CLIENT RECORDS & CONFIDENTIALITY
# Table of Contents

INTRODUCTION .................................................................................................................................................. 1  
   The Issue of Client Privacy .......................................................................................................................... 1  
   The Problems with Sharing Information ...................................................................................................... 1  
   Being Responsible as an Agent .................................................................................................................... 1  

Assessment Introduction .................................................................................................................................. 3  

CHAPTER 1 .................................................................................................................................................... 4  

PRIVACY ISSUES: AN UNDERSTANDING ....................................................................................................... 4  
   Why Privacy is Important .......................................................................................................................... 4  
   Privacy as a Right ....................................................................................................................................... 4  
   Appraising Insurance Risk ......................................................................................................................... 5  
   Understanding Consumer Concerns ........................................................................................................... 6  
   Individual Health Information .................................................................................................................... 6  
   Individual Financial Data ............................................................................................................................ 7  
   Privacy Laws ............................................................................................................................................. 8  
   HIPPA – Administrative Simplification .................................................................................................... 8  
   The Gramm-Leach-Bliley Act (GLBA) ....................................................................................................... 8  
   The Federal Medical Privacy Rule ............................................................................................................ 9  
   The Patriot Act .......................................................................................................................................... 9  
   Other Legislation ..................................................................................................................................... 9  
   Why Compliance Works .......................................................................................................................... 10  
   Improved Efficiency .................................................................................................................................. 10  
   Enhanced Security .................................................................................................................................... 10  
   Drawbacks of Compliance ......................................................................................................................... 10  
   Customer Privacy: Opt-Out and Opt-In standards .................................................................................... 11  
       What is “Opt-Out”? ................................................................................................................................. 11  
       Debates about the Opt-In Clause ......................................................................................................... 11  
       Keeping Check of Personal data ........................................................................................................... 12  
       How Client Privacy is Affected on the Internet .................................................................................. 13  
       Online Communications ....................................................................................................................... 13  
       Privacy Levels ...................................................................................................................................... 13  
       Activities in the Public Domain ............................................................................................................ 13  
       Semi-Public Activities ........................................................................................................................... 13  
       Private Services ................................................................................................................................... 13  
       Monitoring and Recording Activity ..................................................................................................... 14  
       Preventing Privacy in Cyberspace ........................................................................................................ 14  
   Privacy Protection Tools ............................................................................................................................. 15  
       Encryption ............................................................................................................................................ 15  
       Anonymous Re mailers ......................................................................................................................... 15  
       Memory Protection Software ................................................................................................................. 15  
       The Internet Revolution ....................................................................................................................... 16  
       Centralized Databases ......................................................................................................................... 16  

Assessment – Chapter 1 .................................................................................................................................. 17  

CHAPTER 2 ..................................................................................................................................................... 18  

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>28</td>
</tr>
</tbody>
</table>

### Assessments

#### CHAPTER 3

#### HEALTH INFORMATION PRIVACY and PROTECTION

- Medical Records - Their Importance ................................................................. 29
- Rights of Information Privacy ........................................................................... 29
- Doctor-Patient Confidentiality ........................................................................... 30
- Client Privacy and Medical Records ................................................................. 31
- Privacy of National Patient Record .................................................................. 31
- Standard of Safeguards ...................................................................................... 33
- Medical Information Bureau ................................................................................ 34
- Health Insurance Portability, Accountability Act (HIPAA) ............................... 34
- The Rule - Administrative Simplification ......................................................... 35
- Administrative Simplification Purpose in HIPAA .............................................. 35
- Personal Information in Electronic Transmission form ........................................ 35
- Health Care System Today ................................................................................ 36
- Effective Health Care and Privacy ...................................................................... 37
- Harmful Use of Medical Information .................................................................. 38
- Part C - Social Security Act: Administrative Simplification ............................. 38
- Privacy Rule ......................................................................................................... 46
- Privacy Rule - A Summary .................................................................................. 46
- The Acquisition of Consent ................................................................................ 47
- Health Care Operations, Treatment or Payment .................................................. 47
- The Directories ..................................................................................................... 47
- Fund-Raising and Marketing ............................................................................... 48
- Privacy Practices: Notices ................................................................................... 48
- Officials of Law Enforcement .............................................................................. 48

**SAFEGUARDING THE PRIVACY OF FINANCIAL INFORMATION**

- Understanding Financial Data ........................................................................... 18
- The Financial Services Modernization Act or Gramm-Leach-Bliley Act (GLBA) ................................................................................ 18
- Financial Institutions .......................................................................................... 18
- Privacy Warnings ................................................................................................. 19
- Asking for a Privacy Policy .................................................................................. 19
- Joint Accounts ..................................................................................................... 19
- Closed Accounts ................................................................................................. 20
- Explaining the “Opt-Out” Option ........................................................................ 20
- Information that May be Disclosed ...................................................................... 20
- Safeguarding Personal Financial Privacy ............................................................. 21
- Legal Action against Financial Institutions ......................................................... 21
- Federal Agencies ................................................................................................ 21
- Gramm-Leach-Bliley Act ...................................................................................... 22
- Title V of the GLBA .............................................................................................. 22
- Fair Credit Reporting Act (FCRA) ....................................................................... 24
- How Consumer Reports May be Used ................................................................. 25
- Providing Consumer Reports .............................................................................. 25
- Consumer Report Exclusions ............................................................................. 26
- Sharing Investigative Consumer Reports ............................................................ 26
- Consumer Disclosures ........................................................................................ 26
- Challenging Information in a Report ................................................................... 27
- Limitations on Investigative Consumer Reports ................................................ 27
- Using Consumer Reports: Some Guidelines ....................................................... 27
- Using Consumer Reports Responsibly ............................................................... 27
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes in Privacy Practices and The Notices................................................................. 69</td>
</tr>
<tr>
<td>Regulation of Federal Privacy ............................................................................................. 69</td>
</tr>
<tr>
<td>The Privacy Act................................................................................................................ 69</td>
</tr>
<tr>
<td>The Freedom of Information Act ....................................................................................... 69</td>
</tr>
<tr>
<td>Confidentiality Requirements of Federal Substance Abuse ................................................. 70</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act ........................................................................ 70</td>
</tr>
<tr>
<td>Employee Retirement Income Security Act of 1974............................................................ 71</td>
</tr>
<tr>
<td>Federally Funded Health Programs ..................................................................................... 71</td>
</tr>
<tr>
<td>FDA - Food, Drug, and Cosmetic Act .................................................................................. 71</td>
</tr>
<tr>
<td>Amendments in Clinical Laboratory Improvement .............................................................. 72</td>
</tr>
<tr>
<td>Other Mandatory State or Federal Laws .............................................................................. 72</td>
</tr>
<tr>
<td>Federal Disability Nondiscrimination Laws. ....................................................................... 72</td>
</tr>
<tr>
<td>Final Regulation Guidelines............................................................................................... 75</td>
</tr>
<tr>
<td>Individually Identifiable Health Information Privacy and Standards.................................... 75</td>
</tr>
<tr>
<td>Consent of the Patient ......................................................................................................... 76</td>
</tr>
<tr>
<td>Background ........................................................................................................................ 76</td>
</tr>
<tr>
<td>Frequently Asked Questions .............................................................................................. 77</td>
</tr>
<tr>
<td>The Minimum Necessary ...................................................................................................... 80</td>
</tr>
<tr>
<td>A General Requirement ....................................................................................................... 80</td>
</tr>
<tr>
<td>Personal Health Information, Their Disclosures and Uses, Requests for It ....................... 80</td>
</tr>
<tr>
<td>Disclosure and Use of Information and Reasonable Reliance ............................................ 80</td>
</tr>
<tr>
<td>Frequently Asked Questions .............................................................................................. 81</td>
</tr>
<tr>
<td>Oral Communications .......................................................................................................... 82</td>
</tr>
<tr>
<td>The Background .................................................................................................................. 82</td>
</tr>
<tr>
<td>The General requirements .................................................................................................. 82</td>
</tr>
<tr>
<td>Frequently Asked Questions .............................................................................................. 83</td>
</tr>
<tr>
<td>The Business Associate ...................................................................................................... 84</td>
</tr>
<tr>
<td>The Background .................................................................................................................. 84</td>
</tr>
<tr>
<td>A Business Associate-What Is It? ....................................................................................... 84</td>
</tr>
<tr>
<td>FAQs .................................................................................................................................... 85</td>
</tr>
<tr>
<td>In Relation To the State Law ................................................................................................ 86</td>
</tr>
<tr>
<td>Frequently Asked Questions .............................................................................................. 86</td>
</tr>
<tr>
<td>Marketing and Health-Related Communications ................................................................. 87</td>
</tr>
<tr>
<td>Marketing-What is it? .......................................................................................................... 87</td>
</tr>
<tr>
<td>Communications Not Considered Marketing ...................................................................... 87</td>
</tr>
<tr>
<td>Marketing Communications and the Limitations on Them ................................................... 87</td>
</tr>
<tr>
<td>Contractors/Business Associates of Covered Entities ........................................................... 88</td>
</tr>
<tr>
<td>FAQs : ................................................................................................................................. 88</td>
</tr>
<tr>
<td>Research .............................................................................................................................. 89</td>
</tr>
<tr>
<td>Research Rules .................................................................................................................... 89</td>
</tr>
<tr>
<td>Disclosing and Using Protected Health Information within Research ............................... 89</td>
</tr>
<tr>
<td>Unauthorized Research Disclosure/Use .............................................................................. 90</td>
</tr>
<tr>
<td>Use/Disclosure in Research Along With Individual Authorization ..................................... 91</td>
</tr>
<tr>
<td>FAQs : ................................................................................................................................. 91</td>
</tr>
</tbody>
</table>

Chapter 3 – Assessments ........................................................................................................ 93

CHAPTER 4 .............................................................................................................................. 94

THE NAIC: PROTECTING CLIENT PRIVACY ............................................................................. 94

Understanding the National Association of Insurance Commissioners (NAIC): .................... 94
What is the NAIC? .................................................................................................................. 94
How does the NAIC work? .................................................................................................... 94
Protecting the Privacy of Health Information ........................................................................ 94
Preemption.................................................................................................................................................................................95
Privacy and the Insurance Industry ......................................................................................................................................................95
Consumer Grievances...........................................................................................................................................................................96
Assessing Market Conduct .........................................................................................................................................................96
Assessing Financial Solvency .........................................................................................................................................................97
Health Information: Usage and Disclosure ......................................................................................................................................97
Privacy Issues Working Group .........................................................................................................................................................98
Task Force to Review Privacy Notices ..........................................................................................................................................99
Model Insurance Information and Privacy Protection Act ..............................................................................................................99

Assessment: Chapter 4.........................................................................................................................................................................102

CHAPTER 5 ......................................................................................................................................................................................103

INSURANCE AGENTS AND CLIENT PRIVACY ................................................................................................................................103
Respecting Confidential Information...................................................................................................................................................103
Impact of Privacy Laws ......................................................................................................................................................................103
Potential Conflicts ........................................................................................................................................................................104
Creating an Effective Privacy Policy ................................................................................................................................................105
Scope of Marketing Personal Information .......................................................................................................................................105
Misrepresentation ..............................................................................................................................................................................105
Global Privacy Concerns ................................................................................................................................................................106
Principles of Safe Harbor ................................................................................................................................................................106

Assessment - Chapter 5.........................................................................................................................................................................108

CHAPTER 6 ......................................................................................................................................................................................109

PRIVACY DISCLOSURE REQUIREMENTS ......................................................................................................................................109
Common Terms and Definitions ..............................................................................................................................................................109
Universal Client Privacy Rules ...........................................................................................................................................................110
Regarding Consumers: ......................................................................................................................................................................110
Exemptions..........................................................................................................................................................................................111
Essential Recipients .............................................................................................................................................................................111
Mandatory Disclosure Information .....................................................................................................................................................111
Regular Follow-up ..............................................................................................................................................................................112
FAQs on Financial Privacy .................................................................................................................................................................113
Sample Disclosure #1 ........................................................................................................................................................................121
Information we collect: ......................................................................................................................................................................121
Information from Credit Reports or Investigative Consumer Reports .........................................................................................121
Information we may disclose to third parties: ........................................................................................................................................121
Right to access and amend your personal data: ...................................................................................................................................122
Our practices regarding information confidentiality and security: ...................................................................................................122
Sample Privacy Disclosure #2 .............................................................................................................................................................122

Assessment - Chapter 6.........................................................................................................................................................................125
INTRODUCTION

Increasingly, more clients want to ensure that when they buy insurance, the personal data they reveal is protected. As stressed earlier, the agent-client relationship is akin to that of an attorney-client and should be governed by the same ethical and confidentiality standards. Not doing so can result in lawsuits. To tackle this concern, new legislation requires that agents not only notify their clients before sharing personal data with anyone else but also get their explicit approval to do so. Clients can turn down such requests.

The Issue of Client Privacy

Why is there so much concern about client privacy in today's world? For one, it has become frighteningly simple to distribute and exchange information electronically. The way we access healthcare has also undergone a shift, changing from personal, person-to-person doctor-patient interactions to being part of a much larger health network. This also means that the number of people with access to your information just went up dramatically. As a direct result, the potential risk of a breach of privacy and unauthorized access to your personal records also increased.

Simply put, there is a market for the personal data that agents collect from their clients, and such large networks are very likely to share or distribute such information with other interested partners or parties. It is up to you to ensure that your client's privacy is protected at all times.

The Problems with Sharing Information

As with other privacy issues, opinion may be divided on the idea of sharing of personal data. In some instances, especially in cases of medical emergencies, the ability to access personal medical records could mean timely and accurate medical treatment. But consider the alternative. The very same access could be abused – by employers to use information unfairly to turn down candidates, by insurance companies who can use that information to hike premiums, and by anyone with access and the intent to abuse that access. It could be someone who buys a second-hand computer and realizes that it still contains the complete client database of the local pharmacy. Or when someone in the healthcare network inadvertently emails out the medical history of a patient.

When the potential for privacy abuse is so great and the means to do it so simple, it becomes more critical than ever to ensure that there are laws to protect clients, and which hold insurance companies, healthcare providers and financial organizations accountable for any breach in client confidentiality.

Being Responsible as an Agent

Privacy legislations are also applicable to insurance agents who are known as a “financial organization” or “covered entity”. Agents are expected to comply with relevant norms under the Gramm-Leach-Bliley Act, HIPAA, the Federal Medical Privacy Rule, and with the possible inclusion of the new Patriot Act. It is also essential to consult legislation applicable in individual states, which can often be in conflict with the universal norms. For example, HIPAA privacy rules categorize personal data like name, address, social security number etc. as “health data” governed by an opt-in standard. This means that this information cannot be disclosed without the explicit approval of the client. However, in some states, this information is categorized as “financial data” subject to opt-out standards. This allows the agent to freely share such information until the time the client “opts out”.

1
With such conflicting laws, the room for disputes is plenty. And there is much at stake with penalties that can include fines up to $25,000 and/or 1 year prison terms. The agent must clearly notify the client before sharing or disclosing any personal data. Not doing so could result in prosecution as directed by federal and state unfair trade practices rules and by the State Department of Insurance. Additionally, the agent is also liable for a civil law suit brought forward by the client.

This course will try to describe the various complex issues and laws that govern client privacy. The course first outlines the many Privacy Issues and their relevance in today's world of business. Next, Protecting Financial Information Privacy and Protecting Health Information Privacy discuss the two areas that are most relevant to an agent. Finally, the sections on Agent Disclosure Issues answer specific queries on complying with new privacy rules.

The United States still has a long way to go in privacy legislature, so you would be well-advised to keep track of new developments and new laws!

*Always consult a lawyer or your carrier before putting to use any of the information contained in this course in individual or client matters.*
**Assessment Introduction**

1) What are agents referred to in privacy legislation (Page 1, para 6)
   a) Respondents
   b) Complainants
   c) “Financial Institutions” or “Covered entity”
   d) Care providers

2) What does *opt-in standard* refer to? (Page 1, para 6)
   a) A rule that classifies a client’s personal data as confidential and subject to approval by client before sharing by agent
   b) A rule that allows the client to opt to continue his/her policy
   c) A rule that allows the agent to opt to be part of a information-sharing network
   d) A standard that allows a client to opt to be part of an information-sharing network

3) What is the penalty applicable if an agent violates privacy laws? (Page 1, para 7)
   a) A stern warning and undertaking not to repeat the offense
   b) A fine up to $25,000 per incident and up to 1 year in prison
   c) A fine of $100 per incident and community service
   d) Revoking of the agent’s license
Chapter 1

PRIVACY ISSUES: AN UNDERSTANDING

Why Privacy is Important

Privacy is considered the fundamental right of every single citizen. Every state in the United States recognizes this right and enforces it through common or statutory laws. Some have even included it in their constitution.

From the very beginning, privacy issues and laws have formed an integral part of American laws. To quote from 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.” The Constitution outlines many tenets that are primarily concerned with protecting every person's right to privacy while maintaining a balance with larger, national social objectives.

For instance, the Fourth Amendment to the United States Constitution clearly defines 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.” The statement hints at the value American laws place on the notions of privacy – the same notions which require patients be asked for consent before any medical interventions; or the right of every individual to protect private information stored in diaries or medical records. While the right is not absolute, emphasis here is placed on “unreasonable search”.

In the New York Whalen v. Roe case (429 U.S. 589 – 1977), the Supreme Court differentiated between two types of interest in a “zone of privacy” protected by the constitution. Here, the reference was to a created database of individuals who had access to drugs through legal means or otherwise. However, the right to privacy is not absolute – for example, in instances where repressing information about oneself can have public implications, as with communicable diseases.

It is generally accepted practice that a person is allowed to decide how much personal data he wants to share. Specifically, with relation to medical records and health-related information. Most people would balk at such sensitive information being freely and publicly accessible. Perhaps the most sensitive information are notes and records of mental health treatment. In the Jaffee v. Redmond, 116 S. Ct. 1923 (1996) case, the supreme court found that statements made by a patient to the therapist during treatment sessions could not be subject to civil discovery as per the Federal Rules of Evidence. Every state adopts some form of this patient-therapist privilege with the intent to encourage citizens to seek help for mental and emotional problems, thus underscoring the importance of mental health along with physical health.

Privacy as a Right

Privacy is recognized as a fundamental right by many international treaties including the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights. Businesses such as underwriting, financial services, and others, need and demand access to personal client information. It then becomes increasingly important to protect this information and the client's privacy rights.

The world over, the right to privacy is explicitly outlined in the Constitution. At the very least, the constitution recognizes the notion that a home is sacrosanct. Newer constitutions of countries like Hungary and South Africa...
also protect an individual's right to control personal data. In countries such as India and the United States, the right to privacy is outlined overtly in other provisos. In yet others, agreements concerning such rights have passed into law. For instance, the International Covenant on Civil and Political Rights or the European Convention on Human Rights.

Defining the right to privacy can be challenging, and doing so for the law even more so. Since early times, the individual and his right to privacy have frequently been acknowledged as evidenced by references in religious books such as the Bible, and in other cultural texts. While these references are mostly concerned with the right to be alone, each culture defines privacy differently. In the modern world, privacy very often relates to the protection of data or to the way personal data is shared and distributed.

Broadly speaking, privacy rules may be applied as follows:
- **Privacy of Information**: concerned with the collection and management of personal data such as medical records, credit history, etc.
- **Bodily privacy**: concerned with an individual's right to protect himself against invasive procedures like cavity searches, invasive medical tests, etc.
- **Communication Privacy**: concerned with protection of personal communication such as e-mails, telephone conversations, etc.
- **Territorial privacy**: concerned with protecting physical environments such as homes, the workplace, etc.

