10,000 may be assessed. In addition, an insurer or producer that commits a violation may have its license suspended or revoked.



THE INSURANCE AGENT & CLIENT PRIVACY

Protecting Confidentiality

The insurance industry has worked with personal information for a long time. One of its top priorities has been to protect the confidentiality of that information. The insurance agent understands that the *consumer demand* for new and affordable financial and insurance products is met efficiently when the consumer is willing to share information. He also knows that consumers *desire* to protect their privacy. The agent faces the challenge of reconciling these two demands:

- Convenient, speedy service of new and affordable financial and insurance products
- Protection of the consumer's privacy

An insurer should establish and maintain policies and practices to protect the confidentiality and security of financial information. He should also provide customers with a notice of his company's privacy policies at the beginning of the business relationship and continue to do so for at least once a year. Customers should be given the opportunity to direct that financial information not be shared for marketing purposes, unless the products and services being marketed are being offered through an affiliated institution.

Clients should be given access and correction rights to their financial information. The insurance company should have a provision that affirms its right to share financial information when it is necessary to issue contracts and to service its business.

The life insurance industry believes that medical information should be subject to far greater restrictions than financial information. Life insurers have a long history of dealing with highly sensitive personal information. They have always protected consumers' medical information, and they will not depart from that tradition. They recognize consumers have special concerns regarding medical information. That is why the life insurance industry has adopted a broad and definitive statement of principles regarding the confidentiality of policyholders' medical records.

Nonpublic personal information is personally identifiable information that a consumer gives to an agent or broker. It can also be information that an agent or broker obtains from a transaction with the consumer or any service performed for the consumer. It can include a list, description or other grouping of consumers.

GLBA requires that insurance agents and brokers respect the privacy of consumers and customers by protecting the security and confidentiality of the nonpublic personal information. GLBA does make a distinction between a **consumer** and a **customer**. Every individual having dealings with an agent or broker is a consumer but only consumers with a specific of ongoing relationship with the agent or broker are customers. GLBA requires insurance agents to provide initial and annual privacy notices and opt out notices to **all customers**. It also requires the agent to sent notice to non-customers only if the agent intends to disclose the consumer's information to unaffiliated third parties.

Compliance with Privacy Laws

Insurance companies should seek to find a commonsense approach to implementing the new privacy laws in a way that assures consumers adequate notice of privacy policies by insurers without requiring members to duplicate their companies' privacy notices. This approach will save agencies thousands of dollars each year in postage and other mailing costs, as well as thousands of hours of agency staff members' time.

The privacy rules apply to any person or entity that is licensed or otherwise authorized to conduct business by their State Department of Insurance. However, an agent that discloses protected financial information only to the insurance company on whose behalf the information was collected does not have to comply with the notice and opt out requirements so long as the company itself complies with the notice requirements

If the agent shares the information with anyone other than an insurance company, the agent must provide separate notices and opt out opportunities as required by the rules In addition, if an agent, for a fee, provides any other services to an individual such as financial, investment or economic advisory services relating to an insurance product, that individual becomes the agent's customer and must be provided with all required notices about the agent's privacy policy and, if the agent plans to share information with any third party, the opportunity to opt out.

It will be up to the company and the agent to determine who will provide the notice on behalf of the company. The initial notice required by the rules must be given as soon as a person becomes a customer. Some companies may require the agent to provide the initial notice. In that case, it will be the company's responsibility to provide the agent with the notice form to be used. However, after that, it is expected that most companies will probably maintain responsibility to provide follow up and annual notices required by the rule.

As stated previously, the privacy rules apply to agents. However, the rule provides that an independent agent sharing information with multiple insurance companies in order to obtain the best price quote for a client does not need to provide notices to the client. It is the responsibility of each insurance company to comply with the notice requirements as to that client. Note that under the rules, the client will be considered a consumer of each company to whom the client's information is provided, and if the client purchases coverage from one of the companies, the client becomes the customer of that company. However, if the agent discloses or plans to disclose that information to anyone other than the companies, the agent must send that client all required notices and provide the client with the opportunity to opt out.

Because each agency's operations are different, and because the law is designed to reflect all of the different types of information sharing in the marketplace, there is no one single privacy notice agencies can use to comply with the federal law. Each agency will need to develop its own internal privacy policy and consumer privacy notice.

Conflicts

While privacy rules are being refined, there are several issues that represent potential conflict for agents:

For example, the privacy rules under HIPAA state that items such as a person’s name, address, social security number and payment history are protected “health information” subject to an ***opt-***

in standard. Therefore, HIPAA would prohibit any sharing of this information with a third party unless an express release is signed by your client. Many states, however, would consider these same items as "financial information" subject to ***opt-out standards*** where the sharing of client information is allowed until he "opts-out".

Another potential conflict might arise where you might be trying to assist your client by communicating with a third party such as a pharmacy or some aspect of claims processing with an out-sourced company. Be very careful that you have disclosed your intentions to share personal financial and health data or obtained client authorization to do so.

Also be cognizant of privacy law language to avoid potential problems. For example, some rules indicate you should have client ***consent*** to share their nonpublic information; others require ***authorization***. There is a considerable difference! (See page 96).

Semantics become yet another potential conflict when you compare privacy rules that indicate that agents are exempt from disclosure when working on behalf of a compliant carrier; yet, DHHS regulations seem to say that the assessment of whether an entity is covered is more a function of use rather than definition. They exempt, for example, the sharing of client data for treatment, payment and health care operations. Nothing was said, however, about underwriting. Are you exempt?

These potential conflicts are ALL good reasons to develop and maintain a good privacy policy – just in case!

Developing a Privacy Policy

The most important step an insurance agent can take toward satisfying the GLBA privacy rules is to develop a detailed policy for handling nonpublic personal information. In developing a privacy policy, an agency should remember that the disclosure of the policy might be treated as a contract between the agency and its clients. In addition, an agency should consider taking the following steps when developing its privacy policy.

The agent should consider including an alternative dispute resolution provision that could help to reduce the costs of defending against future challenges. He should also consider consolidating multiple privacy policies into a single disclosure form in order to avoid confusion and conflicting obligations.

The insurance company should organize quality assurance programs to ensure that each customer is given the requisite notice and that all other elements of its policies are maintained and followed at all times. The privacy policy may create new liabilities for the company. The agent needs to be sure that his company's errors and omissions insurance is adequate to address these issues.

International Privacy Issues

As e-commerce expands in our global economy, insurers need to focus on the development of privacy law internationally. Many times foreign countries have more restrictive laws than the United States in terms of imposing specific privacy obligations. They have been imposing statutory or administrative obligations while large parts of the American economy have been operating on self-regulation privacy.

Safe Harbor Principles

There has been a lot of debate about the European Union privacy rules. Its directive prohibits exports of person data from the EU to countries such as the United States that do not provide adequate privacy protection. Therefore, American companies that receive information from Europe must be prepared to meet the European Union directive, or otherwise be prepared to meet the safe harbor principles that have been developed to allow the continuation of current activities. The safe harbor principles seek to establish a uniform standard of adequacy for U.S. recipients of data within the scope of the European Directive. These principles are still being developed. Insurers that receive information from Europe will need to demonstrate that they meet the safe harbor principles.

Notice ~ The insurance company must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the agent or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

Choice ~ The insurance company must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.

Onward Transfer ~ The insurance company may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles

Security ~ Companies that are creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity ~ The insurance agent may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, he should take reasonable steps to ensure that data is accurate, complete, and current.

Access ~ Individuals must have reasonable access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate.

Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.

Enforcement ~ The company's privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. Insurers that exchange any information with European countries concerning American or European citizens must be sure that they are following these guidelines.

Marketing Personal Information

The goal of privacy regulations is to give consumers an affirmative opportunity upfront to decide whether they want their information shared or not for marketing purposes. The consumer is to be given the opportunity to opt-in or opt-out, because once their information is disclosed, it will be very difficult to re-protect the information. The purpose of these regulations is not to prohibit companies from offering products, or to prevent insurers or doctors from participating in disease management activities or from mailing appointment reminders or other information to consumers. They are not trying to keep consumers from getting helpful information.

Misrepresentation

While we are on the subject of rules, it is important to realize that representing yourself as someone or something ***other than who you are*** in order to obtain personal financial information can also be a violation of privacy laws. Consider, for example, the case of a marketing scheme known as a "living trust mill". Agents in California were involved in soliciting senior citizens at seminars, purportedly to design and educate about the benefits of a living trust. In other words, representatives misrepresented themselves as experts in estate planning. In fact, their true goal was to discover the extent of client assets in order to sell them annuities. The insurer and its agents were found guilty of deceptive training practices and violating provisions of the Insurance Information Privacy Act. Don't let this happen to you!

AGENT DISCLOSURES AND CLIENT PRIVACY

Privacy Terms

To best understand client disclosure requirements, let's first define some terms that are part of the privacy regulations:

Affiliate: A company that controls, is controlled by or is under common control with another company. For instance, under the Gramm-Leach-Bliley Act, insurers and banks can become affiliates. Affiliates may also be parent companies owned by your agency or common companies under the same holding company structure.

Consumers: Individuals who are seeking to obtain a product or service from an insurance company through your agency are called ***consumers***. For example, an individual who has submitted an application for insurance is a consumer of the company to which he has applied. A prospect for your products and a beneficiary or claimant under an insurance policy are also considered to be a ***consumer***.

Customers: These are consumers with whom you and your insurer have an on-going relationship or those who obtain financial, investment or economic advisory services relating to an insurance product or service from you for a fee. People who buy policies and investments, from you are ***customers***.

Covered Entity: Financial privacy rules require that all "covered entities" issue or provide privacy disclosures. Covered entity includes any individual or entity that receives authorization from the Department of Insurance.

Insurers: This class includes insurance companies, financial institutions or other entities required to comply with the privacy regulation.

Licensees: These are individuals regulated by the Department of Insurance. All licensees are required to comply with privacy disclosures unless exempt.

Nonaffiliated third party: This is a company that is not affiliated with an insurer, agent or agency.

Nonpublic personal information: Nonpublic personal financial information is information that identifies an individual member. It may include an individual's name, address, telephone number and social security number, or it may relate to an individual's ownership of a policy, the provision of insurance services or the payment for insurance services. Nonpublic personal financial information does not include publicly available information, or statistical information that does not identify individual persons.

Opt-Out: The general rule is that information about a person will be shared unless the person notifies the holder of information that he wants his information protected. To "opt-out" is to put an agent or company on notice that a customer prohibits his personal financial information from being shared with non-affiliated third parties.

Opt-In: Under an "opt-in" standard, the general rule is that protected information is not shared unless the person who is the subject of the information signs an authorization or consent that expressly permits the sharing of his protected information with a third party.