**Appraising Insurance Risk**

In arriving at appropriate coverage costs, insurance companies first assess an individual's risk profile. Insurance works by pooling together a set of people with similar profiles so companies can spread the risk. The process of appraising risk allows companies determine what the 'fair share' of each individual is i.e. cost payable appropriate to individual profile. This process allows companies to offer insurance at prices that are reasonable, and sometimes, to offer insurance at all. More importantly, risk appraisal seeks to protect the insurance value for each client while safeguarding the insurance company's financial stability. It also protects against indiscriminate issuance of insurance to people not meeting the eligibility criteria.

A comprehensive risk appraisal process can help the client in many ways:
- **Lower Cost**: being categorized in a favorable or low risk group translates into lower costs for the client.
- **Locked-in Classification of Risk**: the risk classification is future-proof meaning that the client continues to maintain his classification irrespective of future developments such as a deterioration in health.
- **Quality Coverage**: a robust risk appraisal process indicates good business practices at the insurance company.
- **Coverage that cannot be canceled**: once a client completes the appraisal process, the policy issued is lifelong and cannot be canceled for health reasons.
- **Early Warning**: a client can also be alerted to underlying, hidden medical problems through the appraisal process.

The process of risk appraisal therefore, requires access to personal data such as medical and financial records, besides information relating to employment, hobbies, etc. For the process to succeed for both, the company as well as the customer, it is important that the process of collecting information is thorough, and that the information provided by the client is accurate. All information thus gathered is treated as confidential. There are procedures in place through the application process to ensure client privacy.
Understanding Consumer Concerns
Privacy is likely the biggest and most challenging compliance issue the insurance industry will face in coming years. As technology makes access to information fast and incredibly simple, it is natural that consumers grow concerned about just how the information they share is being used.

With new ways to provide healthcare using the Internet and larger networks, consumers are increasingly becoming concerned about confidentially of their records. While technology can help offer healthcare at considerable cost and time savings, it also has the potential for misuse. With some health care websites even disclaiming liability for data use by third parties, it is not difficult to imagine why e-commerce companies struggle to build consumer confidence in such a state of open distrust.

Recent times have seen the number of privacy lobbyists burgeoning. Consumer distrust is further bolstered by the millions corporate America spends in anti-privacy lobbying. More individuals want to know that the information they provide their doctors and healthcare providers is not being shared or distributed without their say-so. Any breach of this inherently confidential relationship can be devastating. Reports such as the March 2000 one by the American Medical Association that highlights the failure of most health websites to comply with stated privacy norms only serve to build more distrust. It is clear that any e Health initiatives can only work if the consumer is confident that his privacy is completely protected.

Individual Health Information
Most individuals perceive their medical records as supremely sensitive and highly confidential. Health histories are very revealing, containing a high level of personal data. Indiscriminate dissemination of this information can have devastating outcomes ranging from social discrimination to loss of employment. As more information goes online, physical files have become a thing of the past. This also means that personal records are accessible more easily, leaving the door open for misuse by anyone from individuals with an agenda to healthcare providers and insurers. And yet, when compared with stricter statutory protections available for investment and banking information, tax records, or even video rental data, privacy norms for protecting individual medical information are surprisingly flimsy.

However, the emphasis on protecting an individual's right to safeguard the privacy of health data needs to be balanced against the larger goals of a public health system. Access to medical records can help healthcare professionals provide better clinical care. Gaining access to health data can also help researchers make a comprehensive analysis of healthcare services. Centralized information makes it easier to control fraud and prevent misuse by individuals. Tracking health and epidemiological investigations become more manageable. Therefore, any health privacy protection must strike a balance between rights of an individual and collective good.

The way health data is being gathered and used is changing. As the healthcare world moves towards a model of managed care, the demand for personal data has increased. Electronic records allow previously separate pieces of information to be tied together. This can mean that private medical information could be used in detrimental ways. A consumer may find that after he has submitted his insurance claim for reimbursement, the bank turns down his loan application due to his health history. Or he may find that he has been turned down at a job interview. He may start receiving calls for products that relate to his medical history. All obvious instances where personal data has been distributed to third parties without the individual's express consent.

According to the National Association of Insurance Commissioners (NAIC), these consumer concerns will be addressed by differentiating between how health data and financial data are treated. Clients will now have access to the “opt-in” standard for individual health data. Agents will need to obtain the express approval of
individuals before disclosing or sharing any personal data. The agent-client relationship is based on trust and governed by confidentiality. To strengthen and maintain this relationship, underwriters should put in place a program to comply with privacy to protect client confidentiality.

**Individual Financial Data**

The term financial organizations refer to the consolidated operation of brokerage and insurance firms and banks. Financial institutions make transactions easier for the customer by providing combined account statements and bundling service charges. On the flip side, this consolidation also extends to the various pieces of information in each individual institution creating large databanks of client information crammed with highly sensitive and confidential data. Recognizing the huge privacy risk this could pose, Title V of the Gramm-Leach-Bliley Act (GLBA) outlines some basic consumer rights intended to help the consumer safeguard his financial privacy.

According to the GLBA, financial organizations must notify the consumer of the following:

- **Privacy Policy:** Consumers must be clearly informed of the various personal data being gathered by a financial organization
- **Opt-Out Rights:** Customers must be apprised of their right of refusal to prevent sale or distribution of their private information to third parties by a financial organization
- **Safeguards:** Financial institutions must put in place requisite policies aimed at preventing unlawful access to confidential client information. Consumers must be informed of such policies.

The deadline for compliance by financial organizations was July 1, 2001.

However, compliance to privacy laws is just one side of the coin. Financial institutions must also build awareness among their consumers of privacy policies being followed. The typical consumer may have his mailbox jammed by privacy notices from credit companies, banks, etc., but in reality, the understanding of what these notices really mean will require more effort and communication. Companies need to adopt a more empathetic approach by trying to understand how their consumers would react to:

- the amount of personal data being collected by the business
- how this information is being used
- if this information is being revealed or distributed to other partners or third parties
- who receives this information
- how this information is finally used by the other parties

It is important that privacy policies are detailed in easy-to-understand language, explaining just how various information collection processes impact the customer. Leaving explanations to the fine print (that nobody ever reads) could result in antagonizing the customer prompting him to start withholding vital financial data. This can have a cascading effect for customers and financial organizations. Financial institutions use credit information to assess credit worthiness of potential customers and to offer credit at lower rates. Competitive rates mean more choice for the customer when he is shopping around for the right credit product at the right price. Credit information also allows financial organizations to track fraud, while helping investors better assess investment opportunities. This is best demonstrated by asset-backed securities. The secondary mortgage market showcases how such secondary markets can succeed. It is estimated that in the United States, prices of mortgages dipped by at least two percentage points because secondary loans were easily available. The same holds true for car loans and credit cards. It is estimated that investors in security backed asset pool control almost $436 billion in credit.
As more banking and financial transactions take place online, financial organizations must reassure customers that their privacy continues to be treated with utmost care and diligence. While customers reap the benefits of the new online marketplace, it is important that they fully understand the new rules concerning online financial services. The new privacy rules prompt both customers and financial organizations to view privacy as a serious issue.

**Privacy Laws**

What follows is a description of new privacy regulations:

**HIPPA – Administrative Simplification**

The concluding rule for the Standards for Privacy of Individually Identifiable Health Information, also referred to as the “Privacy Rule,” puts in place the privacy requirements of the “Administrative Simplification” provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Some healthcare providers, health plans, and healthcare clearing houses are covered by this rule. The regulation also defines standards governing individual rights on personal health data and the use of such information.

Personal health data as defined under the Privacy Rule refers to any information that
- is concerned with an individual's health, physical and mental; the delivery of healthcare and it's payment
- categorizes or may be used to categorize the individual concerned
- may be put together by or delivered to a covered entity
- is distributed and maintained in any format

Privacy rules are founded on the rationale that every individual has a fundamental right to privacy, which is also an integral component of personal and collective freedom. A discussion of how these rules can impact agents follows in later chapters.

**The Gramm-Leach-Bliley Act (GLBA)**

The comprehensive Act regulates how financial organizations (which include insurance companies and agents) can use client information. In November 13, 2000, GLBA regulations were passed. Institutions were expected to fully comply by July 1, 2001. Both, the HIPAA and the GLBA deal with the issue of financial privacy and are applicable to all kinds of financial organizations including:
- traditional banks
- investment-oriented institutions that provide investment advice or underwrite securities
- institutions that insure, guarantee, or indemnify against loss, sickness, disability, loss of life, etc.
- those that provide and issue annuities
- anyone who acts as an agent, principal or broker for activities listed above

The Federal Trade Commission lists businesses that may be governed by these regulations and include: - - - - - -
- vendors who distribute credit cards specific to them
- appraisers of real estate and individual property
- those that prepare tax
- automobile dealer
- developers of financial software
- career counselors in the financial services industry and
- businesses that print and retail checks
Most insurers are covered by these provisions i.e. any individual or unit with approval to conduct business according to state insurance codes. These regulations are applicable to all types of insurance although the GLBA provisions may place restrictions only on health data. While these regulations establish federal privacy protection standards, norms for individual states may vary. An insurance producer licensed by a State is exempt from GLBA privacy requirements providing

- he is an agent, employee, or representing a different licensed agent
- his affiliates supply notices as required
- he does not share or distribute private information to third parties except his employer or his affiliates

These exceptions allow any agent or agency exemption from the GLBA notification burdens as long as the information sharing is limited to the insurer that they represent. Any information sharing to third parties requires the agent to give disclosure and opt out intimations to the client.

If the agent also offers any advisory services (at a charge) covering financial, economic or investment matters to any individual, that person is then deemed a customer and must receive complete disclosure on privacy policies being followed by the agent. This does not apply when the agent sources multiple estimates from several insurance companies in a bid to find the best product at the best price for his client, who is then viewed as a potential consumer of any of the firms that the quote has been sought from. Should the client purchase insurance from any one company, he then becomes its customer.

The exception here is if the agent is going to share client information with third parties besides the companies he is soliciting a quote from. In such instances, the agent must notify and seek client permission to do so. The client retains opt out rights. It is essential that each agent or agency develops its individual privacy policy to suit the needs and type of operation. Any agency that has an exclusive relationship with an insurance company may benefit from being covered by the GLBA policy of that company. The agent exception rule can also be favorable for other traditional types of agencies. For example, any agency that does not automatically share confidential data with third parties. From the agency's perspective, it should ensure that the parent insurance company that it seeks to represent, complies completely with GLBA regulations. An in-depth discussion of the impact of the GLBA can be found later in the book.

**The Federal Medical Privacy Rule**

The Federal Medical Privacy Rule was approved by President Bush in April, 2001, and heralded a big change in the definitions of patient consent. This rule allows the federal government the ability to decide who can access an individual's personal medical information. The Federal Medical Privacy Rule takes away from individual choice and the notion of informed consent which assumes a person has the ability to make an informed choice about allowing access to his/her private health data. Informed choice is applicable only when the patient makes an independent choice free of duress.

**The Patriot Act**

The Patriot Act was passed on April 24, 2002, and came into being after September 11. The Act is intended to deal with terrorism and money-laundering. However, at this point, it is not yet clear how the Patriot Act impacts agents or how it works in conjunction with the GLBA.

**Other Legislation**

There are several other laws that are concerned with client privacy issues. These 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

Why Compliance Works

Improved Efficiency
The new privacy regulations have meant that organizations and insurance providers have had to make significant changes in order to fulfill compliance requirements. Smart organizations have seized upon this as a chance to become more efficient and therefore more effective not just in their operations, but also in the management of patient health data.

Enhanced Security
Anybody that transacts online or runs an e-business knows the threat from hackers and malware. Viruses like the Nimda and Code Red can cause irreparable damage. For instance, it was estimated that the Love Bug virus may have cost businesses as much as $8.75 billion. The Health Insurance Portability and Accountability Act of 1996 is intended to enforce stricter security around patient information at healthcare companies. The act primarily seeks to improve health insurance fraud while cracking down on fraud. Companies that tighten their security protocols are more likely to rank high on customer confidence. Better security also means reduced risk which can translate in to increased administrative efficiencies and cost savings.

Drawbacks of Compliance
Regulations such as the Federal Medical Privacy Rule weaken the individual's ability to control personal medical information. In fact, medical practitioners are required to by law to share patient information with the federal government. They do not have to seek patient consent. Reasons health records are disclosed can include:
- public health interests
- law enforcement activities
- research
- FDA monitoring
- judicial and administrative proceedings
- health care system interests
- licensing
- any work between US health officials and foreign governments

Once this information has passed on to a third party, privacy rules no longer apply. No patient consent is required to use this information nor are there regulations governing the manner in which these private health records may be used. Additionally, information collated before February 26, 2003 is not covered by the privacy rule. Patients cannot explicitly prevent access to their medical records. Furthermore, doctors may refuse treatment to a patient in the event of patient refusal to share their health data. Doctors may also refer to other patient records while planning treatment. There are no penalties for the sharing and disclosing of such
information. Patients therefore have limited or no recourse in the event that a breach of confidentiality of medical data has occurred. Health information like blood banks, sperm banks or databases of genetic information are also not covered by the privacy rule.

As has been mentioned before, the Internet has made the transmission and access of information frighteningly simple. While the privacy rule for medical information seeks to establish standards for a national health data network, the issue of patient confidentiality still looms large. Medical practice advocates are urging for more comprehensive legislation that will guarantee and protect patient privacy.

Customer Privacy: Opt-Out and Opt-In standards

What is “Opt-Out”
“Opt-out” allows individuals to choose to remove their names and personal data from marketing databases and lists. Companies collect information from customers in many ways, most commonly through product application forms. This information may be put up for sale or shared with other third parties such as marketing agencies. It is mandatory for financial organizations to send privacy notices to their customers. While the onus of reviewing and understanding this information is on the customer, federal laws provide the individual some basic right to safeguard personal financial records. A client can ‘opt-out’ i.e. inform his bank, insurance company or other financial organization that he declines consent for the sharing or distribution of his personal data with other third parties. However, unless a customer explicitly opts-out, this data may be freely shared by the financial organization.

Debates about the Opt-In Clause
Consumer advocates lobbied hard to have an opt-in clause established. Such a clause would prevent the disclosure of personal monetary information unless the customer specifically opted-in. However, the clause did not come to pass and the onus to protect financial privacy is still on the consumer.

Opt-in does not protect consumer privacy. Eventually, the call of whether to allow personal data to be used or not still lies with the customer, and there seems to be no significant advantage to the opt-in clause. Neither “opt-in” nor “opt-out” are a true reflection of consumer preferences. Either way, the potential seller would still receive the same information about the consumer. However, providing these choices could distort customer preferences if transaction costs are imposed on either choice.

Transaction costs involved with opt-in may prevent consumers from providing information that accurately represents their privacy choices. The converse for opt-out may also be true. It is the seller who controls the transaction costs involved, and this may be the reason that “opt-in” is a better reflection of true consumer privacy preferences. By making the opt-in option more attractive, the seller incentivizes the consumer to share information. Conversely, by making the opt-out option more laborious, the seller makes the choice to opt-in seem much easier and viable to the consumer.

Opt-in can affect consumer privacy by thwarting efforts to reduce fraud and identity-theft. Opt-ins reduce the amount of data sellers can access about consumers. Sellers usually keep track of spending patterns and consumer behavior that help alert them to unusual activity as an indicator of possible fraud. Restricting access to personal data, ironically, can actually help fraudsters pull off identity-theft. This may be a point to be raised to alert consumers who decide to opt-out – sharing personal data may not always be detrimental.

Opt-in creates more costs for sellers which eventually trickle down to the consumer. Opt-in requires sellers to follow due process in obtaining permission from consumers for the use of their personal data. All these processes add to operational costs. Opt-in also means an inflation of marketing costs, one from an increase in material provided to the consumer, and two, from an increase in target market. Marketing using catalogs and online websites can actually increase costs which is eventually borne by the consumer. Of the two, catalog marketing is more likely to be affected by opt-ins because of the data restrictions that are imposed on it. The
Internet is an interactive tool that counterbalances lack of consumer information from third parties. To completely understand how opt-ins affect sellers, it is important to consider how other industries are so dependent on catalogs as a primary marketing tool.

Privacy concerns play a big role in the relatively slow growth of e-commerce. In a Federal Trade Commission report to Congress, data showed that while 92% of consumers surveyed registered concern about potential abuse of their personal data online, 67% were very concerned. Another 76% though not concerned with inappropriate use of personal data, feared their privacy would be breached online. It is likely that such fears result in loss of sales – a fact demonstrated by other surveys that indicate that customers concerned with online privacy are less likely to transact online. This apprehension also possibly keeps away many first time users as well.

Providing assurances about the confidentiality of personal data could well be enough to encourage more consumers to opt-in and transact online. As e-commerce benefits, resultant operational and cost benefits would counteract extra costs that the administration of opt-in schemes might entail.

**Opt-ins impact market competitiveness.** As operational costs increase, only the leanest and fittest companies will survive in the market. The processes required to collect data for opt-ins create a natural entry barrier for new entrants. Existing players will benefit from the first mover advantage, and from having an established relationship and brand recognition with consumers.

**Opt-in costs get passed on to poorer consumers disproportionately.** Studies show that the consumers most likely to use distance shopping are from rural and inner city areas – populations that are also significantly less wealthy. As companies absorb costs associated with the opt-in scheme and pass them on to consumers, this population group is also the least equipped to weather increased costs.

### Keeping Check of Personal data

The issues of financial privacy gained prominence through the GLBA also known as the Financial Services Modernization Act. Driving the debate is that one question – who ultimately controls how much and how individual financial data is used – the individual or the company?

As discussed earlier, financial organizations, essentially a network of banks, insurers and brokers, commonly share customer data between themselves. While this can result in benefits for customers through tailored products and better pricing, it also means that the consumer is more vulnerable to privacy breaches.

Options such as “opt-outs” do provide consumers with some degree of control over sharing of their personal data with third parties. The consumer, however, has little control of how information sharing takes place between affiliates. What this translates into are hefty dossiers crammed with sensitive personal data from social security numbers, debt levels, income, even medical histories and alimony payments. Enough to make any individual feel intimidated.

Individuals have to be more diligent in retaining control of their personal data. This may not be an easy task when you consider the prospect of even more forms to fill out for an already busy consumer. It is inevitable then, that financial organizations operate on the basis of implied consent, trusting busy lifestyles to stop the consumer from making the extra effort to opt-out. Even where financial organizations follow consumer-centric policies, the institution itself does not have much control over consumer data that has already been sold or distributed.

Where businesses primarily seek to market their services without profiting from the sale of consumer data, opt-ins may work better. Opt-in notices can even be used as marketing opportunities. However a company may choose to use them, privacy notices are mandatory and covered by two federal laws - the Financial Services Modernization Act (also known as GLBA) and the Fair Credit Reporting Act (FCRA). These laws may not be mentioned specifically in privacy notices so it is key for the consumer to be aware of common terms associated with the regulations. The GLBA offers consumers the option to opt-out of sharing of private information between a company and third parties. The FCRA goes a step further and allows consumers the option to opt-out of the dissemination of private information between a company and affiliates.
How Client Privacy is Affected on the Internet
Online business has also raised issues of online fraud and a host of other ethical and legal issues. A company's e-commerce and online activities are more likely to receive careful scrutiny by privacy activists. Unfortunately, these activities do not always receive the due diligence required to track non-compliance from the company's legal and business teams.

Online Communications
Any communication over telephones and the Internet using cables or wireless access is referred to as online communications. To connect to the Internet, a consumer will usually use an Internet Service Provider (ISP) or dial in through a bulletin board service (BBS). The way the Internet works creates many privacy concerns. As information is sent and received over the Internet, it passes through several computers. Each system is managed by a system operator (sysop) and can capture and store information as it passes through. Therefore, a user's Internet activity can be tracked not just the ISP but also by any one of these sysops. With the vast array of information and activities on the Internet, one can see why privacy can become an issue of concern. These Internet-related privacy concerns also impact the insurance sector as more businesses transact online, and could be used as guidelines for future litigation challenges.

Privacy Levels
It is this simple – none of the activities that take place online guarantee absolute privacy. So, no matter what the nature of the activity, consumers must work independently to safeguard privacy.

Activities in the Public Domain
Online activities such as blogs, public discussion forums, chat rooms, etc. are essentially public domains and subject to scrutiny by any one. In fact, the law allows access to any material on sites that are “readily accessible”. Use of such public sites also means that any information stored by such sites like e-mails, addresses, names, etc., are also subject to public view. Consumers should therefore exercise appropriate caution in the type and amount of information that they share. Service providers also usually maintain a directory of their members which is public and which may sometimes be sold to direct marketers.

Semi-Public Activities
Users can often be fooled into thinking that some Internet activities are private because of the use of passwords or access restrictions. However, like any electronic communication, these may be recorded and shared by other users. A typical example of such an activity would be restricted-access chat rooms. While who accesses a site may be controlled, there is nothing to prevent an existing member of the chat room from recording and using these 'private' chats. Consumers should remember that like private e-mail, these activities are governed by similar monitoring exceptions.

Private Services
According to the Electronic Communications Privacy Act (ECPA), it is illegal for any individual to read or share any part of any electronic communication, such as e-mails. There are three exceptions to the Act which are:
· If the service provider suspects the user of destructive activity that may cause harm to the system or another user, the service may then access private e-mail. Service providers may not randomly track e-mails.
· the service provider is legally allowed to access and share private messages if the user consents. New members are usually required to sign a consent agreement at the time of signing up.
· Most e-mails sent from business accounts are not private. The employer is considered the owner of the e-mail system and is legally allowed to monitor, view, and disclose any e-mail sent by an employee.

If an e-mail has been intercepted by a sysop for any of the reasons given above, the sysop is expected to treat the e-mail as private and can share its contents only with the addressee. The disclosure prohibition do not apply when:
· the sender or receiver/s permits disclosure
· a courts orders disclosure
· the message reflects possible involvement with a crime. In such cases, the e-mail may only be viewed by relevant law enforcement authorities.

The sysop is not accountable or liable for prosecution for incorrect delivery of a message i.e. sending to the incorrect person. The sysop, however, could be liable for damages for any negligence in provision of services. Law enforcement authorities need a search warrant issued by the court to access any electronic communication. The EPCA details the process involved in granting such an order. Messages more than 180 days old are subject to more relaxed provisions.

Monitoring and Recording Activity
Not all Internet activity concerns the sending and receiving of e-mails. The Internet is a vast store house of information that users may visit for simple browsing and also to gather information. As discussed earlier, the Internet comprises a network of many computers and systems. Therefore, any activity on the Internet leaves a trail. It is possible to track a user’s Internet behavior by tracking the kind of websites visited, the frequencies of those visits, any transactions conducted on the sites, etc. These reports of user browsing patterns or transaction-generated information can provide online services with revenue avenues. This information may be gathered by service providers or sysops and sold or disclosed to marketers who can use the information for targeted marketing activities.

Again, the onus of browsing the Internet responsibly and of protecting sensitive or potentially embarrassing information lies with the user. Consumers should build their awareness about the Internet works and how private information is captured and stored. Users should also be aware of codes of conduct associated with accessing the Internet and e-mails from the workplace. So, at the end of the day, while it is virtually impossible to detect privacy intrusions, it is the user who must stay vigilant and thoroughly investigate any new online service before signing on.

Preventing Privacy in Cyberspace
A user is at risk every time he is online. It is imperative to be alert and to take the necessary steps to protect one’s privacy. Changing passwords frequently is one way to protect online data. Most experts recommend that password be a combination of alpha-numeric characters and symbols since these are the most difficult to crack. Users should avoid writing down passwords and i-pins anywhere. Extra care should be taken when logging on from public Internet cafes or centers. Never save user names or passwords on public or anyone else’s computer. Clear private data before logging off on public machines. Never exchange personal data such phone numbers, credit card details, passwords, etc. over any electronic communication including e-mails. Users should read the privacy policy of service providers and any online service carefully looking for any information about third-party
sharing of data etc. that may compromise privacy. It is also useful to stay away from services that do not satisfy personal privacy criteria. Also, users should be careful with the type and number of programs downloaded on their computer – only download programs from trusted sources to minimize risk of viruses and malicious software.

Online reviews are a great way to find out how good or bad a provider or service is. People tend to be vociferous about bad experiences! Users should also remember that any information posted on the Internet can be archived. This means that public postings, reviews, chats etc. may be searchable even in the future. Employers often make online background searches for new or potential employees. Marketers also use the Internet to track user and thereby collect data on his online behavior and preferences.

Privacy Protection Tools

Encryption
There are a number of options available to users to protect their privacy. Encryption is one of them. Encryption takes data from e-mails, online transactions, etc. and scrambles it into nonsensical data. This method is most often seen on banking and e-commerce sites to secure and verify extremely sensitive financial data. Encryption is also used to render e-mails unreadable by any individual/s other than the intended recipient. Thus, encryption is a powerful tool that thwarts unauthorized access and viewing of private data. However, this has caused some concern among law enforcement officials since the technology could also be used by offenders to protect their data. The legality of encryption is still being debated.

Anonymous Re-mailers
As the names suggests, these programs clean e-mails of all identifying information before re-sending the message to the original recipients, thus maintaining the anonymity of the sender.

Memory Protection Software
Internet browsing can be risky – there are many programs out there that can install themselves on your computer without your knowledge, and start transmitting data from the files stored on the computer. To counteract these types of malicious software, new security programs help detect and prevent such unauthorized access. For instance, one program uses encryption (using passwords) for every single directory on the computer, thus dramatically increasing barriers to access.

The healthcare industry is moving towards creating inter-linked networks of healthcare providers and institutions. Such linkages can provide many benefits such as consolidated patient records that can provide a complete life cycle perspective of an individual patient’s health history. Patients could access any service in the network using a smart card which could contain their complete history. But such technology also calls for systems to be in place to protect sensitive patient data. Often, the threat in such systems comes from the inside. To tackle this issue, online systems use a combination of multi-level user access and passwords. Individuals are assigned privileges that control their access to data. By requiring log-ins, the system can track usage and follow a trail to identify the culprit when a breach occurs. However, whenever large amounts of sensitive personal data is collated and stored in a single system, there are bound to be privacy concerns. A new initiative proposes issuing a unique patient identifier that will be allotted at birth and preserved the patient’s lifetime. Privacy lobbyists are alarmed at the possibilities for abuse such a system could present. Such a system could also pose a challenge to the notion of informed patient consent.
The Internet Revolution

The issue of using technology to create online healthcare systems has always been a thorny one. The biggest concern being the challenge to patient confidentiality and trust. An integrated network, or even a single online healthcare system, can help collate and analyze information in ways not possible with physical data. An online health database could mean that researchers are able to more efficiently pull together seemingly disparate pieces of information that could help in epidemiological studies and predicting health trends. However, such a database could also be accessed by third parties such as insurers, employers, marketers, and others for reasons that are unrelated to healthcare.

As the concept of managed care gains ground, there is increasing pressure to make healthcare delivery simpler and to reduce the level of difficulty associated with filing health coverage claims. While computerized, online systems make this easier, the concerns about patient privacy remains. Insurers have considerable access to patient data making it easy to build comprehensive patient profiles from a variety of information sources such as doctors, pharmacies and other health care providers. It has to be said – if it is online, the data can be found, leaving the individual patient more vulnerable to loss of privacy than ever.

Centralized Databases

Similar to the way pharmacies store information on a patient’s medications, centralized databases can keep records of a patient’s complete health history. Such consolidation of information can mean enormous savings in time and effort, as well as the availability of accurate information that could mean the difference between life and death.

While there can only be agreement that such health systems can have positive and life-altering impact, what cannot be questioned either is the paramount need for such systems to follow stringent and fool-proof security protocols at the heart of which is the need to protect patient privacy and confidentiality.

Some questions to ponder are:
- what are the ways that centralized databases of medical histories can be misused
- could prospective employer’s gain access to a person’s medical records
- how will insurers react to information about a person’s medical history, and how will this impact how the individual can access coverage

In the final analysis, healthcare networks are vulnerable to the same security threats and breaches as any other online provider. However, the difference here is that healthcare providers also have a responsibility to their patients to maintain privacy and confidentiality. The patient-physician relationship is one of enormous trust. Online healthcare systems must find a way to strike the balance between increasing efficiencies of managed care while continuing to nurture the trust patients place in them.
Assessment – Chapter 1

1) The right to privacy is a fundamental right guaranteed by the ______________ to the United States constitution (Page 1, Para 4)
   a) second amendment
   b) third amendment
   c) fourth amendment

2) What does GLBA stand for? (Page 3, para 1)
   a) Golden Laws of Boston Act
   b) Gramm-Leach-Bliley Act
   c) Graham Leach Baley Act

3) The two standards that can be used by consumers to control information sharing by financial organizations are (Page 7, para 5)
   a) Opt-in and Opt-outs
   b) Federal Medical Privacy Rule and Freedom of Information Act
   c) Non-disclosure and Complete-disclosure
Chapter 2

SAFEGUARDING THE PRIVACY OF FINANCIAL INFORMATION

Understanding Financial Data

Financial data is any data detailing a client's past and current fiscal dealings that is shared with an agent during the time of policy application or filing claims. Since this information cannot be accessed through readily available public information sources such as a phone book, it is also referred to as nonpublic financial information. Such data may also be gleaned from consumer information reports, credit scores, or even by tracking personal data entered on a company website. Financial data includes, but is not limited to, information such as an individual's income, contact details, credit history, social security number, etc.

Financial information usually falls under the purview of the opt-out standards. Therefore, an agent or company can disclose or distribute such information with affiliates or third parties so long as such intent is laid out in the privacy policy, and the client is given the freedom to disallow it. This is different from health data which is covered by opt-in standards, a detailed discussion of which follows in a later chapter. There are some overlaps between individual components of either classification of information – for example, personal contact details (phone numbers, e-mails) and social security information are protected under HIPAA and cannot be disclosed or shared without the express consent of the individual concerned. The GLBA, though, classifies the same data as financial data and allows a company or agent to use “opt-out” standards.

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

The Act which came into being on July 1, 2001, governs how client financial data may be used by companies. Also covered by this Act are nontraditional services such as ISPs, which facilitate online financial trading (stocks, bonds). Even though compliance costs are low, experts believe the rates of compliance are also low – an issue that could pose a challenge for enforcement agencies such as the Federal Reserve Bank, Federal Deposit Insurance Corp. and Federal Trade Commission. Often, the reason for non-compliance is simply that a company may not have previously been categorized as a financial organization – for example, stores will often collect data from consumers for the issuance of their credit card. This can be classified as financial data, and therefore subject to the GLBA.

Financial Institutions

For the purposes of the GLBA, a financial organization is defined as any organization engaged in financial activities or activities that are incidental to financial activities. These include banks, insurance companies, credit unions, thrifts, credit companies, insurance companies, insurance agents, broker-dealers, notification filers, mortgage lenders and brokers, pawn shops, and any institution offering financial products. According to the GLBA, all such financial organizations (or "covered entities") are required to put in place adequate measures to protect the privacy of client data as well as non public personal data.

Further, the GLBA allows several of these entities such as banks, brokerage firms, and insurance companies to merge their operations. What these means is that any affiliate can sell services or products of any other affiliate. So, a bank can well offer its clients an insurance product. For the client, this can mean ease of management, consolidated statements and accounts, and a reduction in service charges. However, on the flip side, such merged entities can also share consumer data without restriction among themselves, or even share
or disclose it to other third parties. This represents reduced control of private information for the client, and consequently, poses a higher privacy risk.

All financial organizations are required to draw up and share a privacy policy that details the institutions policies with regard to consumer data, and also consumer rights with regard to these policies. This policy must be shared with new customers when entering into the client relationship, and every year subsequently. Consumers must also clearly be notified of their right to “opt-out” of sharing or distributing of their nonpublic data to any third party that is not an affiliate. Distribution of such information among affiliates is permitted by the GLBA. An agent or company may also disclose private client financial data to a third party for the purposes of finding a product or service for the client. The GLBA is only applicable to individual client information and not to the overall business.

Information covered by privacy laws include:
- account information
- securities listings
- any transactions to do with financial products or services
- any information provided to a financial organization by a consumer in order to procure a product or service
- any information procured by a financial organization while offering a service or product to a client

Privacy Warnings

Once the GLBA was in place in July 2001, every financial organization was expected to send out privacy warnings to all customers. Companies are also to send periodic notices at least once every year. Where a customer has multiple accounts, a single notice may suffice. Given the affiliate arrangement, a customer could even receive a privacy notice from an institution with which he does not have a formal relationship.

The privacy notice must be sent to each individual customer in hard copy or electronic format; the institution cannot simply put up a notice onsite. A single notice may include several announcements covering confidentiality, information disclosure, and opt-outs. Therefore, it is up to the individual to stay vigilant and take appropriate measures to safeguard his/her privacy. There are no prescribed guidelines or formats. The regulation only states that privacy notice be clear and conspicuous and designed to call attention to the nature and significance of the information contained.

Asking for a Privacy Policy

A consumer is entitled to view a company’s privacy policy either if he is an existing client, or when he enters into a client relationship with the institution. A consumer who is considering a relationship with an institution may request to see the company’s privacy policy but can be refused. In order to receive annual privacy notices, an individual must have an ongoing relationship with the institution also referred to as a customer relationship. Where a consumer only has a consumer relationship, i.e. a one-off transaction, such as withdrawing money from an ATM, the institution is not mandated to provide privacy notices except where there is intent to share personal financial data with third parties.

Joint Accounts

Where an account is held by more than one person, each individual may exercise the right to opt-out. If both or multiple parties wish to opt-out, separate notices must be provided. Consumers should ask for and carefully review an institution’s privacy policy specific to joint accounts.
Closed Accounts
Where an individual has closed an account, the financial organizations are not obligated to send disclosure or privacy notices. However, for an existing customer, an opt-out notice would remain valid even in the event was later closed. Any new accounts, either with the same financial organization or another one, would require the issuance of separate privacy policies.

Explaining the “Opt-Out” Option
Once a privacy notice has been received by a customer, he is allowed reasonable time to act, usually 30 days. Customers should note that any response must reach the institution inside that 30 day period, not be dispatched within thirty days. Those individuals that have just a consumer relationship with the financial organization may have different time frames to respond; sometimes, even immediate. No matter what the customer type, to choosing to opt-out means that the individual has implicitly consented to the sharing of personal financial data by the financial organization. Any individual may exercise the right to opt-out at any time; however, the confidentiality and privacy clauses will not apply to any personal data prior to that date.

The financial organization is also expected to provide the customer a reasonable way to opt-out, usually through check boxes in notices, e-mails, toll free numbers or printed/online response forms. Written letters are not considered reasonable means. The burden to follow appropriate processes as defined by the individual financial organization rests on the consumer.

Information that May be Disclosed
Legally, a financial organization need only inform the consumer of the various types of information it gathers or shares/sells. So, a customer can be told that data such as phone numbers, emails, income, etc. may be disclosed, but may not know all such information that is being shared. Therefore, unless a customer specifically opts-out from the sharing of any and all data, information such as previous debt/s, mortgage and alimony payments could be disclosed. However, the GLBA prevents a financial organization from disclosing specific access codes and account information that may be used by tele or direct marketers.

There is even more ambiguity regarding medical information. While the Department of Health and Human Services regulations apply to any health-related organizations, they do not apply to medical information gathered by financial organizations. So, if an individual uses his credit card for a health-related transaction such as a bill payment, that information could be recorded and disclosed by his financial organization.

The level of protection and privacy assured may differ by each state. Some states disallow the selling of personal data by an insurer to a financial organization. Other states have stricter rules governing insurance that offers greater protection of medical information.

Besides specific individual transactions, companies compile consumer information from multiple sources such as reporting agencies, consumer reports and records in the public space. Such information is accessed freely or bought from companies that specialize in consumer data. Companies usually use personal data to profile a consumer, used for targeted marketing of other products and services. Between the information supplied by the consumer himself, and that which can be accessed or bought, a financial organization can pretty much obtain the complete financial, medical, and social history of that person.
Consumers should also be aware of exactly what types of information, and how much of it, is protected by an opt-out clause. For example, consumer information can be shared without consent with a marketing company if the financial organization has a formal affiliation with such a company. However, the GLBA states that the privacy notice should adequately explain and elaborate the opt-out standard under the Fair Credit Reporting Act (FCRA). Thus, a consumer can prevent the sharing of some information, such as credit worthiness, with an affiliated company. However, privacy protection is still limited since information about transactions and experience may still be disclosed without consumer consent. Federal regulations also prevent the sale third parties of credit header information by a credit-reporting agency (CRA). Included are data such as name, contact information, social security information, etc. The issue is a contentious one with several CRA’s filing claims disputing the restriction.

Remember, ultimately the onus of preventing data from being shared or sold lies with the consumer. A customer may still register objections to the use of personal data by the financial organization even in cases where such use is legally permitted.

Safeguarding Personal Financial Privacy
As stated earlier, protecting personal privacy is up to each individual. Simple rules work best. Carefully reading a financial organizations privacy policy for instance. Understanding and exercising the right to opt-out if deemed necessary. Consumers should also fully grasp the different nuances in the privacy regulations that govern how financial organizations deal with personal data. Also important is to understand how rules affect affiliates and third parties. While transacting with a consolidated entity may save time and effort, a consumer should take into account how such consolidation impacts personal financial privacy. Prevention is the best policy when it comes to data protection — once private information has been shared, the consumer has very little control on where and how it is used.

Legal Action against Financial Institutions
While the GLBA does not provide consumers with a private right of action, i.e. the ability to file a legal complaint, a number of state laws provide provisions that can help a consumer claim a violation of personal rights.

A consumer may lodge a complaint with one of seven federal agencies. These agencies have legal authority over financial organizations, and may bring action against an institution if it is found violating GLBA regulations. These agencies are independent and can neither act as a consumer representative nor provide legal advice.

Federal Agencies
- Federal Deposit Insurance Corporation (FDIC)
The FDIC provides coverage to deposits made by consumers in savings associations and banks. The FDIC, in conjunction with other federally-run banking agencies, conducts frequent checks of these institutions to ensure they follow sound financial practices and comply with consumer protection regulations.
- Board of Governors of the Federal Reserve (Federal Reserve)
The Federal Reserve functions as the country’s central bank. It is responsible for monetary policy and the regulating of banking institutions.
- Office of Thrift Supervision (OTS)
The OTS, a U.S. Department of Treasury agency, controls thrift institutions that are state chartered such
as savings banks as well as savings and loan companies.

- **Office of Comptroller of the Currency (OCC)**
  The OCC is also a U.S. Department of Treasury agency. The OCC licenses, controls, and oversees all national banks, including federal branches of international banks.

- **National Credit Union Administration (NCUA)**
  The NCUA monitors and checks federal credit unions. These unions are not-for-profit, financial co-operatives.

- **Securities and Exchange Commission (SEC)**
  The SEC is responsible for monitoring equity markets which include stock exchanges, broker-dealers and their affiliates, as well as investment advisors.