Privacy Policy Statement: A disclosure form handed to clients or posted on a website that describes an agent's intention to share or not to share any nonpublic information about his clients with a non-affiliated third party. Statements may describe the personal information typically collected in the process of providing insurance, a list of non-affiliated parties who may share nonpublic information, a notification right for the client to "opt-out" (an instruction the agent not to share this information), normal practices concerning confidentiality and security for any nonpublic information collected, policy concerning dispute resolution, the right to sell information when the agent's business is sold or transferred, the right to change the stated privacy policy and a place for clients to acknowledge the privacy policy disclosure.

General Client Privacy Rules

For Consumers:

Licensees may not disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless permission is granted by the consumer.

Licensees must provide consumers a privacy policy and an opt-out notice along with a reasonable time to opt-out prior to the sharing of information.

Licensees may not disclose any nonpublic personal financial or health information about a consumer to a nonaffiliated third party, unless:

- The consumer received a notice prior to the disclosure
- The consumer received an explanation of the opt-out procedure
- The consumer had a reasonable opportunity to opt-out prior to disclosure and
- The consume did not opt-out

The GLBA notice obligation requires all insurers and financial institutions (including insurance agents) to provide an understandable notice of their privacy practices to their customers when a customer relationship is established and at least once a year thereafter. This obligation does not require agencies to adopt specific information handling practices. It only requires that they disclose the practices in which they engage. In other words, most agents can satisfy client privacy requirements by issuing or posting a simple disclosure form (two samples are provided below).

For Customers:

A customer must be given an annual notice of the licensee's privacy policies and practices until such time as the customer relationship terminates.

A licensee may not disclose any nonpublic personal information about a customer to a nonaffiliated third party unless a notice is provided.

A privacy notice must contain a description of privacy policies ad practices, an opt-out notice, and a reasonable time to opt-out prior to the disclosure of information.

Licensees may not disclose any nonpublic personal financial or health information about a customer to a nonaffiliated third party, unless:

- The customer received a notice prior to the disclosure
- The customer received an explanation of the opt-out procedure
- The customer had a reasonable opportunity to opt-out prior to disclosure an
- The customer did not opt-out

Exemptions

In general, most federal and state privacy regulations apply to agents. However, an agent does not have to comply with special disclosures and opt-out requirements if:

- The agent is appointed with a company or designated with an agency (principal) that complies with, and provides all of the notices required by the regulations, and

- The agent does not disclose protected, personal financial information to any person othr than the principal or its affiliates.

In other words, if an agent wishes to disclose a consumer or customer's protected information to an entity other than the insurance company with which the agent is appointed, or the agency with which the agent is designated, the agent must give the consumer a copy of the agent's privacy notice and an opportunity to prohibit the disclosure of that information to non-affiliated parties.

In theory, this would seem to exempt most agents from the disclosure requirements. However, the question remains, are the principals (your insurer or agency) making the required disclosures in the necessary format? Can you rely on them to make them annually where needed? Any doubts? Use your own disclosure.

Required Recipients

Unless the underwriter or insurance agency qualifies for the special agent exception, they must provide a privacy notice to any individual who purchases a financial product or service through that agency that is to be used primarily for personal family or household. All **customers** are entitled to receive a GLBA privacy notice at the beginning of the customer relationship.

A privacy notice must also be provided to all **consumers** if the agency is going to share their information with a non-affiliated organization. If the agency is not going to share the information of its consumers with a non-affiliated organization, it does not owe the consumer a privacy notice.

Required Disclosure Information

In most instances, federal and state privacy regulations do not make specific requirements about the type of privacy policy that an insurance agency must use. It only tells them what facts it must disclose. The disclosure must be clear and easy to find. It must be understandable and designed in a manner that calls attention to it. A disclosure will be easy to find, read, and understand if it uses short and clear explanatory sentences or bullet lists in simple language.

Here is a short list of features you might include in your privacy notices:

- Categories of nonpublic personal financial information collected.
- Categories of nonpublic personal financial information collected.
- Categories of affiliates and nonaffiliated third parties to who information is disclosed, except as part of an insurance transaction.
- Categories of nonpublic personal financial information about former customers disclosed and to whom disclosed.
- Categories of information disclosed and to whom disclosed as a result of contractual relationships or servicing or joint marketing.
- Explanation of consumers' right to opt-out of disclosure of his nonpublic personal financial information to nonaffiliated third parties and the methods to utilize to opt-out.
- Policies and practices for protecting the confidentiality and security of nonpublic personal financial information.
- If making disclosures (information about customers) as part of insurance transaction, that the licensee makes disclosures to other affiliated or nonaffiliated third parties, as permitted by law.

The disclosure must include the types of nonpublic personal information that the agency collects. This would describe the nature of the information collected and the way in which it is collected. The disclosure must also mention the types of nonpublic information that may be disclosed and the categories of affiliates and non-affiliated third parties to whom the disclosures may be made.

The agency must describe in the disclosure its policies and practices in sharing nonpublic personal information about former customers and consumers. If these policies and practices are the same for both groups, the same clauses may be used for both.

The notice must list the categories of nonpublic personal information disclosed according to agreements with third party service providers and joint marketers, and the categories of third parties providing the services. The notice must disclose the consumer's right to opt out of the disclosure of nonpublic personal information to non-affiliated third parties.

The notice must include any disclosures regarding affiliate information that the agency is providing. The notice must disclose the agency's policies and practices in protecting the confidentiality, integrity and quality of the nonpublic personal information it collects.

Required Distribution

The insurance agency must disclose its privacy policy when a customer relationship is established and once a year thereafter. There are different ways of providing the initial notice to customers.

The agency may choose to provide their own notice. They may provide a joint notice to the customer that represents both the carrier and the insurance agency. They may give the carrier's notice to the individual.

Regardless of which option the agency chooses, the initial notice can be provided when a purchased policy is delivered or when an agreement to provide other insurance services is

completed. The notice itself can be given along with other materials that an agency delivers to the customer such as with a bill for premiums.

The annual notice may be delivered in the same way. GLBA does not require the insurance agency to provide the annual privacy notice to a former customer. Agencies that provide title insurance or other real estate settlement services in which the contact with the insured is limited to the time when the policy is sold are not required to deliver the annual privacy notice.

Agencies who sell group insurance policies are required to deliver a privacy notice to the plan sponsor. They do not need to deliver a notice to plan participants as long as they do not disclose the participants' personal information to non-affiliated organizations.

Financial Privacy Questions and Answers

The following are general questions and answers concerning privacy notices. Please bear in mind that your individual state may have their own specifications that may meet or exceed these requirements. Also, do not act on these answers in personal or client matters unless you first check with a competent professional and/or company superior.

Do agents need privacy policies?

Yes. Agents are financial institutions and should have privacy policies in compliance with GLBA. However, keep in mind that an agent is exempt from the notice and opt out provisions if the conditions set forth in the definition of "licensee" are satisfied.

I'm a paid representative of one insurance company and I only represent that company and its line of insurance and financial services products. What are my responsibilities under this new privacy rule?

You are subject to the regulation, but you are not required to comply with the notice and out-out requirements of the regulation if:

- The company with which you are appointed complies with the regulation; and
- You do not disclose protected information to any person other than that company or its affiliates.

I'm an independent agent and therefore represent a variety of insurance companies. What are my responsibilities under the privacy rule?

Just like other agents, you are subject to the regulation, but you are not required to comply with the notice and out-out requirements of the regulation if:

- The company or companies for which you are appointed or the agency with whci you are designated, with respect to a particular consumer or customer complies with the regulation; and
- You do not disclose protected information to any person other than that company or companies, agency or affiliates of that company or agency.

I'm an independent agent and need to share consumer information with many insurers in order to get the best prices for my clients. Is this permissible under the privacy regulations?

Yes, an agent may share nonpublic personal financial information with multiple companies in an effort to compare prices at the consumer's request. In such situations, the individual will be a consumer of each of the companies and will be entitled to privacy and opt-out notices from any of the companies that wishes to share the individual's protected financial information with non-affiliated third parties.

What about disclosing personal health information?

NO. The notice provisions of the privacy regulation do not cover health information, In most states, an agent may not disclose the nonpublic personal health information of a consumer or customer to an affiliate or non-affiliated third party unless an authorization is given from the individual whose information is sought to be disclosed. An authorization to disclose nonpublic health information must include:

- The identity of the consumer or customer.
- A description of the type of information to be disclosed.
- General descriptions of parties receiving the information.
- The consumer's or customer's signature.
- The length of time the authorization is valid and the procedure for revoking the authorization.

Do I have to go back to every one of my existing clients and tell them about this new privacy rule?

Maybe. You're required to provide privacy and opt-out notices to a client if the client is considered your "customer". However, if you are appointed with a company or designated with an agency that is meeting the privacy regulation and you do not disclose protected information, you are probably exempt.

Every company is different. Of the companies I represent, how am I supposed to know which ones send out notices?

Like all aspects of the agent-agency or agent-company relationship, effective compliance with privacy regulations will require on-going communication and coordination between the parties.

What if one or more of my clients didn't receive a notice from a company? Who is responsible?

In general, a failure to provide a required notice is a violation of agency rules subject to enforcement by the Department of Insurance. In addition, enforcement action for unfair trade practice can also be taken. An individual whose information has been share in violation of the rules may also bring civil action against a covered entity regardless of any action taken by the State. Specific compliance violations will most likely be decided on a case-by-case basis.

The bottom line? <u>It is the responsibility of YOU, the agent, to determine whether the company's or agency's notice is sufficient to exempt you from providing your own notification.</u> If, on the other hand, your standard procedure is to provide a privacy notice to every client, you would have a good argument that you are NOT responsible for the company's omission.

I am an agent who NEVER intends to disclose or share my client's personal financial information with anybody except my own company? Do I still need a privacy notice?

As long as your company provides responsible and proper notices, you are probably exempt. However, why not provide a simplified notice that spells out the types of personal financial information you collect in the process of selling insurance, your policies and practices with respect to protecting the confidentiality of nonpublic personal information and a statement that the disclosures made to affiliated or non-affiliated parties are permitted by law. In any case, you can promote customer goodwill by doing so. And, if all or most of your competitors provide privacy notices and you don't, will your clients begin to wonder why?

What about phone-in requests for information on insurance products. Do we have to tell these callers the privacy policy of each of the company?

Not normally. If these individuals are simply requesting information and not purchasing a product, they are likely to be considered consumers. However, at the point where you collect nonpublic personal financial information and you are going to share it with a non-affiliated third party, you will be required to provide a privacy and opt-out notice. If you do not intend to share the protected information, it is not necessary

When the individual actually purchases a product from you over the telephone, he is considered a customer. Normally, customers are entitled to privacy and opt-out notices at the time the customer relationship is established. With a telephone transaction, however, delivery of notices can be delayed with customer consent.

The same obligations would apply to the companies fr which you are appoint as an agent.

I'm an independent agent and I perform servicing and processing functions for several insurers. Does the exchange of private information require notification?