- **Federal Trade Commission (FTC)**
  The FTC investigates issues relating to consumer protection and fraud matters that do not fall under the authority of other federal agencies. This jurisdiction extends to credit reports, credit repair services, debt collection, lending, telemarketing, and others.

The recent *Standards for Safeguarding Customer Information* adopted by the National Association of Insurance Commissioners fulfills GLBA norms that require insurance regulators keep a check on how insurers protect consumer private information.

**Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act of 1999 allowed commercial banks, investment banks, securities firms and insurance companies to consolidate. The key rules under the GLBA govern the collection and disclosure of customers’ personal financial data by financial organizations. It also requires all financial organizations to design, implement and maintain safeguards to protect customer information. This applies not only to financial organizations that collect information from their own customers, but also to financial organizations – such as credit reporting agencies – that receive customer information from other financial organizations.

Financial institutions are defined under the Act as companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. However, health insurers are exempt from the jurisdiction of the seven federal agencies that regulated the GLBA. Each state can identify relevant insurance authorities to regulate health insurers within that state.

**Title V of the GLBA**

This includes specific provisions that govern privacy of insurance transactions. Title V, Subtitle A, Section 501, states that *each financial organization 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 data.*

Accordingly, the GLBA lays out appropriate standards to be followed to:
- 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 norms are regulated by appropriate authorities. Usually, insurers in a state are regulated by the relevant office of the state insurance commissioner and state statutes.

Section 502 of Title V of the GLBA outlines provisions for the disclosure of personal data. A financial
organization cannot share or otherwise distribute nonpublic personal data to third parties that are not affiliated unless:
- a privacy notice is given that clearly informs the consumer that personal data may be shared with third parties;
- the consumer is made aware of opt-out standards, and is also given the opportunity to do so;
- the consumer is provided adequate information on how to opt-out from allowing the financial organization from disclosing his/her personal data

Any third party that is not an affiliate of the financial organization may not disclose nonpublic personal data further to other third parties that are similarly not affiliates of the institution. Such disclosures are only legally permitted if made by the financial organization itself, with client consent.

Below are excerpts of specific rules governing the disclosure of nonpublic personal data:

(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 organization, 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 organization'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 organization, 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 data 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 organization for examination, compliance, or other purposes as authorized by law.

Section 503 of Title V of the Act, also requires that financial organizations give a clear and conspicuous disclosure to consumers about how the financial organization deals with nonpublic personal data:
· and how it is shared with affiliated third parties and other non-affiliates;
· of former consumers; and
· of current consumers and the measures in place to safeguard such information

The notice of disclosure must contain:
· the processes by which the financial organization shares nonpublic personal data third party non-affiliates;
· the individuals or groups such information may be shared with;
· how private data of ex-consumers is dealt with;
· the various types of personal data gathered by the institution;
· the financial organization’s privacy and confidentiality policies; and
· other requirements as mandated by the Fair Credit Reporting Act.

The regulation of any insurer according to the Act is the responsibility of appointed state insurance authorities.

Section 521 of Title V of the Act regulates how confidentiality of consumer data at financial organizations is maintained. Consumer information may not be procured through false means, including:
(1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial organization;
(2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial organization; or
(3) by providing any document to an officer, employee, or agent of a financial organization, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

Law authorities seeking consumer information in the course of their official duties are exempt from these restrictions. These exemptions also apply if insurers, or any employee or official thereof, seeks customer 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.

According to Section 523, any willful violation of the norms of Section 521 can lead to a fine or imprisonment, or both.

**Fair Credit Reporting Act (FCRA)**
The FCRA regulates the generation of credit reports, and consumer and investigative consumer reports. Originally put in place in 1970, the Act has since been amended.
Some of the provisions and definitions of the Act are below:

General definition:
(1) The term “consumer report” refers to any communication, written, oral, or otherwise, by a consumer reporting agency that reflects or investigates a customer’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].

Exclusions:
(2) The term “consumer report” excludes
(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 outlines the definition of “investigative consumer reports”, also known as inspection reports.

General definition:
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.

How Consumer Reports May be Used
Under the FCRA, consumer reports are regulated by strict restrictions on their use. For insurers, such reports may be used if it is being used primarily to underwrite an insurance policy for the concerned individual.

Providing Consumer Reports
Under the FCRA, when a consumer report request is not made by the client, the report may be provided by the
relevant reporting agency provided the customer has authorized such a release, and the report will be used for what the customer believes is a “firm offer of insurance.” Where such a report is issued because a “firm offer of insurance” exists but the release of the report has not been authorized by the consumer, then the report should include only the customer’s name and address which is provided only to confirm the identity of the customer. The report should not include any other information regarding the customer’s credit history or experience.

**Consumer Report Exclusions**

Consumer reports, whether generated on consumer request or authority, may not include the following:

- information on any bankruptcy that happened over ten years prior to the report;
- information about any arrests, civil suits or judgments more than 7 years before the date of the report of the governing statute of limitations has expired;
- any liens on paid tax that were cleared 7 years prior;
- any collection accounts or profits/ loss 7 years prior; and
- any damaging information dating back 7 years prior. The exception here is information on previous criminal records and convictions.

**Sharing Investigative Consumer Reports**

Before a consumer report can be compiled, there must be a clear disclosure to the consumer detailing the nature of information it will contain and its extent. Such a disclosure must:

- be made in writing;
- be sent to the consumer within 3 days of the request date; and
- inform the consumer about his/her rights to more information about the reason the report is compiled.

In the event that a consumer requests more information about the investigation and its scope, the individual who requested the report must respond, in writing, within 5 days of such a request.

**Consumer Disclosures**

If a client should so request, a consumer reporting agency, as mandated by FCRA, is required to divulge the following:

- all information that is in the customer’s file. Risk predictors such as credit scores need not be disclosed;
- sources from where the information was compiled which may be asked to be presented in court during the discovery process. Information being used only for an investigative consumer report is exempt.
- information on any individual that may have requested a similar report over the past year; and
- specific information that were contributing factors in compiling a negative report. These could include dates on which checks were issued, original payees and check amounts.

A reporting agency is also required to include a “Summary of Rights” in addition to the disclosure. Such a Summary includes:

- a short explanation of the FCRA and applicable consumer rights;
- information on exercising of these consumer rights as laid in the FCRA;
- names and contact information of federal enforcement agencies;
- a notice informing the consumer of potential rights under state laws; and
- notice that a consumer reporting agency may retain in the report any information that may be negative but that is accurate.
**Challenging Information in a Report**

In the event a consumer challenges the content of a consumer report, the agency is required to conduct a fresh investigation at no extra charge. The agency usually has 30 days within which to verify the information being disputed and to remove any information found inaccurate. If the agency deems a request frivolous or immaterial, such a request may be denied.

**Limitations on Investigative Consumer Reports**

A consumer agency must thoroughly verify all information before compiling any subsequent consumer report. Harmful information must be deleted from the report unless specifically re-checked, or if such information was gathered in the preceding 3 month period of the report.

**Using Consumer Reports: Some Guidelines**

Insurance companies frequently use consumer reports in the process of underwriting. Such uses are regulated by the FCRA, especially in instances where the report may contain information that ends up being damaging to the potential client. In such cases, insurers must:

- give the consumer notice of such action either orally, electronically or in written format;
- give the consumer the name and contact information of the consume reporting agency that compile the consumer report with a disclaimer that the agency cannot provide additional information on the reasons for an unfavorable action;
- give the consumer notice (orally, electronically or in written format) of his rights to a copy of the report, free of charge, and to challenge the veracity and comprehensiveness of the information it contains.

**Using Consumer Reports Responsibly**

When using a consumer report in the process of an insurance matter that has not been prompted by a consumer, and that may be classified as a “firm offer of insurance”, the consumer must be provided with the following:

- a written statement which informs the consumer that information derived from a consumer report was referred to in finalizing the transaction, and that such a transaction had been completed because the consumer had met the eligibility criteria for the insurance product being offered;
- a disclaimer reserving the company’s right to rescind the offer of insurance should the consumer not satisfy insurability criteria;
- a notice of the consumer’s right to prevent any information in a consumer report from being disclosed in other insurance or credit transactions initiated by parties other than the consumer.

The individual or company offering the insurance product, must maintain a record all the criteria used to evaluate eligibility of consumer for the offer for up to 3 years from the date of the offer. This record may also include information on the consumer’s credit worthiness and insurability, and details of collateral provided as a prerequisite for insurability.
Assessments – 2

1. The burden to follow appropriate processes to safeguard the privacy of nonpersonal public information as defined by the individual financial organization rests on the ------------------. (Page 18, Para 2)
   a. Insurer
   b. Enforcement authority
   c. Consumer

2. The regulation of consumer reports and credit reports is done by the (Page 18, Para 6)
   a. ICRA
   b. FCRA
   c. ECRA

3. Who regulates the implementation of GLBA regulations at financial organizations? (Page 19, Para 7)
   a. State governments
   b. State-appointed enforcement authorities
   c. Federal agencies such as the SEC
Chapter 3

HEALTH INFORMATION PRIVACY and PROTECTION

Medical Records - Their Importance

Information about health and medical records sometimes disclose the most personal aspects of an person's life. Along with information both diagnostic and testing, the medical record also involves the details of an individual's familial history, genetic tests, history of conditions, diseases and treatments, drug usage history, sexual practices and orientation, and tests for sexually transmitted disease. Subjective remarks upon a patient's manner, character, and mental condition are also at times, part of medical records.

Medical records are also acts as primary source for a lot of health care information looked for by people not directly involved with health care delivery. This data is important information about health care can influence decisions on a person's access to credit, an admit into educational institutions, and their ability to become employed and obtain insurance. Inaccurate entries in the information, improper disclosure of the same, can deny a person entry to these basic requirements of life, and may pose a threat to a person's financial and personal well being.

Around the same period, comprehensive and accurate health care information has been and is crucial to the quality of delivery of health care, and to the patient-physician relationship. Many people believe that the effectiveness of health care relations is dependent on the patient's understanding that the recorded information with a physician would not be revealed. Without these clarifications, many patients may refuse to give physicians certain kinds of information required to provide appropriate care.

Rights of Information Privacy

Privacy, confidentiality rights have been defined largely dependent upon the definitions provided for the health record and the decision as to who actually owns it. A generalized definition of a record is any information that is collected and utilized to diagnose or outline treatment of a patient's health issues. State statutes, federal law and case laws regulate the use and ownership of medical records and medical data of patients. Some statutes and commonplace law doctrines are applicable to any type of medical record stored in any kind of medium; others look to have little to no application with regard to electronically stored medical records. Still others are applicable only to records that were recorded and maintained by specific types of providers.

The laws which exist attempt to protect the individual's privacy by prohibiting or limiting the disclosure of knowledge which may identify a person or which may make public, private facts about a person. The federal laws that apply, like the Privacy Act, mostly regulate permitted usage by government employees and agencies, or uses of specific narrowly defined kinds of medical information. Few state laws allow widespread applicability, concentrating alternately on certain kinds of information like HIV results or specific types of providers. In many state laws, the creator/originator of medical records usually is the one the records are owned by. This kind of ownership, is almost always subject to the patient's best interests with respect to information within the record. Simply put, a patient has a right to limit (not always absolute) or define the disclosure of the medical records.
He may order the release of information or may wish that the information be kept private, all subject to exceptions.

In a clinical data management atmosphere, where no individual entity creates the medical record, it is ambiguous with whom the medical record's ownership lies. It's also not clear, as non-treatment associated data are also included in the patient's records and as further records are recorded, just what comprises the individual's medical record. A whole bundle of rights to privacy is based on common, ethical law along with statutory requirements - those of which protect the patient's privacy or autonomy in an individual's medical record. It is useful to comprehend these privacy rights as what a few commentators have deemed "information privacy rights."

**Doctor-Patient Confidentiality**

The doctor-patient relationship is confidential. If it were not the case, the patients would be hesitant to reveal information required for the diagnosis and subsequent treatment of their problem. The physician is obligated to keep medical records of patients private and confidential, a practice derived from ancient physicians' oaths, presently retained at its core, and also, further recent legal acknowledgment that a patient has a right to maintain that information as private that he/she desires to be maintained private. Many states' physician license statutes require that, except when the laws otherwise require and unless directly involved with the care and treatment of a patient or consented by the patient being treated, a physician should keep all client information private. Pennsylvania, for example, requires that a doctor undergoes the disciplinary process for "revealing identifiable information, obtained as a result of a doctor-patient relationship, without previous individual's consent, except authorized and required by law." Courts in multiple states have also held hospitals to the same obligation, following a contractual or fiduciary obligation to an individual, or as provided for in a contract.

The indispensable norm of the doctor-patient relationship is confidentiality. Rules of doctor patient confidentiality and other similar doctrines protect an individual's privacy rights. Confidentiality is a very significant and relevant mechanism by which an individual's right to privacy will be respected and also maintained. Privacy protection, isn't absolute however. Privacy may be conditional upon the public's justifiable right to information, or a legitimate interest by the government, specific information. It can be waived away or consented by the individual concerned. A consent or waiver should be a result of the decision that is made following being informed of all benefits and risks of the disclosure. Confidentiality, privacy and informed consent principles are nothing novel in health care or a medical records manager. Clinical Data Management systems, however, form new or exacerbate existing legal problems. From the 1970s till the present, groups like Privacy Protection Study Commissions have investigated privacy protection in electronic health medical records systems. They also advocate a number of safeguards that are as guidelines to system planners of CDM. As an example, AMA's Current Opinions necessitate "the utmost effort as well as care" in order to safeguard the confidentiality and privacy of electronic medical records. Amongst the AMA guidelines are instructions that both the doctor and patient be given advice about the existence of computerized electronic medical databases. The AMA also requires that this medical information be given to the patient as well as doctor prior to the physician releasing the information into the database. Most important, the AMA characterizes full revelation to the individual of the information as expedient to procuring the patient's completely informed consent to the treatment prescribed.

The CDM systems must outline, define and ensure security, which is defined as per Task Force for National Information Infrastructure as the safeguards in totality within an electronic-based information system. Methods must protect both system and information contained from access which is unauthorized and abuse, and inadvertent damage. It comprises of software, hardware, policies for personnel, policies for information
management, including disaster readiness.

The most effective kind of CDM system has design safeguards, which will ensure the respect of privacy rights. Ways of achieving it include:

- Execution of User Agreements which indicate specific obligations of users concerning system access and use, collection and dissemination collection of the patient's information
- Establishment of employment and institutional policies that outline non-permissible and permissible uses of patient's data and establishment of mechanisms that review and enforce the policies
- Re-design of patient consent and releases forms which enable patients to agree to release and utilization of information which might be easily linked with the patients and can be used for, treatment, diagnosis, quality assurance, utilization review and reimbursement
- Public-key encryption usage in information to ensure safeguarding of information and data creator identifiability.
- Blockage of user access, via various security stages of to data fields, access codes, or records in an unauthorized manner subject to the patient's consent
- Establish mechanisms for patient accessibility to all the information collated that identifies the patient and introduce and enforce methods which enable patients to correct and verify erroneous information.
- Usage of patient identifiers apart from the social security number of the patient in order to make sure that users (unauthorized or authorized) may not gain access to and collate records that they did not intend to access

When health care delivery processes integrate and managed healthcare pervades the market, the ability to assimilate, interpret and distribute health care data tends to become a highly critical challenge of quality, cost-efficient, outcome-driven healthcare delivery. CDM systems allow health care organizations, payers and employers, through a core data storage system, to deliver and manage better care to employees, patients, and the insureds. CDM planners should find a commonality, in terms with protection of privacy, to comply with often contradictory and differing regulatory and statutory requirements.

**Client Privacy and Medical Records**

Individual medical and health data can be assimilated, collated in a repository, distributed and analyzed in unprecedented numbers and put to varied uses. Payers can utilize patient data for patient payment of claims. They use health data for underwriting, utilization review and patient coverage decisions. The employers utilize health data in reducing their costs of health care and costs of worker's compensation, in addition to pinpoint employees who might become more expensive in the future. Providers of health care utilize the data to research, to take reimbursements, coordinate the diagnosis and the treatment, conduct assurance of quality and also monitor other providers. Repositories of clinical data and management processes will likely bring down costs of health care and better the quality of patient care. The clinical data management processes and increasing automation in the EMR area also present important patient confidentiality and privacy issues, among others, that the executives and planners should recognize. Understanding these areas ensures that EMR and CDM systems are effective and useful without revealing its users and hosts and exposing both to liability.

**Privacy of National Patient Record**

Each time a person sees a doctor, and admitted to a medical facility, goes to a druggist or sends a reimbursement request to a health coverage provider, a record is kept of their confidential medical information. Previously, family doctors and various health care providers safeguarded the confidentiality of the patients' records by sealing those away in file storage and refusing to show them to others. Today, the disclosure and use
of this knowledge is protected by patchy state rules, leaving loopholes in patients' confidentiality and privacy protection.

Congress realized the need for nationwide standards in patient record privacy in 1996 when the body brought about an Act regarding Health Insurance Portability as well as Accountability in 1996 (the HIPAA). This law included provisions crafted to save money in health care businesses via encouragement of electronic transactions, however, it also required newer safeguards to protect confidentiality and security of that data. The laws gave Congress until the 21st of August, 1999, to pass legislation regarding comprehensive health privacy. When Congress didn't enact such legislation even after 3 years, the Health - Human Services department (HHS) was by law required to craft these protections by regulation.

HHS proposed regulations that guaranteed patients new protections and rights in opposition to the disclosure or misuse of their records in November 1999. President Clinton in December 20, 2000, presented the final draft of medical privacy rules and regulations proposed by the HHS. These rules and regulations are the very first type of federal privacy protections regarding health information and would be applicable to both electronic and paper health records. HHS began writing the regulations when the Congress didn't pass the federal legislation regarding medical confidentiality and privacy on 21st August, 1999.

December 2000 saw HHS issue a last rule that made important changes to address issues that were raised in reference to comments given by the public. The provisions to ensure that final rule would safeguard patients' privacy without forming unanticipated consequences that may harm the patients' access to quality health care, Tommy G. Thompson HHS Secretary, threw open the final rule to public opinion for thirty days. When that comment period lapsed, Secretary Thompson and President Bush allowed the final rule to be effective on 14th April, 2001, as it was scheduled, and made appropriate revisions during the following year to correct potential problems and clear up the requirements that could threaten the availability or the health care quality. HHS had issued its initial guidance set to answer common queries and clarify confusion with regard to the final rule's requirements on 6th July, 2001. As mandated by HIPAA law, most entities covered have two complete years - until 14th April 2003 - to fully comply with requirements of the final rule. HHS has the authority, by law, to form appropriate changes in the final rule prior to date of compliance.

HIPAA requires that the final rule cover health care clearinghouses, health plans and providers of health care that conduct certain administrative and financial transactions like invoices and fund transfers electronically. Every health record and various individually identifiable medical information which is disclosed or used by covered entities, whether in electronic form, on paper, or verbally, or any form come under the purview of the final rule. In the final rule, the patients would have relevant new powers to control and understand how their information pertaining to health is used:

- Patients can see and access copies of their individual health records, and can request for amendments. They may also have a history in non-routine disclosures that must be made patient accessible.
- Health policies and providers are required to give individuals a clear written clarification of how the entity covered may reveal and use their health information.
- The patients have rights to a formal complaint filing with a health plan or covered provider, or with HHS, with regards to violations of this rule's provisions or the procedures and policies of the entity covered.
- The health care providers that see patients are required to get patient consent prior to sharing the patient's information for health care operations, payment, and treatment. In addition, patient authorization should be separately obtained for most non health care requirements and non-routine disclosures. Individuals will retain the right to ask for restrictions with regard to the disclosures and uses of their information.