No. An insurer can share nonpublic financial information with agents acting as service providers or third parties that perform services for the company or functions on the company's behalf. The only requirements are that the company must provide an initial notice to the individual, and, where third parties are involved, must enter into a written agreement prohibiting the third party from using the information other than to carry out the purpose for which it was intended. Of course, reuse and redisclosure provisions apply to the company.

Is the agent an affiliate of the company for which it is acting as agent?

No.

Can an insurance company share information for marketing purposes with its agent?

Yes, a company can share information for marketing purposes about a particular individual for whom the agent is acting as agent. In this situation, the agent would not be the company's service provider and would not have to enter into a confidentiality agreement.

Can an agent share information for marketing purposes with a company for which it is acting as agent?

Not unless such information sharing has been disclosed to the consumer through either the company's or the agent's privacy notice.

If an agent discloses information to a non-affiliated third party, does he have notice and opt out obligations to the consumer/ customer? In other words, by such disclosure does the agent lose the exemption gained under the "licensee" definition?

No, if the disclosure is within the scope of its agency relationship with the principal and the agent complies with the privacy notice provided by the principal to the consumer. However, the agent loses the exemption if the disclosure is made for the agent's own purposes.

How long does a customer's request to "opt-out" last?

An opt-out is effective until the customer r consumer revokes it in writing.

Are brokers subject to the agent exemption definition of "licensee"?

In many states, brokers are considered "producers" and treated like agents for purposes of the privacy regulation. In most cases, an insurance broker or who can demonstrate that they were a representative of the principal would be subject to the agent exemption.

Are independent adjusters treated like agents?

Yes.

Does agent exemption apply when business is through a clustered arrangement or broker?

Yes.

Does agent exemption apply when agency assets are sold, but not the business?

Yes.

Can an agent share with its affiliates or just the principal's affiliates? Does it matter if the agent's affiliate is a bank?

Agents who are taking advantage of the exemption in the "licensee" definition may disclose nonpublic personal financial information only to the principal and the principal's affiliates. If the agent chooses to disclose to its affiliates, the agent is subject to the notice provisions of the regulation.

What does a privacy notice look like?

We have provided two samples below for your review and inspection by a competent professional. In a nutshell, the notice must be clearly written and conspicuous ad contain information about the types of information you collect, how it is normally protected, what might be disclosed to a third party and who they are and an opportunity to opt-out of any sharing.

Where can privacy notice be disclosed (application, prospectus, newsletter, renewal notices, direct mail, with opt out notice)?

Generally, this issue must be decided on a case by case basis. If a licensee is unsure as to whether its manner of distribution for privacy notices is acceptable, the licensee should discuss

with the regulator. If the licensee operates in several states, the licensee should discuss with the regulator of each of these states. Keep in mind that the model privacy regulation provides that a privacy notice can be disclosed in a prospectus or newsletter or sent with a renewal notice, direct mail campaign or opt out notice.

Can I send privacy notices, opt-out notices and health information authorizations together in the same mailing? Can they be sent with other customer mailings?

Privacy, opt-out and health authorizations notices can be sent together or separately, and they can be sent with other customer mailings. In addition, affiliated companies may send notices together, or they can send combined notices. No matter how they are sent, however, all notices must identify the companies and policies to which they apply. They must be accurate, and they must be clear and conspicuous so that the customer can read and understand them.

If my customer is conducting some personal business, say at his attorney's office, and calls my office to fax over a copy of his policy to the attorney, would this be an exception under the privacy rules?

Yes, a notice and opportunity to opt-out of the sharing of consumer's information would not be necessary, as the agent is sharing the information at the consumer's request. However, it might be a good idea to note the client's file about the request.

If a customer's policy is subject to renewal, can I request quotes from various insurance companies in an effort to shop the coverage without providing notice to the customer and an opportunity to opt-out?

Yes, if the customer has requested the shopping of his insurance coverage. If the customer has not requested renewal quotes, his information cannot be shared with companies unless a privacy notice and opt0out has been provided.

What if I'm asked to share a client's personal financial information with the Department of Insurance?

It's ok. Sharing information with regulatory authorities has jurisdiction over company or agent disclosures.

Can licensees require consumers/customers to disclose social security numbers in order to opt out (or opt in)?

Requiring a consumer's social security number in order for that consumer to exercise the consumer's opt out right is inconsistent with the language and the intent of the model regulation. Although an opt out notice can include a request for a social security number, compliance with such request must be optional on the part of the consumer. In addition, the fact that it is optional must be disclosed to the consumer, and an opt out notice without a social security number must be treated as a valid exercise of the consumer's opt out right. If a voicemail system or other automated response system is used for exercising the opt out, it must be accessible without the consumer/customer having to provide a social security number.

Who gets the notice when the policyholder of an individual life policy is different from the insured?

The policyholder is a "customer" of the licensee as that term is defined in the model regulation and is therefore entitled to receive initial and annual notices. An insured is a "consumer" of the licensee if the licensee discloses nonpublic personal financial information about the insured to a nonaffiliated third party. An insured that is a consumer is entitled to initial notice and the opportunity to opt out.

How does the new regulation impact the disclosure of information about beneficiaries?

A beneficiary of a life insurance policy is considered a consumer under the regulation if you disclose or share any protected information. As a consumer, the beneficiary is entitled to a privacy notice and opportunity to opt-out of the disclosure. If you do not share nonpublic personal information about beneficiaries with non-affiliated third parties you have no obligation to notice them.

Does access to third party claimant information give rise to privacy obligations for agents?

A claimant under any insurance policy is considered a consumer under the regulation if you disclose or share any protected information. As a consumer, the beneficiary is entitled to a privacy notice and opportunity to opt-out of the disclosure. If you do not share nonpublic personal information about claimants with non-affiliated third parties you have no obligation to notice them.

Insurers may give agents access to records that contain third party claim information for the agent's client. Access to such information does not give rise to any privacy obligations beyond the general obligation to protect the confidentiality and security of personal information. However, such information could not be disclosed to non-affiliated third parties outside the exceptions without giving notice and opportunity to opt out.

My appointed company provides on-going settlement option for beneficiaries and claimants. Is that person a consumer or customer?

Beneficiaries and claimants that submit a claim under a policy choosing a settlement option involving an on-going relationship with an insurer are considered consumers not customers. Thus, the company and agent will be required to provide the individuals with privacy notices and an opportunity to opt out.

Are HMOs required to send initial notice/opt out to subscribers and dependents?

For individual coverage, yes. The definition of "licensee" encompasses HMOs even in states that do not regulate HMOs as insurers. Group HMO coverage, however, is regulated like any other group plan, if an HMO sends initial and annual notices to the group policyholder and does not share any nonpublic personal financial information outside the exceptions to the rule, then the HMO has no notice/opt out obligations.

Do notice and opt out provisions apply to single premium policies and paid-up policies?

The privacy notice and the opt out notice do not have to be provided to paid-up policies or single premium policies if there has been no contact with the policyholder within the last twelve months prior to July 1, 2001. These policies are typically considered "dormant." Similarly, if the policy becomes paid-up or a consumer purchases a single premium policy after July 1, 2001, notice

must be provided until there is no longer contact outside of providing a privacy notice or opt out notice with the policyholder for twelve months.

I am a licensed insurance agent and I sell variable annuities. Am I required to comply with the privacy rule?

You are subject to the regulation, but you are not required to comply with the notice and out-out requirements of the regulation if:

- The company with which you are appointed complies with the regulation; and
- You do not disclose protected information to any person other than that company or its affiliates.

Are health insurers required to comply with GLBA and the financial provisions of the model regulation (notice and opt out) if they only have identifying information (name/ address/ social security number) that, by itself is not financial or health information?

Health insurers would be hard pressed to prove that they do not possess nonpublic personal financial information. For example, unlisted telephone numbers and social security numbers are nonpublic personal financial information. This information cannot be disclosed outside the exceptions unless the consumer has been given notice and the opportunity to opt out.

Are large employer groups (50+ plans under ERISA) required to send notice and opt out to consumers/customers? In other words, is an insurer that provides coverage to the ERISA group required to comply with the privacy rule with respect to information gathered from the large group?

Yes, to the same extent as any other groupholder. The privacy regulation is not preempted by ERISA.

Could there ever be a situation in which a group plan shares information outside the exceptions (thus giving rise to notice and opt out requirements), but the group plan does not have enough information about the individual to contact him? Could this scenario arise with claimants/beneficiaries?

This is an unlikely scenario, but if such a situation were to exist, the group holder must take reasonable measures to obtain enough information to contact the individual.

Is a privacy notice permitted under section to the workers' compensation policyholder?

The workers' compensation plan participant is the workers' compensation policyholder. Notices may be sent to such policyholders.

How do I determine if the privacy notice regulations apply to a particular professional or institution?

Ask the following three questions: (i) is the professional or institution a licensee? (ii) is the licensee providing an insurance product or service? (iii) is the licensee providing the insurance product or service to a consumer? If the answer to these questions is "yes," the regulation clearly applies.

It may be difficult to determine if the individual is a "consumer" of the licensee. In such situations, if the licensee is acting as the individual's insurer and holds nonpublic personal information about the individual, the licensee is required to comply with the regulation.

All commercial lines are subject to the regulation for individual non-commercial claimants. Specific examples include: TPAs (licensed; unlicensed; TPAs for self-insured plans); MGAs; Charitable annuity societies/donor annuity organizations; Service contract providers; Prepaid health services plans; Premium finance companies (if policy placed for personal use); Independent adjusters of worker's compensation claims; Financial guaranty insurance; Title insurance; Surety bonds (if bond placed for personal uses).

Interestingly, viatical settlements, key man insurance and business auto policies are excluded. As are personal umbrella policies, professional liability coverages and most they are commercial lines that are not used for personal, family or household purposes.

In essence, if nonpublic personal information is collected in the underwriting of such policies, such information is not protected under the regulation.

A TPA that is not required to be licensed is providing services to a partially self-funded group with stop-loss reinsurance from an insurer who says the stop-loss contract is not a group plan. Is the broker/agent on the stop-loss required to send notice to the plan/group sponsor or employer? What if agent/broker has no protected information?

If the stop-loss insurer or producer holds nonpublic personal information about covered employees, the stop-loss insurer is "acting as an insurer" for the employer, and must treat the employer like any other group policyholder under the regulation: if the stop-loss insurer sends initial and annual notices to the group policyholder and does not share any nonpublic personal financial information outside the exceptions to the rule, then the insurer has no notice/opt out obligations. The stop-loss producer might be able to rely on the agent exemption if it meets all the requirements. In this scenario, the TPA is not required to be licensed and therefore is not subject to the regulation.

A trust hires a broker to find group health coverage for employees. The broker goes to an independent agent to find coverage. Is the independent agent a "service provider"?

No.

In cases involving a sub-producer, general agent and an insurer in the placement of a risk, must all provide the privacy notices?

The agent exception in the "licensee" definition applies in this situation in cases in which a policy is run from the sub-producer through the general agent to the insurer.