With few exceptions, like the appropriate law enforcement requires, an individual's medical information may be utilized only for health requirements. Health information which is covered by final rule usually cannot be used in areas not associated with health - like disclosures to financial entities - not without explicit permission from an individual, or to employers that make personnel decisions. In general, revealing of information is limited to a
necessary minimum for the requirement of the disclosure. This provision, however, doesn’t apply to the revealing of medical records required to treatment because doctors, specialists, and various health care providers need a full record to give quality health care.

**Standard of Safeguards**

The final rule lays down the standards of privacy safeguards that covered institutions should compulsorily meet, but also extends covered entities the allowances to design custom policies and processes to meet the safeguard standard. The needs are scalable and flexible to allow for differences in the entity's business, and their resources and size. Covered entities generally must:

*Implement written privacy procedures.* Involving those that can avail of protected information, how that shall be used in the entity, and time in which disclosure of information is done. Covered entities would also need to follow steps to ensure their business associates safeguard the privacy of medical records.

*Train workers and assign a privacy official.* Covered entities are required to train their people in their privacy processes, and must designate a person to be accountable for ensuring the processes are followed properly.

*Establish responsibility for health records use and discharge.* Congress provided for penalties applied to covered entities that abuse personal health information in HIPAA. The penalties include:

- Federal criminal punishment - Congress, under HIPAA, also laid down criminal penalties for entities that were purposely abusing patient privacy. Criminal penalty can go to $50,000 as well as one year imprisonment for getting or/and revealing protected health records; up to $100,000 as well as up to 5 years imprisonment for acquiring protected health information using "false pretenses"; and $250,000 and ten years for obtaining and/or revealing protected medical records with intent to transfer sell or utilize it for commercial purpose, malicious harm or personal gain.

- Civil penalties: Providers of health plans and the clearinghouses that violate those standards will be subjected to civil liabilities. Civil penalties are a hundred U.S. dollars per violation, up until $25,000 per person/year for each prohibition or requirement violated.

*Balance privacy protections with public responsibility.* Within certain type of circumstance, the final rule allows - but doesn’t require - entities covered to continue certain existent disclosures of health records without individual authorization as a response to certain public responsibilities.

The permitted disclosures include the:

- identification of a body of a dead person
- emergency situations
- public health requirements
- the reason of death
- oversight in health care process
- research, usually limited when an authorization waiver is approved independently by a board of privacy or the Institutional Review Board of the institution
- Law enforcement activities subject to limitations.
- administrative and judicial proceedings
- activities that are related to security and national defense

All these disclosures could happen today under existing regulations and laws, although the final privacy law establishes limits and safeguards. If there isn’t any other law requiring information disclosed, entities covered will use professional judgments to resolve whether to disclose information, reflecting the entities policies and ethical guidelines.

*Provide protection for notes in psychotherapy.* Psychotherapy notes utilized only by psychotherapists are
provided higher levels of protection only because they aren't part of the health record and are not ever intended to be discussed with anyone else. Every other personal health data is considered sensitive and protected with consistency under this regulation.

**Making equivalent requirements for the public entities.** Provisions in the final rule usually apply equally to public sector and private sector entities. An example would be, both government hospitals and private medical units must be compliant with complete range of requirements, like providing notice, give rights and requiring permission for routine uses.

HIPAA law itself requires, tighter state laws (like the ones covering mental health, AIDS information and HIV infection) continue to apply. The confidentiality protections are usually cumulative in nature; the final rule sets a national "floor" with regards to privacy standards which protect all Americans, however, in some states patients enjoy additional protection. Certain circumstances where states decide through law that requirement of certain disclosures regarding health information, isn't preempted by final rule in these mandates.

**Medical Information Bureau**

MIB is non-profit, an organization comprised up of most insurance companies within the country. The collective purpose that MIB operates on isn’t to be the industry “big brother” collating all kinds of record information belonging to insurance applicants and then "black booking" them permanently if something adverse happens.

The actual purpose of MIB premises on simply safeguarding insurance companies from significantly missing information, misinformation or information with regards to underwriting life insurance. MIB codes comprises of information on medical or underwriting problems, sources of the records, the date the specific code has been reported on, and an approximate date of actual information. Codes don't contain information on the insurance entity that reported the code, what underwriting directive the insurance company followed. There is no "rated" or "decline" code. It makes no measurable difference that someone with a heart attack history in 1980 gives an application to a company that is conservative and gets declined and applies to a company that is liberal and gets regular coverage. Either way, the code to the bureau would be reported saying that this client has reported a heart attack history in the year 1980 which is found in APS.

**Health Insurance Portability, Accountability Act (HIPAA)**

Congress, in 1996, passed the Act, called as HIPAA. HIPAA is broadly scoped, addressing the many facets in health insurance, including long-term care, employer sponsored group plans, the Medical Savings Accounts, accelerated death benefits, medical insurance plans for the self-employed and more. The premise of this section dwells on “Administrative Simplification,” which is a part of provisions of HIPAA’s, and a following “Privacy Rule” created.

Administrative Simplification can be found in the HIPAA Sections 261 to 264. In its provisions, the Congress gives a directive to the HHS (the Secretary) for adoption standards for transactions such that information is exchanged electronically among medical plans and providers. The provisions require these entities covered to maintain appropriate and reasonable safeguards to safeguard the confidentiality and integrity regarding information, and to safeguard against the threat to the safety of information and unauthorized disclosures and uses. The entities are even required to enforce its workforce and officers compliance. The provisions further require that the Secretary issue standards with regard to the individuals' privacy of identifiable medical information.

A few lines within HIPAA that address these actions have spawned many a requirement for the providers of health care, health plans, and various entities working with them. The companies covered by those provisions,
called as “covered entities,” should now make public privacy notices, obtain permission or authorization for the many discourses and uses of medical information, and the entities shall be subject to compliance reviews by the HHS. They must also establish procedures and training to implement legal requirements, create notices and forms, other documents, and maintain and create processes to keep health records private and secure. Entities should keep their compliance records with the requirements of Administrative Simplification and also ready to give an accounting to the individuals associated and the federal regulatory officials.

Below, we will explore the Administrative Simplification rule, the Privacy Rule with other federal privacy laws affecting insurers. Initially, we shall look at the provisions of Administrative Simplification, the reasoning behind many of federal government statements in its key provisions. Secondly we shall examine the rule known as “Privacy Rule,” which is issued by the HHS, which puts forward the standards of privacy from within the Administrative Simplification Secretary. Other federal privacy rules follow including the set Guidance prepared for Privacy Rule which is issued by the HHS.

The Rule - Administrative Simplification

In the final rule, Privacy of Health Information of Individually Identifiable standards, known as “Privacy Rule,” puts into place the privacy requirements of “Administrative Simplification” provisions in HIPAA in 1996. The rule applies to medical plans, some health care providers as well as clearinghouses. Also included are standards with regard to the rights of patients regarding their health record information, procedures for using these rights and authorized and required use of the information given. The chapter will consider HIPAA provisions, in Sections 261-264, referred to as “Administrative Simplification.” Also provided are some insights into the thought process behind the enactment in this section of the HIPAA.

Administrative Simplification Purpose in HIPAA

Administrative Simplification Rules found in HIPAA are for the purposes below:
1. Protection and enhancement consumer right by giving access to the health information but limiting the inappropriate uses of the same information;
2. Improvement of the quality of medical care by restoring trustworthiness in the medical care process among consumers, persons committed to the deliverance of care and health care professionals
3. Improvement of the efficiency as well as effectiveness of health care delivery by forming a nationalized framework for medical privacy protection that further constructs upon efforts by, health systems, states and individuals and individual organizations.

Personal Information in Electronic Transmission form

The provisions of Administrative Simplification of HIPAA specifically, in electronic form, address information. The protection of every individually identifiable information regarding health turned into the subject of Privacy Rule, however, the actual genesis of the rules established in the issue about how easily large numbers of confidential information is stored, accessed and transmitted via the system of electronic information. Federal Register, cited earlier within the same issue that observes, “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
This an permitted dollars communities, businesses ground information disease, patients, accessibility care establish An intensive financial Health: Greater of individual access electronic System System... health:... care... health... care... health... care... health... care...

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.’ [Networking Health: Prescriptions for the Internet,’ National Academy of Sciences (2000).]

Progression into an electronic system after a paper system reduced or eliminated numerous operational and financial barriers that had previously served like a natural barrier of protection surrounding the personal records’ privacy. Allowing easy access, easier duplication, and still easier communication of data that would have previously been difficult to assemble and gain access to, expensive and cumbersome to copy, and time-intensive to share has broken down old protective walls.

As of now, because information flows easily and freely in the form of a broad and swift torrent of communication, purposeful protection of privacy regulation has turned into, according to federal government, an essential requirement. The coming of effective electronic data transmission also caters to marketing and entrepreneurial opportunity. Some of the opportunities utilize information well and might help both society and individuals. Other opportunities might have harmful potential, particularly should individually identifiable information be utilized maliciously, such as identity theft. To create the consummate “target market,” businesses might attempt to utilize private information in a way that may cause embarrassment or worse with regard to the individuals within the information they access. That is why Administrative Simplification includes ground rules of marketing standards, the regulation of what marketing uses have been prohibited and the permitted uses of health data for marketing purposes.

An additional reason for federal regulation in privacy laws is because the electronic age caused easy accessibility of information easily all across the country. This information may profit those in other states and communities, if shared by means that protect privacy rights of patients. By relying on the individual states to establish these rules, it may become difficult for those that may utilize information beneficial to many complying with contradicting laws amongst the states within which it requires to access information. It is for this reason, that Congress has passed federal regulations overseeing the protection of potentially harmful health information.

Health Care System Today

The electronic data transmission is only a single facet of the overhaul within America’s health care and medical care system across the last few decades. Previously, health care provided was largely through one-on-one interactions betwixt patients and their doctor or their clinic. These days however, the quality of managed care spawns huge integrated networks of health care delivery. These networks assimilate, process and share individual information to provide treatment. The activities result in rising numbers of people that have health data access as well. Besides the workforce inside the entity giving health care, workforces of entities which perform specific duties for the provider of health care, like billing, have data access as well. Employers also
often do certain duties that relate with health plans they provide, such as processing of front-end of claim forms, enrollment forms and thus employer workforces might also have health information access. Other companies with health information access to may include clinical laboratories, pharmacies, life as well as health insurance companies, medical information and self-insured employers.

Prior to enactment of Administrative Simplification, no rules governed how health data was used by second tier and third tier users. An example would be, a pharmacy received health information to confirm if an insurance plan is able cover a prescription, then use that data to market relevant products of companies to the patient. Federal Register: 28th December, 2000, Volume 65, No. 250 listed recent privacy breaches to demonstrate the requirement for privacy regulation:
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).
- 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 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).
- 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).
- 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).”
- 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).

The ever-growing amount of health information, easily accessed by an increasing population, is grounds for the Congress to authorize passage of provisions of Administrative Simplification under HIPAA.

**Effective Health Care and Privacy**

Protecting the health information privacy avoids misuse, not authorized use, harm and embarrassment, and may also contribute towards the provision of better effective health care. The cornerstone of providing efficacious medical care is the complete understanding of the patient’s condition. Should the patient be concerned with regard to the ways with which her or his medical information may be utilized, the patient is inclined to conceal more intimate and private details of their medical history. Patients should confide in their physician and health care provider sufficiently so that they can provide them a complete health, symptoms picture and medical history, including other minutiae in their lives. If the patient doesn't provide accurate and full information, a provider of health care may prescribe a regimen of treatment that is fully inappropriate for an individual.

Also significant for the public health activities is accurate health information. Accurate and complete information is required by agencies of public health and all involved with public health drives to recognize
public health trends, to evaluate public programs as well as plans. A health insurance field also needs correct information to enable relevant underwriting, identification of fraud, and claims processing. Researchers conducting research need accurate information. Protecting utilization of medical information and its disclosure should indicate a higher likelihood of the fact all entities would not be given false or incomplete health data from individuals who are afraid it will be employed in inappropriate or improper ways.

**Harmful Use of Medical Information**

Federal Register has cited several instances in which health information was abused in an obviously harmful manner:

- 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 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 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).”

Congress enacted Administrative Simplification due to the above examples of health information abuse.

**Part C - Social Security Act : Administrative Simplification**

The first part in the provisions of Administrative Simplification, §1171, provides important terms and definitions, within the law are:

**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 non standard 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.

The section 1172 is applicable to the standard within Administrative Simplification, Part C, to health plans, the health care providers as well as health care clearinghouses that transmit health information connected to transactions as referred to § 1173(a)(1). It includes as well procedural requirements the standards' adoption.

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 rule making procedures of sub chapter 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 Work group 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).

The section 1173 mandates that HHS Secretary adopt standards in transactions to help health information be given electronically. The section 1173(a)-(1) finds and confirms the transactions these laws cover, which include other transactions appropriately determined by the HHS Secretary. It requires the HHS Secretary to also adopt specific stands in unique health identifiers, security standards, code sets, electronic signatures, and information transfer between health plans. The section 1173(d) part of the Law is one that specifically requires covered entities to keep appropriate and reasonable safeguards to make sure of the confidentiality and integrity of information, safeguard against anticipated threats within reason or security hazards or information integrity or the unauthorized disclosures or uses of information and also to make sure of Administrative Simplification compliance by the entity’s officers as well as its 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 dis enrollment 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

(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.

The section 1174 mandates that the HHS Secretary establish standards on specified dates, dependent on type of transaction. The final rule in these transaction standards, referred to as Transaction Rule, had not been promulgated till August 17, 2000, post the specified date. Roundabout 17,000 comments had been received as responses to the rule proposed and the HHS tried to address those and build a consensus regarding the standards in the industry.

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.

The section 1175 deals with Transaction Rules as well and forbids health plans from denying to delay or to process transactions given in standard format. A compliance timetable is established as well.

§ 1176-Civil penalties in violation of Part C are

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.

The section 1177 penalties for knowingly utilizing a health identifier, or getting or revealing individually identifiable health information, 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.

The section 1178 issues that statements of Part C, any standards, implementation, specifications taken under Part C, will preempt contrary law of state. Should state laws (1) be necessary, as confirmed by the Secretary, in certain purposes that are set forth within the statute, (2) take into consideration controlled substances, determined by HHS Secretary,(3) are contrary to the federal law and more stringent than the federal law, they would not be preempted.

**THE 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—
(II) to prevent fraud and abuse;
(III) to ensure appropriate State regulation of insurance and health plans;
(IV) for State reporting on health care delivery or costs; 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.

The section 1179 says provisions set forth within the provisions are inapplicable to financial institutions during “authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.”

Section 264 is a provision in HIPAA which addresses provision of Administrative Simplification. The Secretary is required to issue the standards regarding privacy of health information that is individually identifiable.

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 supersede 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.
Privacy Rule

Privacy Rule - A Summary

The final regulations needed under Administrative Simplification are effective as of 14th April, 2001. These rules are usually referred to as “Privacy Rule.” The covered entities under Privacy Rule covers include health care clearing, houses health plans, and the health care providers that conduct specific administrative and financial kind of electronic transactions. Medical plans include health insurers, HMOs as well as group health plans which include welfare benefit plans for employees. Health care clearinghouses entities process medical information from a payer to health-care provider. The kind of information protected by these rules include every medical record and health information that is individually identifiable, used and revealed by covered entities, whether it is electronically, or orally, or on paper.

The Privacy Rule will be applicable equally to both private and public sectors. Usually, if laws enforced in states are stronger than federal laws with their regulations, then state laws apply. Types of health data that are protected under Privacy Rule are those that:
1. relate to an individual’s physical / mental health, or of health care payment, the provision of health care
2. identify or can be used to pinpoint, the person that the information is about
3. may be received or created by a covered entity and
4. can be maintained or transmitted in any medium.

Privacy Rule presents the initial federal rules with regard to protection of health data privacy and guarantee patient accessibility to information that have been drafted. States have enforced privacy regulations regarding protection of health data, but state regulations usually apply only to specific types of conditions, like mental illness, HIV and AIDS, cancer and other specified condition. These federal rules are far broader than those to be seen in most state’s regulations.

Privacy Rule enables patients to have accessibility rights to their medical records. Previously, patients didn’t have the luxury to review their health information as a right as well as have access to their information could be denied. Health plans and Providers are now mandated to provide patients a written clarification of how the individuals’ information may be utilized and disclosed. For providers of health care to share information regarding a patient for payment, treatment as well as health care operations. The health care provider should obtain patient permission. Specific separate authorization should also be obtained in non-routine disclosures, also most non-health purposes. Patients can exercise a right to request limitations on the use as well as disclosure of their medical information. In addition, patients have access to one's own health data, the patients also have a right to procure documentation of others that have had access to information regarding the patient. Furthermore, individuals can exercise their right to request corrections or amendments to health data that is incomplete or incorrect, however certain exceptions are applicable to these rights to access their data, such as when it would endanger the safety or life of a patient.

The rule clarifies that a patient’s health information might only be used in health purposes. Any utilization of information unrelated to health care should be explicitly authorized, obtained from the patient. Furthermore, disclosure of health data should be restricted to a minimum necessary required to achieve the disclosure purpose.

Each covered entity which is covered by Privacy Rule should adopt privacy procedures that are written. The procedure must include those that have protected data access, how it shall be used within the entity, and how as well as when the information can be disclosed. Furthermore, covered entities must instruct employees in their procedures of privacy, and must hold an individual responsible for ensuring that procedures are followed.
In the provisions of Administrative Simplification of HIPAA, usual penalties that have been laid down for the people who violate the rules and misuse private health information. Civil penalty can apply to providers, clearing houses and health plans that violate privacy standards. The penalties are $100/violation, up to a 25,000$/person/ year for each prohibition or requirement violated. Criminal penalties under federal jurisdiction are also applicable to those that knowingly violate privacy of the patient. Criminal penalties can go up to Fifty thousand U.S. dollars and up to one year imprisonment for disclosing or obtaining health information which is protected, and can be $100,000 as well as up to 5 years imprisonment. For procuring protected health information gotten under false pretenses, can be up until Two Hundred and Fifty Thousand U.S. dollars and up to ten years imprisonment for disclosing or obtaining protected medical information with the intention to sell, use or transfer the information to gain commercial advantage, or personal gain or/and malicious harm.

The rule does allow persons and covered health organizations to continue specific disclosures unless authorized by the individual for certain public responsibilities. Circumstances under which these disclosures are permitted are:

- Health needs of the Public
- Body Identification of the deceased person or cause of death
- Circumstances warranting an Emergency
- Oversight in the system of health care
- Research in specific circumstances like when approval of waiver of authorization obtained by Institutional Review Boards or privacy boards
- Administrative and Judicial proceedings
- Activities that relate with national security and defense
- Limited law enforcements

Psychotherapy notes are shielded under special rules because of the nature of their sensitivity. These notes, which should be used only by qualified psychotherapists, do not comprise a portion of medical records and are never to be shared or discussed by anyone else. Disclosures in written form are usually required, health plans cannot condition eligibility or enrollment for benefits of a patient providing authorization to use as well as disclose psychotherapy derived notes.

### The Acquisition of Consent

Specific activities require individuals' consents under Administrative Simplification and the Privacy Rule.

### Health Care Operations, Treatment or Payment

Before disclosing or using protected health data to give treatment, health care operations or payment, a provider must generally acquire a patient's consent. The provider of health care can condition treatment upon a patient providing the consent form. The health plans can condition enrollment on the provision of consent given by an individual.