Under what circumstances is a licensee considered to be working as an agent/employee/other representative of another licensee and can therefore rely on the principal licensee's notices to customers and consumers instead of issuing his/her own notices?

Determining whether an agent/employee/other representative of a licensee can rely on the exception in the "licensee" definition depends on what that agent/employee/other representative

is doing for the licensee. It is a factual determination requiring analysis on a case-by-case basis.

If a licensee is considered to be an employee, agent or representative of another licensee for compliance purposes, is the licensee then able to operate under the disclosure exceptions of the regulation?

Yes, an agent/employee/other representative can operate under both the "licensee" exemption and the exception. Under the standard interpretation of the agent/principal relationship, agent can act on behalf of the principal, with the same powers, and the same limitations on powers, as the principal. If the agent discloses nonpublic personal information outside those limits, the agent must comply with the notice and opt out requirements of the regulation.

Can licensee share health information with its affiliate if both licensee and affiliate are working on same claim?

Yes, to the same extent as any other party providing claims services.

In one state, insurers are refusing to give hospitals claim information claiming that disclosure is prohibited under GLBA and state privacy rules. True?

It depends on the reasons the hospitals are requesting claim information. When in doubt, get authorization.

Once a licensee is in compliance with the HHS privacy regulation (and is then deemed "in compliance"), does the state or HHS enforce? Who enforces against a licensee that is not subject to the HHS regulation but chooses to comply with that regulation rather than the model regulation?

Because the HHS privacy rule is incorporated by reference into the regulation, the state and HHS have concurrent jurisdiction when the licensee is subject to the HHS regulation. The state has exclusive jurisdiction if the licensee is not subject to the HHS regulation and is complying with HHS standards for the purpose of satisfying its obligations under the regulation.

Does the regulation permit disclosure of account numbers used among companies in affinity plans?

Yes.

May companies share nonpublic personal financial information for policyholder service functions or for purposes of risk management and loss control (e.g., loss runs) under the business purpose exceptions?

The phrase "policyholder service functions" is too general to determine whether or not a specific function falls under the initial notice and opt out exceptions. More information is needed to make that determination.

Risk management and loss control would both fall under general servicing and processing exceptions

What our my obligations if I receive nonpublic personal information from another entity?

Your use and disclosure of that information is limited to the original financial institution who gave it to you; affiliates; or to any other excepted entity.

I receive information from banks and securities firms that are themselves subject to privacy regulations. What rules do I follow?

Most institutions must abide by reuse and re-disclosure of protected client information. Generally, these rules permit you only to share nonpublic information with the original financial institution you received it from.

Can my company charge lower rates to policyholders that permit their information to be shared?

No. Premium rates cannot be based on an individual's choice to prohibit or allow the sharing of his information. However, this does not prevent a company from offering discounts for other reasons. What reasons? Well, we all know that insurers cannot discriminate against a consumer for prohibiting the disclosure of their personal information by raising rates or dropping coverage. However, the same insurer does not have to offer them the special offers that might be available to customers who permit their personal information to be disclosed.

Sample Privacy Disclosures

To aid agents understand features and wording of required privacy disclosures, we are providing an actual sample.

IMPORTANT: Prior using any information or disclosure form, consult with a competent attorney or professional before using these forms in personal or client matters.

Sample Disclosure #1

Purpose of This Notice

As provided by law, we are generally prohibited from sharing nonpublic personal information about you with a third party unless we provide you with this notice of our privacy policies and practices describing the type of information that we collect about you and the
categories of persons or entities to whom that information may be disclosed. Accordingly, we are providing you with this document, which notifies you of the privacy policies and practices of (agency).

Furthermore, we wish to inform you that we do not share your personal information with any non-affiliated third parties for any purpose that is not specifically authorized by law unless we obtain your affirmative permission.

Privacy Policies and Practices

Information we collect:

We collect non-public personal information about you from the following sources:

- *Information we receive from you on applications for insurance or from other insurance forms you complete.*
- *Information we receive from the companies we represent which provide insurance policies to you.*
- *Information from consumer reporting agencies.*
- *Information about your transactions with us, the companies we represent.*
- *Information from other sources, such as employers or government agencies.*
- *Information from visits to our Website.*

The type of information we collect is related to the insurance you requested from us and may include your name, address, social security number, driver's license number, ownership of property, marital status, health information, and other information required to get insurance coverage for you.

Unless it is specifically stated otherwise in an amended Privacy Policy Notice, no additional information will be collected about you. We may collect nonpublic personal information from individuals other than those proposed for coverage.

Information From Credit Reports or Investigative Consumer Reports
If you authorize us to do so, we may obtain information about you from credit reports or other investigative consumer reports prepared by third parties at our request. If you authorize us to request such information and we request such information, you should be aware that:

- *You have the right to request to be interviewed in connection with the preparation of an investigative consumer report.*
- *Upon request, you are entitled to receive a copy of the consumer reports.*
- *The information obtained from the reports prepared by a third party may be retained by the third party and disclosed to other persons.*

Information we may disclose to third parties:
In the course of our general business practices, we may disclose the information that we collect (as described above) about you or others without your permission to the following types of institutions for the reasons described:

- *To a third party if the disclosure will enable that party to perform a business, professional or insurance function for us.*
- *To an insurance institution, agent, or credit reporting agency in order to detect or prevent criminal activity, fraud or misrepresentation in connection with an insurance transaction.*
- *To an insurance institution, agent, or credit reporting agency for either this agency or the entity to whom we disclose the information to perform a function in connection with an insurance transaction involving you.*
- *To a medical care institution or medical professional in order to verify coverage or benefits, inform you of a medical problem of which you may not be aware, or conduct an audit that would enable us to verify treatment.*
- *To an insurance regulatory authority, law enforcement, or other governmental authority in order to protect our interests in preventing or prosecuting fraud, or if we believe that you have conducted illegal activities.*
- *To a group policyholder for the purpose of reporting claims experience or conducting an audit of our operations or services.*
- *To an actuarial or research organization for the purpose of conducting actuarial or research studies.*
- *In addition to those circumstances listed above, and unless you direct us not to by completing the attached Opt Out Form, we may disclose certain information about you to third parties whose only use of the information will be for the purpose of marketing a product or service. Under no circumstances will we disclose for marketing purposes: any medical information, information relating to a claim for a benefit or a civil or criminal proceeding involving you, personal information relating to your character, personal habits, mode of living or general reputation*

Right to access and amend your personal information:

You have the right to request access to the personal information that we record about you. Your right includes the right to know the source of the information and the identity of the persons, institutions or types of institutions to whom we have disclosed such information within two (2) years prior to your request. Your right includes the right to view such information and copy it in person, or request that a copy of it be sent to you by mail (for which we may charge you a reasonable fee to cover our costs). Your right also includes the right to request corrections, amendments or deletions of any information in our possession. The procedures that you must follow to request access to or an amendment of your information are as follows:

To obtain access to your information: You should submit a request in writing to the (insurance agency). The request should include your name, address, social security

number, telephone number, and the recorded information to which you would like access. The request should state whether you would like access in person or a copy of the information sent to you by mail. Upon receipt of your request, we will contact you within thirty business days to arrange providing you with access in person or the copies that you have requested.

To correct, amend, or delete any of your information: You should submit a request in writing to (the insurance agency). The request should include your name, address, social security number, telephone number, the specific information in dispute, and the identity of the document or record that contains the disputed information. Upon receipt of your request, we will contact you within thirty business days to notify you either that we have made the correction, amendment or deletion, or that we refuse to do so and the reasons for the refusal, which you will have an opportunity to challenge

Our practices regarding information confidentiality and security:
We restrict access to nonpublic personal information about you to those employees who need to know that information in order to provide products or services to you. We maintain physical, electronic, and organizational safeguards to protect information about you.

Sample Privacy Disclosure #2

Dear Clients:

As a current customer of our agency, we take this opportunity to both thank you and share with you the importance in which we hold the privacy and confidentiality of your insurance and personal information. XXX Agency, as a member of the financial services industry, has been and continues to be subject to federal and state privacy laws regarding the collection and exchange of your insurance information.

Working with you, XXX Agency gathers the necessary information from you and other public and insurance sources to execute the insurance market search and placement for the insurance coverages your needs/risk exposures require. We collect nonpublic personal information about you from the following sources:

- *Information we receive from you on applications or other forms;*
- *Information about your transactions with us, our affiliates or others; and*
- *Information we receive from a consumer reporting agency.*

In doing so, XXX Agency exchanges such information only with other insurance related parties that are similarly obligated under state and federal privacy laws and have in place the appropriate procedures to keep all treatments and exchanges of your information with in the requirements of these laws.

We may disclose the following kinds of nonpublic personal information about you:

- *Information we receive from you on applications or other forms, such as your name, address, social security number, assets, income, and beneficiary information;*
- *Information about your transactions with us, our affiliates or others, such as your policy coverage, premiums, and payment history; and*
- *Information we receive from a consumer reporting agency, such as your creditworthiness and credit history.*

OR

We may disclose all of the information we collect, as described above. And as we place your insurance with these carriers, both our agency and the carriers work together (as well as individually) to retain uses for only those activities required to underwrite, issue and services your policy of insurance, as well as conduct claims activities - should that be necessary on your behalf. We restrict access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

As the scope of our agency business and your needs expand, XXX Agency is proud to advise you that we are formally engaged in joint marketing ventures with additional financial service providers. The businesses listed here are tops in their field of expertise and round out the scope of product and services we can offer to you. This permits us to better respond to the multi-financial services needs that you shared with us. We may disclose nonpublic personal information about you to the following types of third parties:

- *Financial service providers, such as life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents;*
- *Non-financial companies, such as retailers, direct marketers, airlines, and publishers; and*
- *Others, such as non-profit organizations.*

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- *Information we receive from you on applications or other forms, such as your name, address, social security number, assets, income, and beneficiary information;*
- *Information about your transactions with us, our affiliates or others, such as your policy coverage, premium, and payment history; and*
- *Information we receive from a consumer reporting agency, such as your creditworthiness and credit history.*

OR

We may disclose all of the information we collect, as described above to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

All of these professional financial services operations are subject to state and federal privacy laws and are bound by their agreement with us to also comply with the insurance requirements in this area as well. Should you purchase their product or service, a copy of their privacy practices will be sent to you.

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). ***If you wish to opt out of disclosures to nonaffiliated third parties, you may call the following toll-free number: (insert number).***

We know that you have other choices when it comes to insurance and financial services. That is why we at XXX Agency appreciate your decision to place your financial service needs with us. We value you and your business, and look forward to a continuing client relationship with you. XXX Agency wants to earn your partnership to explore your financial service needs, determine the various placement options that may respond to these needs and over time build the type of financial service portfolio you need to secure your family needs and assets.

Should you have any questions, please do not hesitate to call me.

Sincerely,
Agency-Owner Principal

INDEX