### The Directories

The information, if it is provided to the directories, like the hospital's directory of patients, or next of kin or other people, the individual must have notice prior to information which will be disclosed and should have the
option to opt out of the use of data.

**Fund-Raising and Marketing**

Where the information shall be utilized for fund-raising and marketing, the covered entities must give individuals the option to opt out of additional disclosures within the time period of initial individual contact.

**Privacy Practices- Notices**

Health care providers as well as health plans should give written notice of the entities’ privacy practices, including descriptions of a person's rights regarding health information which is protected. The notice should also include anticipated disclosures and uses of the given information that can made without the individual's written authorization.

**Officials of Law Enforcement**

In certain conditions health data may be revealed to the law enforcement official without consent. An example, health information might be disclosed following a subpoena, order, or warrant issued by a judiciary officer, following a subpoena by the grand jury, or summons or pursuant to a subpoena obtained administratively, investigative demand civil in nature or a similar kind of certification if the three part test is fulfilled:

1) The request was specific and to the point
2) the information holds relevance
3) information that is de-identified cannot reasonably be utilized.

**In Research**

The researchers may be given protected data if the involved researchers’ protocol was reviewed after which it is approved by the privacy board as well as/or the Institutional Review Board.

**Administrative Simplification Regulations and the State Law**

In § 160.201 – 160.204 of Privacy Rule, the conditions in which the state law might become preempted by Privacy Rule are explained. Usually, a standard implementation or requirement of the rule is “contrary” to the state law, federal regulation preempts law of the state. The word “Contrary” has been defined as:

(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.)

The exceptions are present to the concerned general rule with regard to the preemption of s law of the state. The state should compulsorily submit to the HHS Secretary, a request for exception of the specific law from preemption, in addition the Secretary must usually evaluate the basis of request on whether the state's law:
· is required to stop abuse or fraud in the provision of the health care payment,
· to fulfill a compelling need relating to public safety, welfare or health; requires the primary purpose of the rule of the manufacture, distribution, registration dispensing or any other type of control of the controlled substance.
· to ensure the appropriate type of state regulation in insurance and the health plans, for reporting on costs, of delivery of health care

The Secretary can also ascertain that the state's laws are more stringent, more so than the Act needs, and thus the state's law would not be preempted. The phrase "More stringent" has been defined within the rules 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 sub chapter, except if the disclosure is:
· Required by the Secretary in connection with determining whether a covered entity is in compliance with this sub chapter; 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 sub chapter may be construed to preempt any State law to the extent that it 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 identifiable 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 record keeping 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.

Reviews-Complaints and Compliance

If a patient believes a covered entity isn’t complying according to the rules in the Act, the patient can file a complaint directed to the Secretary. Lodged complaint should be written, either on electronically or paper. The contents in the complaint should have the name of the entity which is believed to have been non compliant and the description of omissions or acts the entity has done that may be in violation. The complaints should generally be lodged within 180 days when the complainant was cognizant, or should have knowledge of, that
the omission or act was committed. When a complaint has been received, investigation by the Secretary may begin, including reviewing relevant policies, practices or procedures of the covered entity which is the target of complaint. Besides the investigation of complaints, the Secretary can also conduct compliance reviews concerning covered entities. The aim of the reviews is determination of whether the covered entity is regulation compliant.

If the entity has a compliance review or complaint investigation, the covered entity should:
- permit information access, including its, books, facilities, records, accounts with any other information which is pertinent to the review or investigation.
- cooperate with compliance reviews and complaint investigations,
- provide compliance reports and records to the Secretary,

Use and Disclosure

§ 164.500-534 of Final Regulations deal with the Privacy of Individually Identifiable Health Information, the basis of which is in Section 264 of HIPAA. These rules are also applicable to health care clearinghouses, health plans, and providers of health care that deliver medical information electronically as defined according to the Act.

Disclosure and Use of Protected Health Information-General Rules

A covered entity can generally disclose or use the protected health information:
- to disclose or utilize protected health data with regards to the patient.
- Should consent not be a requirement, to mete treatment, health care operations or payment?
- in compliance with the consent and the authorization requirements found within the regulations.

“Minimum Necessary”- The Standard

Usually, when the covered entity is disclosing or using protected health data, or is seeking protected health data from a second covered entity, the entity should make a fairly reasonable effort to limit protected health information to intended purpose of disclosing, using or requesting information to a “minimum necessary”. This minimum necessary rule doesn't apply to the disclosures made to a provider of health care for requests or treatment by the provider for treatment nor to disclosures to a patient, or the disclosures to the Secretary relating a complaint placed against a specific covered entity.

The disclosures necessitated by law, like when the public health authority must gather information for the intent of controlling or preventing disease, injury, etc, too aren't subject to the standard of minimum necessary.

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

The covered entity can create information which isn't individually identifiable health information using
protected health information. It can also disclose this information to a contractor or “business associate” to create de-identified health information. According to the regulations, the person who is a “business associate” is defined as:

(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.

When information is de-identified, it will be considered protected health information should a code or another means of identification of record is disclosed which would cause the data to be individually identifiable.

The Standard of Disclosure to Business Associates

The covered entity can usually disclose health data to the business associate, and might allow the business associate to receive or create protected health information for the entity, if a covered entity acquires satisfactory assurances that the business associates will appropriately protect the given information. The “satisfactory assurance” should be in the agreement or written contract between a business associate and the covered entity.

Business Associate Contracts-Their Specifications

The contract between business associates and covered entities:
- Should lay down the required and permitted disclosures and uses of the type of the information by a business associate
- may allow the business associate to give data aggregation services related to the operations of the concerned covered entity in health care.
- may allow the business associate in disclose and use of the protected health information on behalf of the administration and management of the business associate, or to perform the business associate's responsibilities of the within legal areas.
- must show that the chosen business associate shall report to covered entity any disclosure or use that isn't
allowed by contract of what it isn't aware of.
   · must show that information given to any one of its agents, which includes subcontractors, will be covered by the exact conditions and restrictions as those applicable to the selected business associates
   · must show that a business associate shall not further disclose or utilize the information other than as required or permitted by law or by contract
   · must show that a business associate will ensure appropriate measures to make sure that protected information isn't disclosed or used other than permitted by contract
   · must be shown that the entity will have the contract terminated should the business associate violate the contract or a material term in it
   · must show that a business associate will give protected health information out to the individual according to the applicable rules
   · must give the data necessary for accounting of disclosures by the business associates of the protected health information and be done according to the law
   · should show that any amendments permitted under the law are incorporated into the protected health data by the business associates
   · show that the business associates make their internal records, books and practices relative to the disclosure and use of the protected health information which is available for purpose of determining the entity’s compliance with regulations, to the Secretary
   · should provide that upon the termination of contract between the entity and business associate, if practical, all health information be either destroyed or returned, or if not practical, allow for further limitations and protections on the disclosure and use of the information

**Personal Representatives and Deceased Individual standard**

In case of the protected health data of an individual deceased, the personal representative, like an administrator or executor of the estate of the deceased, may be dealt with as the person for purposes of Administrative Simplification regulations.

Should an individual be authorized to work on the behalf of an emancipated minor or an adult in making decisions upon health care, that individual can also be viewed as the personal representative. Final regulations also deal with the issue of guardians, parents, or another person an issue of guardian, parents, or other person representing *in loco parentis* behaving as the personal representative for the child. State laws differ with respect to whether guardians or parents must be notified and or given authorization for a child to receive the health care. The federal final regulations recognize these departures by stating that should an unemancipated minor be able to consent legally to health care without parental consent or of guardian, the guardian or parent may not act the part of personal representative and thus receive protected health data about the minor. However, if the guardian or parent has the authority on behalf of the minor and deny or give authorization regarding health care services, covered entities should consider the guardian or parent as the personal representative and reveal to the guardian or parent applicable protected health data about the minor, unless the guardian, parent, or other individual representing *in loco parentis* agrees to a privacy agreement regarding health information betwixt health care provider and minor.

Covered entities have some room for circumspection regarding the information disclosure to the personal representative. Should covered entities have a “reasonable belief” in?

   · an individual may have been or has been subjected to abuse, domestic violence or neglect by the personal representative;
   · it isn't in the individual's best interests to address the person as the personal representative of the individual's,
on the basis of the entity's professional judgment can choose to not treat the person like the personal representative of individual.
· treating the individual as the personal representative would possibly endanger the individual that is the topic of protected information or health care

**Whistle blowers and Disclosures**

The “whistle blower” is an employed individual or another member of the covered entity's workforce, or the business associate who communicates to the authorities of an apparent or real violation of clinical standards, the law or the professional standards by the entity. The whistle blower may reveal that which would otherwise be deemed protected health information should the whistle blower think that the conduct the covered entity is engaged in, is illegal, or otherwise is in violation of clinical or professional standards, that the service, care, or the conditions that are provided by the entities potentially endangers workers, patients, or the public. A whistle blower could disclose this information to the authorized public health authority or health oversight agency to oversee or investigate allegations of misconduct done, or can also communicate with an attorney that has been retained to determination of legal options that are there for the whistle blower.

**Workforce Members - Disclosures by Those That Are The Victims Of Criminal Activity**

Should a workforce member of the entity’s consider himself the victim of criminal actions, he can disclose what would normally be protected health data to an enforcement official, ensuring that information disclosed regarding the perpetrator suspected of the crime is limited to the information that is used for the identification of the fugitive, suspect, missing person or material witness, which includes:
· the address and name;
· the birth place and date;
· the ABO blood type and RH factor;
· the social security number;
· the injury type;
· the time of the treatment and date;
· the time of death and date, if it is applicable; and
· the description of physical characteristics that are distinguishing, which includes eye color, gender, weight, race, hair and height, absence or presence of scars, facial hair, and tattoos.

**Group Health Plan Requirements**

Usually, for the disclosure of the protected health data, or to allow disclosure to the sponsor by a group health plan, the group health plan records should restrict the use and the disclosure of the information concerned, according to the law and the regulations.

The health insurance issuer, the group health plan, the HMO may disclose a summarized health record to the sponsor of the plan should the sponsor request the data for obtaining bids of premiums from various health plans, or to amend, terminate, or modify the group health plan.

The definition of “**Summary health information**” as defined within the final regulations: *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.

Information within §164.514(b)(2)(i), as above, usually includes:

2) Names
3) all dates that are directly related to the individual, like birth date, date of death, admission date, discharge date and so on.
4) all subdivisions lesser than a state geographically, which includes street address, county, city, zip code, precinct [§164.514(b)(2)(i)(B)]
5) email address
6) numbers of the medical record
7) fax number
8) telephone number
9) social security number
10) account number
11) beneficiary health plan number
12) device identifiers and serial number
13) vehicle identifier
14) certificate/license number
15) IP address number
16) full photographic image of face
17) biometric identifying data, includes voice and finger print
18) other unique identifying numbers, code or characteristic
19) URL

Requirements of the Plan Document

Plan documents in a group health plan should incorporate provisions:

3) which require that plan sponsor agree with the following before the protected health information is disclosed by a group health plan:

1. to establish permitted and required disclosures and uses of information by the health plan sponsor, according to the regulations
2. a sponsor won’t disclose or further use information other than which was required or permitted by a health plan, or required by law
3. a sponsor will make sure that the agents, including subcontractors, shall abide by all the same conditions and restrictions referring to the protected information as the sponsor itself
4. a sponsor will not disclose or use protected information for related employment decisions and actions or in connected to employee benefit plan or any other benefit a sponsor shall incorporate any rectified the protected health information accordingly with the rules
5. a sponsor will communicate to the plan any disclosure or use of the data of that it is aware of that isn’t allowed by the group health plan
6. a sponsor disclose information required to investigate the complaint or is required for a review regarding compliance
7. a sponsor shall make its internal records, books, and practices related to the disclosure and use of protected group health data gotten from the group health plan accessible to the Secretary to
determine that they comply with the regulations the concerned group health plan follows
8. a sponsor shall incorporate any rectified the protected health information accordingly with the rules
9. a sponsor will make information accessible which is needed for accounting of disclosures as mandated under the law
10. describe those classes of employees, etc under the plan sponsor’s control are to be provided accessibility to protected health data which is being disclosed, and any person or employee who gets the protected health information regarding payments under, the health care operations, or other matters referring to the health plan
11. a sponsor shall return or destroy the protected health information which is no longer required, if feasible, and should that not be feasible, to restrict its further disclosure and uses

Furthermore, the group health plan should provide for “adequate separation” betwixt the plan sponsor and group health plan. To accomplish the “separation,” according to Privacy Rule, group health plan documents should:
4) provide a mechanism which is effective to handle the noncompliance according to the rules by the sponsor’s workforce members or employees
5) restrict availability to the functions of the plan administration and use by the employees that which is the responsibility of the sponsor

Disclosures or Uses in Carrying Out Treatment, Health Care Operations or Payment and Consent

Usually, the provider of health care should obtain the patient's consent prior to disclosing or using the protected health information in order to give treatment, health care operations or payment. If the health care providers have a relationship termed “indirect treatment relationship” with a patient, the provider of health care doesn’t need to get consent before disclosing or using protected health data for these purposes. The term “indirect treatment relationship” has been defined according to the regulations to be: 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 provider of health care who has an indirect treatment relationship will behave on the basis of authorization or consent obtained from the patient as a relationship of direct treatment with the individual.

A provider of health care can also disclose or use protected health data with no prior consent if in an emergency, should the provider of health care attempt to get permission quickly within reasonable limits. Furthermore, if a covered provider of health care is mandated by law to give treatment to the person and attempts to get consent but isn't able to get consent, the provider of health care may disclose or use the protected health information for the aim of treatment, health care operations or payment.

A covered provider of health care is able to disclose or use the protected health information with no consent to give treatment, health care operations or payment if the attempted to obtain consent by the provider has been made but to no avail, the provider of health care may disclose or use the protected health data give the treatment, health care operations or payment. A covered provider of health care may also disclose or use the protected health information with no consent for treatment, health care operations or payment if the health care provider attempted to gain the consent but isn't able to because of substantial barriers in communication
with the individual, the provider of health care concludes that the patient's consent to get treatment is assumed in the circumstances. Within circumstances where a provider of health care is not able to gain consent, and in its stead, follows the regulations relating to these circumstances then carries out treatment, health care operations, or payment, the health care provider should keep documentation with regard to the attempts made to get consent, and the reasons or reason why consent was not obtainable. A covered provider of health care may require permission as the condition to enroll a patient in a health plan or condition for provision of treatment. Consent for disclosure and use of the protected health data may be compounded with different types of legal authorizations from the patient as long as consent is organizationally and visually separate from all other separately dated and signed written legal permission by the individual. The covered entity should document and retain consents which have been signed.

Consent Revocation

Consent revocation by an individual for disclosure and use of the protected health information can be done at any point of time. The revocation however, should be written.

Requirements of Consent Content

To comply with final regulations, the consents should:

4) be written in comprehensible language
5) the individual should be informed that, if the covered entity retains the prerogative to change its privacy practices, and that the changes may occur in the practices and if it does, the individual can get a revised notice with regard to the privacy practices
6) the individual should be informed that she or he would be able to apply for a comprehensive description of practices of privacy that the entity employs and also that the patient has a right to receive notice prior to having the consent form signed
7) the individual should be informed that the protected health data may be disclosed and used to give treatment, health care operations or payment require that the patient date and sign the given consent
8) state that the patient has a right to revoke, in writing, the consent given
9) state that the patient has a right to ask the entity to restrict how the protected health information would be disclosed or used, state that the entity is not bound by law to agree to restrictions requested, and should the covered entity does consent, the restriction is considered binding on the entity

The Authorizations

Authorizations and consents differ from each other in that authorizations provide license to the covered entities to make use of specified protected health data for specific purposes, usually other than treatment, health care operations or payment, and may also provide license for the entity with regards to the disclosure of the protected health data to the third party as consent provides providers of health care with a relationship of direct treatment with an individual, license to disclose and use all the protected health data in treatment, health care operations or payment. Consent forms are less specific than authorizations and will include a date of expiry. Usually, the obtaining of authorizations should be required to reveal any data that is not covered according to the rules of consent, which means that almost all disclosures or uses apart from the disclosure or use of protected health data to give treatment, health care operations or payment by the provider of health care with which an individual has a relationship of direct treatment.
Authorizations and Psychotherapy Notes

Usually, covered entities should obtain an authorization in any disclosure or use of notes in psychotherapy, with the exception of:

- usage by the psychotherapy notes originator for treatment
- disclosure or usage by covered entities in their training programs within which practitioners, trainees, or students in mental health find out under supervision, how to improve or practice skills
- usage for determination of compliance, by the psychotherapy notes originator or to make an inquiry a complaint
- disclosure or usage by the entity to defend proceedings or legal action brought about by the patient

Contents of Authorization

For an authorization to be valid, it should have:

- the description of the data to be disclosed or used
- specific identification or name of the person or a class of persons that are authorized to disclose or use the data
- specific identification or name of the person or a class of persons the covered entity can make a requested disclosure or use to
- an expiration event or date of expiration after which authorization is invalid
- the statement that the patient has revocation rights to authorization
- the statement that data disclosed or used after authorization may be used by the recipient for re-disclosure and is no longer safeguarded according to privacy regulations
- date and signature of the patient

Unlike consents, usually, covered entities cannot place conditions on provisions of treatment, eligibility upon providing an authorization, payment, enrollment within a health plan or except in circumstances that are listed below. Authorizations may be needed by the entity:

- in research-related treatment
- if the provisions of health care are for the purposes of creating the protected health data for third party disclosure
- in determining a patient's eligibility of for risk ratings health plan or the determination of underwriting or, before the patient enrolls in the health plan
- if necessary for the determination of claim payment.

If a request for authorization is made by an entity, for covered entity to disclose the protected health data to the requesting entity for treatment, health care operations, or payment, the requesting entity should include in the authorization form, the usual elements of authorization, including the following:

- the description of every purpose of the disclosure requested
- a statement stating that an individual can choose to not sign the authorization form
- a statement stating that, apart from the permitted exceptions for the requirement of an authorization of treatment, enrollment or payment the entity shall not condition the other services upon the receipt of the authorization.

The entity should also give the individual a duplicated signed authorization.
Protected Information for Purpose of Research and Its Authorization for Disclosure and Use
The authorizations used for gaining approval to disclose and use data for the purpose of research should contain the information an authorization usually requires, including:
- the description of to what extent the data will be disclosed or used to give treatment, health care operations, or payment
- a reference to privacy notices to or applicable consents from the patient
- the description of any utilizations that go beyond that which does not require authorization or consent

Disclosures and Uses Which Do Not Require the Authorization of Consent, However, Require the Opportunity for Agreement or Objection
Certain disclosures and uses of the protected health data are permitted without a formal authorization or consent, if the individual is intimated prior to the disclosure or use and has an opportunity to either object or agree. The process of intimating the patient and obtaining objection or agreement can be oral. If the individual doesn't object, the following data may be used in a facility directory:
- name of the individual
- religious affiliation of the individual
- condition of the individual which is described in a way that doesn't provide specific medical data
- location of the individual in the facility

This data may be disclosed the clergy members. This information with the exception of religious affiliation, can also be revealed to anyone requests for the patient by their name.

Disclosures and Uses for Involvement in the Patient's Notification and Care
Specific protected health data can be revealed to member of the family, another relative, a close friend of the patient, or another person that has been identified by the patient. Information that is pertinent to the person's involvement in the individual's payment or care that is in direct relation to the health care of the patient is permitted to be disclosed or used.

Should the patient be present and capable of making decisions regarding his or her health care, the covered entity should get the patient's consent and also provide the opportunity for objections or use their professional judgment in determining that the patient would not object prior to the disclosure of the patient's health information to a family member or other person? If the individual is absent, or is not capable of giving consent, or in a situation of emergency, the entity can use its professional judgment for the determination of whether the disclosure would be in the patient's best interests, and should that be the case, disclose the protected health data that is only directly pertinent to the involvement of the person in the patient's health care. The entity may also permit the person to decide on the individual's behalf to get medical supplies, filled prescriptions, X-rays and other forms of protected health data.

Disaster Relief and the Purpose of Its Disclosure and Use
An entity can disclose or use the protected health data to a private or public entity assisting in efforts of disaster relief to coordinate with these entities any of the allowed disclosures and uses of protected health information.
Disclosures and Uses for Which Consent, Authorization, or an Opportunity to Object or Agree isn't required

Specific disclosures and uses of the protected health data can be made with no authorization, consent or providing the patient a chance to object or agree. These are the disclosures and uses:

- that are required by law for the public health authority, if not, then another appropriate government authority which is authorized to receive reports of child neglect or abuse by law
- that are for activities of public health to control or prevent disease, disability or injury report of adverse events, problems, biological product deviations or product defects required to be made by a person to the Food and Drug Administration
- to enable repairs, recalls, or replacements of a product under the Food and Drug Administration to the person who could be at risk of spreading or contracting a condition or disease, may have had exposure to a contagious disease, if the entity or the public health authority is by law, required to give the person notice.
- tracking of a product by the Food and Drug Administration required by a person to lead post-marketing surveillance in compliance with the requirements or as directed by the Food and Drug Administration
- about an employee to an employer, of an entity who is a workforce member of the employer or the provider of health care to the patient at the behest of an employer to carry out a rating related to workplace surveillance, or to rate if the patient has an injury or illness that is work-related,
- to the employer about the employee should the protected health data that has been disclosed comprise of findings which concern an illness or injury that is workplace-related medical surveillance or work-related
- to the employer about the employee should the covered provider of health care give written notice to a patient that the protected health data relating to medical overview of the concerned work-related and workplace injuries and illnesses has been given to an employer by providing the individual a duplicated notice of the notice in the time period that posting the notice at an obvious location at the location of health care provision.
- to the employer about the employee should the employer require the information to be in compliance with workers compensation or other laws.

Victims of Domestic Violence, Neglect or Abuse and Disclosures

An entity can reveal protected health data regarding the individual who is believed to be, within reason, by the covered health care provider to be an abuse, domestic violence or neglect victim, to the concerned public health authority which is authorized to accept reports of domestic violence, neglect or abuse:

- Should the disclosure be expressly required by regulation or statute, the entity believes that disclosure is a must to avoid harm to the patient or other victims, or potential victims
- Should the individual agree to disclosure
- Should the individual be incapable of acquiescing to the disclosure, an authorized public official and law enforcement represents that protected health data isn't intended to be utilized against the patient and that immediate enforcement activity is dependent on the disclosure which would be adversely and materially affected by waiting till the patient is capable of agreeing to the disclosure

Usually, if the covered determines that the disclosure of health information regarding the victim of abuse shall be done, the covered entity should communicate to the patient of the report that was made. But, should the entity believe informing the patient would put the patient at risk or do serious harm, the entity isn't required to communicate to the individual about the disclosure.
Health Oversight Activities and Their Disclosures and Uses

Protected health data can be revealed to the health oversight agency to oversee activities of oversight authorized by law, like audits, criminal, civil or administrative investigations, licensure, inspections, or disciplinary action, and the criminal proceedings. Usually, the disclosures permitted according to the rules should be for activities that are necessary for health care system oversight, benefit programs of the government for which health data is pertinent to eligibility of beneficiary, entities which are subjected to regulatory programs by the government which require health data to determine program standards compliance, or entities which are subject to laws of civil rights which require health data for compliance determination.

Administrative and Judicial Proceedings Disclosures

Should an administrative tribunal or court order the covered entity to reveal protected health data which is conveyed in the given order or should an entity receive a discover request, subpoena, or another lawful process, it can disclose protected health data should the party requesting the information gives a written statement and also supporting documentation that:

• It has made an attempt in good faith to give written notice to the individual
• With regard to the unresolved objections against disclosure or use, none were filed inside the time frame designated
• Included in the notice, was sufficient information with regard to litigation or advancing to permit the patient to raise dissent to the administrative tribunal or court

A covered entity can also reveal protected health data in this situation should the requesting party secure an order of “qualified protective order.” The qualified protective order is of the administrative tribunal or court order that forbids the parties from disclosing or using the protected health data apart from the purpose it was requested for and requires the destruction or return of the protected health data in the proceedings end.

Law Enforcement Disclosure

The covered entity can usually disclose protected health data as needed by law which includes laws which mandates the reporting of physical injuries or specific types of wounds or other types of injuries. It can also reveal protected health data to comply with a warrant, court order, summons or subpoena, or subpoena by a grand jury. So long as a request of an administrative nature, or an alike process which is authorized by law requests data which is material and relevant to an inquiry by legitimate law enforcement, is limited and specific in scope for which the data is desired, and de-identified data could not be used for the purpose, the covered entity can disclose protected health data following such a request. As a response, a law enforcement official's request for the purpose locating or identifying a fugitive, suspect, missing person, or material witness, the covered entity can usually reveal:

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

Should an individual be considered a crime victim, the covered entity can usually reveal protected health data should the patient agree to the disclosure. Protected health information regarding such an individual can also be given to a official of law enforcement if the individual's agreement could not be obtained either due to emergency or incapacity, as long as, representations by the officer are based on:

- required information to determine if violation of law has occurred by a person apart from the victim
- it is in the individual's best interest to have the information disclosed as deemed by the covered entity's professional judgment
- activity by the law enforcement would be adversely and materially affected by waiting on the individual's agreement
- the data isn't meant to be utilized against the victim

Should an entity suspect that the death of the individual could have been as a result of criminal conduct, it can disclose protected health data to the officer of law, alerting them to the circumstances. The entity may also reveal protected health data to the officer of law if it, in good faith is of the belief that criminal conduct has occurred on the premises.

Should a covered provider of health care, responding to an emergency medical in nature, give care off the provider's premises, it can reveal protected health data to an officer of law enforcement which is necessary in alerting the officer of commission and the crime's nature, victims of a crime, the description of or, identity and the perpetrator's location.

Decedents and Their Disclosures and Uses

The covered entity can disclose the protected health data to a medical examiner or coroner to determine the cause of death, identify a deceased person, or other duties authorized by the law. It can further disclose data to directors of funerals, as permitted by law, to enable the directors to do their duty properly.

The covered entity may can reveal protected health data to an organization of organ procurement or other entities which are involved in the procurement, transplantation, or banking of organs, tissues or eyes to facilitate transplantation.

Disclosures and Uses for Purposes of Research

The covered entity can disclose or use the protected health data for research purposes, ensuring that the covered entity has a waiver of authorization approved as required according to the law. It is discoursed over a great deal within this course's final chapter.

Disclosures and Uses to Obviate a Threat of a Serious Nature to Safety or Health

Should a covered entity believe that the disclosure or use of protected health data is required to lessen or prevent an imminent and serious threat to the safety or health of the public or person the covered entity can disclose the information to the person who is reasonably capable of lessening or preventing the threat? It could also reveal protected health data should it believe the data is essential for authorities of law enforcement to apprehend or identify the individual that admitted to taking part in a crime of violence that the entity believes could have caused serious injury to the victim, or should it appear that an individual is at large from lawful custody or a correctional institution. But, if an individual is under therapy or counseling treatment by the
covered entity during which admission of the individual taking part in a crime has occurred, the covered entity does not usually reveal the data.

**Workers’ Compensation and Standard Disclosures**
The covered entity can disclose protected health data as essential to be compliant with workers’ compensation laws or similar programs.

**Disclosures and Uses of Protected Health Data Relating To Other Requirements**
The covered entity should identify the class of people or persons within its workforce that require access to health information to do their jobs. The categories or category of protected health data that requires to be accessed should be documented for every identified class or person, in addition to the conditions which are appropriate for such access. A covered entity should also make or efforts within reason to restrict the access to protected information by the class of people or persons.

For disclosures that are routinely made, the entity should implement procedures and policies to restrict the protected health data disclosed to an amount reasonably essential to achieve disclosure purposes. For other disclosures, covered entities must follow the rules that follow:

a) development criteria designed to restrict access to the protected health data to that essential to achieve the disclosure's purpose i.e. the minimum necessary standard

b) the review of each disclosure in purview of the established criteria

**Representations of the Minimum Necessary**
A covered entity, in some cases, may not be required to ascertain of its accord when a disclosure fits the standard of the “minimum necessary”. Should a disclosure be made to officials according to regulations and a public official represents within reason that the information requested is of the minimum necessary, that representation may be relied upon by the entity. Furthermore, should a covered entity receive a request for disclosure from a different covered entity, ensuring the minimum necessary standard is the requesting entity's responsibility? Additionally, should a professional workforce member of an entity or one who gives to the entity, professional services, requests protected health data and represents within reason that it fits the minimum necessary standard, the professional person's representation may be relied upon by the entity. The entity may not disclose, use or request an complete medical record, except when specifically justified as essential within reason to achieve the request purpose of disclosure or use.

**Protected Health Information-Disclosures and Uses for Marketing**
The covered entity doesn't have to possess authorization when it discloses or uses protected health data to create marketing communication in a meeting that is face-to-face, to an individual, or concerning services or products of minimal value. Authorization is not required when the covered entity markets services and products that are health-related belonging to the entity or a third party done by communication and the communication done:

- has the covered entity that making the communication identified
- prominently discloses the receipt or future receipt of remuneration by the entity, if applicable
- comprises of instructions that describe how opting out of getting future communications may be done, the exception being that the communication is the device of general communication, like a newsletter, which is distributed across a broad section of enrollees, patients or other group
The covered entity should also make reasonable efforts to ensure that the patients who opt out of are not sent any further communications.

**Marketing Targets**

Should an entity use protected health data to target individuals with regard to communication based on the patient's health condition or status, the entity should make a determination about a service or product marketing to the targeted market before communicating that the service or product may be of benefit to the patient's health in the group targeted. Targeted communication should, in addition, explain the reason for targeting the individual and the relationship possible between the service or product and the individual's health.

**Requirements for Verification**

Before disclosing any of the protected health data, the entity should affirm the person's identity, requesting the protected health information and the person's authority to access protected health data, except when the person's identity is known to the covered entity. Covered entities should also procure any representations, statements or documentation, written or oral, from the requesting party, when it is required according to the regulations.

**Privacy Practices Notice and Protected Health Information**

A patient in the group health plan maintains the right to a privacy practice notice from the covered entity which directly gives health benefits, either an issuer of health insurance, group health plan, or an HMO. Should a group health plan provide benefits via a contracted HMO or health insurer, receives or creates summary health information and protected health data or information with regards to if the individual is a participant within the group health plan, enrolled or dis-enrolled patients, should maintain a notice of the privacy plan and give it to anyone requesting information.

**Contents of Notice**

The notice of privacy should be recorded in plain language and it should include the statement below as prominently displayed as a header:

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.

Privacy notice should also contain:

- The description of types of disclosures and uses that the covered entity is allowed to give for the health care operations, treatment and payment, which includes, at the least, an example for each purpose
- Should it be applicable, a statement that contacting the individual by the entity may be done with an appointment, treatment alternatives reminders, or other related health benefits and services
- The description that disclosures and uses shall only be done with the written authorization of the individual, and that the patient can revoke the authorization
- The description of other purposes the covered entity is allowed to disclose or use without written authorization or consent of the individual
- Should it be applicable, the statement that disclosure of protected health data to the plan sponsor can be made by an insurer of health, a group health plan or even an HMO.
• Statement of the patient's right to get communications of a confidential nature at by alternate methods or another location, as authorized according to the regulations, and description in brief how this right may be exercised by the individual of the patient's right to ask for restrictions on specific disclosures and uses of the protected health information, also the entity isn't bound to acquiesce to the requested restriction, and a description in brief of how this right may be exercised by the individual
• Should it be applicable, the statement that an entity can contact the patient to fund raise for the entity
• the statement of the patient's right to copy and inspect protected health data, and a description brief of how this right may be exercised by the individual
• the statement of the patient's right to make corrections in protected health data, and a description in brief of how this right may be exercised by the individual
• the title, name or phone number of an office or person to reach with regard to the complaints
• Should it be applicable, the statement that an entity can reserve the right to modify the notice terms and to make new provisions for privacy which shall be effective for the entire protected health data the entity upkeeps, and the description of how patients shall be provided with new notice of the like
• the statement of the right of an individual to get an account of the disclosures of the protected health information, and a description in brief of how this right may be exercised by the individual
• the statement that an entity will be bound to follow the notice terms currently in effect and the statement of the right of the individual to get a paper duplicate of the notice by the covered entity upon request, and a description in brief of how this right may be exercised by the individual
• the statement that an entity is bound by law to the upkeep of the protected health information's privacy and to give notice to patients of the duties of the entity's and privacy practices according to the law with regard to protected health data
• the date of effective notice, which should not be earlier than published date
• the statement that patients may lodge a complaint with the entity and the Secretary as well, if they are of the opinion that their privacy rights are being violated or have been violated, the description of the process of filing the complaint and the statement that there shall be no retaliation against the patient for filing the complaint

Notice Provision
The Health plans should provide notice not later than the date of compliance, which is 36 months post publishing of the final rule in a Federal Register for health plans on a small scale, and 24 months post publishing for the other health plans on a larger scale, to every individual who is covered by the health plan.

Henceforth, health plans should provide at the time of enrollment, notice to the new enrollees and inside 60 days of revision to material to the individuals who are covered by the health plan. Additionally, once every 3 years at the very least, the health plan should apprise the individual who is covered by the health plan of notice availability and to obtaining the notice. The provider of covered health care which has with an individual, a direct treatment relationship should give notice not later than the first service delivery date after the date of compliance for the provider of covered health, which is 24 months post publishing of the final rule within the Federal Register. Should the provider have a location at which physical service is given, the notice should be present at the physical service location for an individual to ask to take along with them and have the notice posted in a prominent, clear place where it can be expected within reason that the individuals seeking the service shall be able to view it.

Should the covered entity maintain a web site online which gives information about its customer benefits or services, the notice should be posted on its web site and should make the notice electronically available through its website. The Notice can be given through e-mail should the individual, this manner, agree to receive
it. If the entity is cognizant of the fact that the e-mail has failed to go through, it should give a physical paper notice to patients. Should the first service for the individual be made in an electronic format, the notice should be made contemporaneously and automatically to the individual at that time. Individuals that receive electronic versions of the notices should have a right to get paper notices as well.

Revisions Notice
Should a notice be revised materially, the covered entity should promptly revise and then distribute to the individuals the notice which has been revised, to whom the covered entity should make notice.

Individuals' Right to Request Restrictions on Disclosures and Use
An individual has a right to request an entity to restrict, beyond normal practices of privacy found within the notice, the disclosures or uses of the protected health information with regard to:

- permissible disclosures to the members of the family and others to facilitate the individual’s treatment, health care, or payment operations
- carrying out of health care operations, treatment, or payment

An entity isn’t required to acquiesce to a request for restriction. Should a covered entity agree to a requested restriction, it cannot violate the restriction agreed upon while it is still in effect, apart from emergency situations? The covered entity should disclose protected health data to a health care provider in an emergency situation, the covered entity should request that the health care provider not disclose or use the protected health information further.

Restrictions that may not be applied to disclosures are:

- to the individual
- as mandated according to the law, like when investigating a complaint
- in the facility directory for legal use
- as authorized according to the regulations for activities of public health
- with regard to abuse victims, neglect victims or domestic violence victims which are authorized under regulations
- by the health oversight agency for authorized use
- for administrative and judicial proceedings for authorized use
- as authorized according to the regulations for purposes of law enforcement,
- for purposes of research, according to regulations
- to avoid serious threat to safety or health
- as defined in regulations for specialized functions of the government,
- with workers’ compensation and also similar laws for compliance

The restriction can be terminated in writing or orally by the individuals, if documentation of an oral agreement is done. The entity may also end a restriction by written communication with the individual.

Requirements for Confidential Communication
The covered provider of health care should permit patients to request for information and should be accommodating of reasonable requests by the individuals for the receipt of communications of the protected health data from the provider of health care by alternative locations or alternative means. A provider of health care may not need an individual’s explanation for the request because the condition for giving information on the basis of confidentiality. However, a health plan can require to receive communications by request by
alternative means or in an alternative location or have a statement contain that the disclosure of part or all of the information which could put the individual in danger.

**An Individual's Access to Protected Health Information**

The individual has a right to the receipt of protected health data regarding themselves, with the exception of:

- notes of psychotherapy
- information collated for use in or in anticipation of a criminal, civil or administrative proceeding or litigation
- inmates by obtaining information which would endanger the safety, health, rehabilitation or security of an individual or of the other inmates, or of an officer's safety, an employee's safety or another person in a correctional institution
- protected health data that is subject to Clinical Laboratory Improvements Amendment, access by individual is forbidden by law
- the information which is obtained within the duration of the research being done, when an individual has given consent to the participation in research which includes the treatment and had been informed that right of access shall be reinstated upon research completion
- Should the data have been obtained from a source other than the provider of health care with a confidentiality promise and the requested access would be likely to reveal within reasonable limits, the information source
- specific records controlled by agencies of the government and protected according to the Privacy Act, 5 USC §552a

Besides the circumstances here defined according to regulations as a reason for access denial, there are more circumstances in which the covered entity can deny individuals access to the protected health data. They include when the:

- licensed professional in health care that has affirmed that access requested is within reason, likely to put in danger, the physical safety or life of an individual or other person
- requesting individual is the personal representative of an individual and a licensed professional in health care affirms that access is within reason, likely to induce substantial harm with regards to the individual or the other person
- protected health data refers to the other person and the licensed healthcare professional affirms that access requested is within reason likely to induce substantial harm with regard to the person

Should the covered entity deny access for any one of the above reasons, it should permit the individual a right to review access denial. A licensed health care professional who is designated by the entity is the one who conducts the review and who didn't take part in the decision to deny.

**Access Being Provided**

Should an entity provide access to information requested, to the individual, it should give a copy, or permit an inspection, even both can be given. It should provide the data in the format or form it is requested in, should it be readily available in the requested format. Should the data not be easily produced in the requested format, the covered entity should supply the requested data in a hard copy format which is readable, or another format agreed upon by both the individual and entity?

An explanation or a summary information can be given in response to the access request, conditioned upon the individual agreeing beforehand to the explanation or summary. Should any fees be involved, the patient should
agree beforehand to the fees quoted by the entity. Covered entities should answer to an access request within 30 days of receiving the request. The entity should set up a convenient place and time for the patient to scrutinize the records, should it be applicable. A fee for access can only include the cost of:

- copying, inclusive of labor and supplies costs.
- make the other requested data accessible, should it be possible
- organizing a summary or an explanation of the protected health data, should it be applicable
- if the information mailed at the individual's request, the postage

Should a covered entity deny access to part or all of the information requested, the entity should:

- make the other requested data accessible, should it be possible
- give a denial in written in 30 days after receiving the request which includes:
  - the denial's basis
  - the description of the manner in which the individual can file a complaint with the Secretary or covered entities, and the title or name, and phone number of the person to be contacted to file a complaint with
  - should it be applicable, the statement that an individual can request a review done of the reasons for denial.

If the entity doesn't maintain the protected health data which is the topic of the patient's request, however, is cognizant of where it is kept, the entity should inform the patient of where the information can be requested. An entity should document the indicated record sets which can be accessed by individuals, and titles of the offices or persons responsible for processing and receiving access requests by individuals.

**Protected Health Information Amendment**

A person has a right to have the entity amend the record or a protected health data in an indicated record set. A covered entity should permit the individual to request an amendment. It could require that a request be written and the individual provide the justification supporting the request, ensuring that the individual was informed beforehand regarding the requirements.

Amendments requests should be acted on within 60 days after receiving the request. Should the entity accept the amendment, it should, at the very least, locate the records in a record set that has been designated as the amendment impacted record set and have them appended or give a location link of the amendments. It should also intimate the person that an amendment has been accepted and procure the person's agreement. Future disclosures should have the appended material included, or have the information summarized accurately. Should the entity deny the amendment, it should provide a written reason for denial which:

- would state that should the person not file the statement, the person could request that the entity give the person's amendment request and subsequent denial along with any disclosures made in the future, of the applicable protected health data
- gives a process description for the individual for filing a complaint with the Secretary or covered entity, and provides the title or name and phone number of the person to be contacted for complaints
- gives reasons for the denial of the amendment, the right of the individual to file a written disagreement with denial of the amendment, and the filing process of statement of disagreement.

Should the individual submit a written document of disagreement, the entity may prepare the written rebuttal for it. Should a rebuttal be prepared, it should give a duplicate to the person submitting a disagreement of statement. Whenever applicable, the entity should link the records affected with the person's amendment.
request for, denial of request, and statement of disagreement, rebuttal statement. Should an entity be notified by another entity of an amendment made to protected health data, the entity must accordingly amend its records.

**Disclosures of Protected Health Information - Their Accounting**

The individual has a right to get disclosures accounting of protected health data that is created by the entity in the 6 years before accounting date requested. An accounting can usually exclude disclosure:

- to give treatment, health care operations and payment
- to law enforcement officials or correctional institutions
- to persons, the disclosures made for intelligence purposes or national security
- for the facility directory or the person involved in individual’s care

The accounting should include, for every disclosure made:

- the disclosure date
- the entity or person's name that got protected health data and, if available, their address as well
- a description in brief of the disclosed protected health data
- a statement in brief of the disclosure’s purpose which within reason informs an individual, the basis of disclosure, or a reproduction of the written authorization by the individual, or a reproduction of the written disclosure request

Should an entity be unable to give an accounting within the required 60 days on receipt of request, the entity could extend it by 30 more days ensuring that the requesting individual has been informed or the reason for delay and date of accounting in writing.

The initial accounting that is requested within a 12 month period should not be charged. Subsequent requests by the same person within a 12 month period may be charged a cost based fee within reason. The individual should be informed of the involved fee and given a chance to modify or withdraw the request that is subject to the fees.

**Standard Training**

The covered entity should have all its workforce members trained in procedures and policies with regard to protected health data as is required for proper functioning. The training should be given before the compliance date and no later than it. New workforce members should be trained in a reasonable time period within joining and should a workforce member have a change of function affecting responsibility with regard to health information, retraining should be done as soon as possible.

**Safeguards**

An entity should have proper administrative, physical and technical safeguards protecting information privacy which should be safeguarded from unintentional or intentional disclosure or use which is in violation of implementation, standards, regulations or specifications.
Compliance

The covered entity should give individuals the process of filing complaints with an entity regarding its procedures and policies. The entity should document every complaint it receives and their dispositions if any.

Sanctions

A covered entity should apply and create sanctions against workforce members of the entity who are non-compliant with the entity's procedures and policies developed according to regulations. These sanctions should be documented when applied.

Retaliation

An entity cannot threaten, coerce, intimidate, discriminate or make any retaliatory action against individuals that exercise their rights according to regulations which include testifying, filing complaints, opposing unlawful practices according to regulations.

Changes in Privacy Practices and The Notices

Should an entity include within its practices of privacy the right to change its privacy practices, it can change its practices if the entity revises the notice and makes it available to affected individuals.

Regulation of Federal Privacy

Congress passed numerous laws which regulate privacy and this chapter deals with the various laws of the federal government that Privacy Rule interacts with dealing with an individual's privacy protection in summary.

The Privacy Act

The Privacy Act of 1974, seen in 5 U.S.C. 552a, regulates the records disclosure maintained within a record system which is maintained an agency of the federal government. This Act usually forbids disclosure of records without the request or consent in writing by the individual, except when the request or consent requirement includes allowing agencies to disclose data should the disclosure qualify as 'routine use' in the Act and the Federal Register publishes the utilized information. The Act is applicable to every federal agency and specific contractors that operate record systems which are subject to Privacy Act on the behalf of agencies of the federal government. Some contractors and agencies subject to Privacy Act are covered by Privacy Rule as well and these contractors or agencies must be compliant with all federal statutes applicable as well as legislation, whether it is in Privacy Act or Privacy Rule.

The Freedom of Information Act

The Freedom of Information Act, found in 5 U.S.C. 552, and regulates public disclosure of numerous types of information within the federal government's possession. It permits public disclosure of the data, upon any
person's request which is subject to 3 exclusions and 9 exemptions. Medical, personnel and like files can be withheld. As an example, should the disclosure constitute a clear unwarranted personal privacy invasion? Disclosures permitted according to the Freedom of Information Act are seen in §164.512(a) of Privacy Rule which allows disclosures or uses necessitated by law should the disclosures fulfill the law and its relevant requirements. But, federal agencies should usually utilize the medical, personnel and similar files exemption to forbid disclosure should it violate Privacy Rule. Federal agencies should evaluate disclosure on by-case basis to confirm if a disclosure would be violating Privacy Rule.

Confidentiality Requirements of Federal Substance Abuse

The Federal Confidentiality of Substance Abuse Patient Records Statute, Section 543 of The Public Health Service Act, 42 U.S.C. 290dd-2, and the statute's implementing regulation, 42 CFR Part 2, help regulate the requirements for confidentiality of patient records which are maintained and connected to any program's performance that is federally assisted with regard to specialized drug abuse or alcohol abuse. The providers of health care could be subject to this Statute and Privacy Rule. Health care providers must not find conflict within these two law sets but comply with both. The Statute and its related laws do not permit disclosure without authorization of the patient, law enforcement disclosures, administrative and judicial proceedings, health oversight, public health, assistance with directories and other purposes permitted according to Privacy Rule. But, since Privacy Rule doesn't require disclosures to be done for these purposes, the provider of health care can deny the disclosures for which it would violate the Substance Abuse Statutes. Privacy Rule requires individuals to be provided access to their health data, which is permitted disclosure according to the Substance Abuse Statute, allowing an entity that is covered by both categories of rules to disclose information and still be compliant with both sets of laws. The Statute also permits disclosures in the case of emergencies of a medical nature, for research, to the FDA, for audit and activities involving evaluation, in response to specific court orders. According to Privacy Rule, these disclosures are necessary and the entities that are subject to both law sets and that should permit disclosures according to Privacy Rule remain compliant with the Statute. Substance Abuse regulations need the giving of notice for confidentiality requirements of patients under substance abuse and allows for disclosure's written consent. Privacy Rule also necessitates notice and, usually, consent as well. An entity which is subject to both laws may make notices and the consent forms meeting both their provisions.

Family Educational Rights and Privacy Act

Family Educational Rights and Privacy Act, or FERPA, found in 20 U.S.C. 1232g. FERPA gives the students that are 18 or over (eligible students) and the student's parents protection of privacy for student records maintained by federal educational agencies or their representatives. Education records applicable under FERPA are exempt from the definition 'protected health information'. As an example, an individual student's health information (under 18 years of age) formulated by a public school's nurse and subject to FERPA is considered an 'educational record'. FERPA deals with the manner of protection regarding education records, including an exclusion under 'protected health information' definition within FERPA rules are the records (a) maintained by the psychologists, psychiatrists, physicians, other professional or paraprofessional assisting, (b) of students 18 years or over attending educational institutions that are post-secondary, (c) that are only maintained, made or utilized in meting treatment to a student and (d) aren't available to any person with the exception of an appropriate professional like a physician reviewing the student designated record. Any utilization of these records according FERPA apart from persons that provide treatment to students converts them into 'education records' and these records are subject to FERPA protection. But, should a school not be federally funded, it isn't regulated by FERPA and its records could be considered 'protected health information.'
Employee Retirement Income Security Act of 1974

Also called ERISA, it regulates welfare employee benefit plans and pensions that are laid down by unions, private employers or both in order to give benefits to their workers and dependents. ERISA defines "employee welfare benefit plans" as plans that give “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.” HIPAA in 1996 amended ERISA to acquire nondiscrimination, renewability and portability of the benefits of health care given by the group health insurers and group health plans. ERISA plans are usually covered by HIPAA regulations regarding "health plans." In ERISA, §514(a), found in 29 U.S.C. 114(a), the laws of the state that relate to the employee benefits plans have been preempted by ERISA except when state laws are more restrictive that ERISA apart from insurance regulated by state laws. Additionally ERISA plans aren't deemed an insurer for regulation of these plans according to state insurance laws.

Federally Funded Health Programs

Health programs which are aided by federal funds including veterans and military personnel, Medicaid and Medicare. According to HIPAA "health plans" are inclusive of the below programs :

- Medicaid;
- Medicare;
- Group plans according to ERISA that either are handled by an entity apart from the employer that maintains and established the plan or have fifty or greater participants
- organizations which are health maintenance programs and federally qualified;
- active military personnel health care program;
- CHAMPUS - Civilian Health and Medical Program of the Uniformed Services;
- supplemental policies of Medicare;
- veterans’ health care program;
- Health Benefits Program for Federal Employees.
- Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.- the Indian health service program ;

Apart from the listed programs in HIPAA, other federally regulated, conducted or funded programs which don't fall under statutory definition of the "health plan," however the statute could apply when a federally regulated, federally funded or a federal entity gives health services. Circumstances such as these qualify the entity as a provider of health care and thus subject to Privacy Rule.

FDA - Food, Drug, and Cosmetic Act

The Food, Drug, and Cosmetic Act, found in 21 U.S.C. 301, et seq., gives the responsibilities of Food and Drug Administration regarding monitoring the effectiveness and safety of devices and drugs. Responsibilities of the agency include procuring reports regarding tracking medical devices, adverse events, and engagement in post marketing surveillance of others. Reports like these often comprise of protected health data and the health information could be regulated by Privacy Rule.

The Privacy Rule, in distinction from others permits the disclosure of protected health information by covered entities to the person that is subject to the Food and Drug Administration's jurisdiction for the purposes held in distinction from others. The specified purposes could include tracking medical devices, reporting of adverse
events, or engagement in post marketing surveillance of other kinds.

**Amendments in Clinical Laboratory Improvement**

Clinical Laboratory Improvement Amendments, or CLIA, found in 42 U.S.C. 263a, with its accompanying regulations, seen in 42 CFR part 493, regulates the clinical laboratories and their standards with regard to human specimen testing. According to this law, the clinical laboratories are necessitated to disclose results of the reports or test to only persons who have been authorized, defined by the state law.

The authorized person according to federal law has been defined as the individual who arranges the test.

Different states could have different definitions regarding what qualifies as an “authorized person.” A person arranging for the test can be the health care provider, instead of the person who is the topic of protected health data. It means that a law could forbid the clinical laboratory from giving the individual subject to the report or test with protected health information access available to them. Privacy Rule, thus, doesn’t require the covered entities keeping the protected health data subject to the CLIA to give individuals that have the right to inspect or the right to access and procure a reproduction of this data if this right is forbidden by CLIA. But, should the state authorized to oversee the covered entity utilizes another definition of an “authorized person” as applicable to CLIA, and also includes the patient in this definition,

Privacy Rule doesn’t exempt this covered entity from a necessity to give individuals with access rights or inspection rights to obtain a reproduction of this data.

**Other Mandatory State or Federal Laws**

Privacy Rule excepts specific types of disclosures, uses from the usual authorization requirements. Privacy Rule allows covered entities to give disclosures mandated by law, and numerous federal laws necessitate covered entities to give certain information to certain entities in certain circumstances. SSA, including Medicaid and Medicare provisions, Public Health Service Act, the Family and Medical Leave Act, regulations of Department of Transportation, the National Labor Relations Act, Environmental Protection Act with its accompanied regulations, Federal Aviation Administration, rules of Federal Highway Administration, could contain provisions that need entities and other agencies to disclose or use the protected health information for certain purposes.

The covered entity should determine if the disclosure is necessary according to a federal law which applies to a disclosure if a disclosure is usually forbidden according to Privacy Rule. Should disclosure be mandated, the covered entity can disclose the data according to Privacy Rule, §164.512(a). Should the disclosure be allowed by the federal laws applicable, but not compulsory, then the entity should determine if the disclosed information falls in one of the allowed disclosures according to Privacy Rule. If the disclosure requires an authorization, the entity should obtain authorization from the concerned individual, or should de-identify the data prior to disclosure. Should a federal law apart from Privacy Rule forbid the covered entity from disclosing or using information, but Privacy Rule permits the disclosure or use of the information, the federal law takes precedence and the entity should not use or disclose the data.

**Federal Disability Nondiscrimination Laws**

Two primary federal disability nondiscrimination laws are the Rehabilitation Act of 1973, 29 U.S.C. 701 et seq. and Americans with Disabilities Act, or ADA, 42 U.S.C. 12101 et seq. There are different federal laws that forbid discrimination based on disability as well, and these include
provisions of privacy protection.

Section 2 of ADA explains the reasoning of the 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 non productivity.
(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.

Americans With Disabilities Act Section 501 deals with disability and insurance:
(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.

Nondiscrimination laws of federal disability like the ADA cover 2 types of entities that may be affected by
Privacy Rule: entities and employers receiving financial assistance from the federal government. Employers
aren’t considered covered entities according to Privacy Rule. However employers are subject to the laws
of federal disability nondiscrimination and are expected to safeguard medical information confidentiality of all
their employees and applicants. ADA covers with specific intention, the employment agencies, the labor
organizations, labor management joint committees, employers employing 15 or more employees, in its
provisions for employment. The obligations of confidentiality for these employers include handling employee
and applicant medical information confidentially. Communication of health data to an entity by the employer,
like the group health plans, are dependent on confidentiality restrictions by the ADA. ADA can be interpreted
to allow the employer to use health information for purposes of insurance 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]. Communication of medical
information to the entity by the employer falls under “use of medical information for insurance purposes.”
Medical information disclosure by the group health plan too can be considered utilization of information for
purposes of insurance.

The entities that get financial assistance from federal agencies and can be covered entities as well according to
the Privacy Rule are regulated by §504 of the Rehabilitation Act (29 U.S.C. 794). Every federal agency proclaims
regulations which are applicable to the entities that get financial aid from the agency.

The above regulations can include provisions of privacy protection which limit medical information disclosure of
persons who participate in or apply to a financially assisted program by the federal government. As an example,
Section 504 regulation of Department of Labor mandates that the entities which get funds which conduct
programs related to employment, to maintain confidentiality with regard to any information pertaining to
to history of applicants or medical condition or the participants in the activity or program. The data needs to be
separated from other information regarding the participant or applicant and may be provided only to specified
individuals under specific limited circumstances.

The recipients of monetary assistance from the HHS, like hospitals, too also regulated by the ADA’s
nondiscrimination standards in employment. Thus, they should maintain confidentiality of both the medical
condition and history regarding both employees and applicants.
Final Regulation Guidelines

Individually Identifiable Health Information Privacy and Standards

A Guidance was published on the 6th of July, 2001, proclaimed by the HHS, to give direction for implementing the “Standards for Privacy of Individually Identifiable Health Information,” usually known as “Privacy Rule.” Responding to the question “What does this regulation do?” Guidance states that Privacy Rule was effective on the 4th of April, 2001 and that Privacy Rule for the very first time creates national standards to safeguard medical records of the individuals and other personal medical information. Guidance sums up Privacy Rule as below:

- 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.

Guidance includes summing up of how patients are affected by the rule as well. It expresses that the rule allows patients to ascertain their personal health information and what information of theirs has been disclosed and how it may be utilized, that the rule limits the release of data regarding the patient to a minimum reasonably required for the disclosure's purpose, and gives patients a right to obtain and examine a copy of the medical records in addition to requesting corrections. Within Guidance, the need for regulations is justified. Guidance indicates that the Congress mandated the formation of standards for individually identifiable information privacy when Congress brought in the Health Insurance Portability, Accountability Act in 1996.

Regulation of personal information regarding health was by a variety of state and federal laws before HIPAA enactment by Congress. It was according to these laws potentially possible for information about a person's personal health to be shared for reasons other than a patient’s health care reimbursement or medical treatment. As an example, Guidance mentions that before the Rule's enactment, patient data controlled by the health plan could be shared with a lender who could then deny the individual's application regarding a credit card, even a home mortgage, could also be shared with the employer who could use it in personnel decision making.

The next question dealt with in Guidance is, “What does this regulation require a run of the mill health plan or provider to do?”. Guidance names 5 activities which are required according to the rule that are:

- Giving information to patients regarding their privacy rights including the ways that their information could be utilized.
- Providing employees with training so they comprehend the procedures of privacy
- Adoption of clear procedures of privacy for its hospital, plan, or practice
- Patient records which contain individually identifiable health information should be secured to ensure that the records aren’t easily accessible to people that do not need the records.
- Appointing an individual that is to be held responsible for ensuring that the procedures of privacy are followed and adopted

Guidance highlights that plans and providers vary in need and size and thus Privacy Rule provides flexibility to plans and providers to formulate their own procedures for privacy. The question that is answered “Who must comply with these new privacy standards?”
Guidance states that Privacy Rule encompasses health care clearinghouses, health plans and the providers of health care that conduct specific administrative and financial transactions in an electronic form. These entities are referred to as “covered entities” in Guidance, as well as in Privacy Rule. The question answered next in Guidance is “When will covered entities have to meet these standards?” Guidance puts forward that most entities will have 2 complete years from the effective regulation date to become compliant and health plans which are smaller have 3 complete years to become compliant. Guidance then deals with the question “Do you expect to make any changes to this rule before the compliance date?” which in response, suggests that it shall issue the proposed modifications to rectify any unintended negatives upon the facts of Privacy Rules on quality of health care or on access to quality care. Guidance asks next “What changes might you be making in the final rule?” to which it lists 4 examples of standards up for proposed changes which 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.

Guidance also says that HHS may reevaluate Privacy Rule to ensure appropriate access to data about the well being and health of their children is provided to parents.

Finally, the question in the section introducing the Guidance asked “How will you make any changes?” Guidance states that changes of any sort should be made according to Administrative Procedures Act which will be published by HHS on rules changed within the Federal Register, a proposed rulemaking notice and shall invite public comment and after reviewing and addressing these comments HHS shall put forth a final rule which will implement appropriate modifications made. Guidance also highlights that Congress had specifically authorized HHS as modifier of the rules as considered appropriate in the 1st year after the impact of final rule is known to ensure Privacy Rule be implemented properly.

**Consent of the Patient**

45 CFR § 164.506

**Background**

Under Guidance, the grounds for Consent rules is that providers of health care obtain the patient’s consent routinely for information disclosure to insurance companies or other purposes. Privacy Rule lays down a uniform standard with regard to procuring consent for disclosure and use of health information of a patient to meet health operations, payment or treatment.

As observed in Guidance, provisions of rules regarding Consent generally include:

- Patient consent requirement prior to a provider of covered health, who has, with the patients, a direct treatment relationship disclosing or using protected health information for health care operations, payment or treatment purposes.
• Allowing certain disclosures and uses for health care operations, payment or treatment like in an emergency, whenever a provider is mandated by law to give treatment to the individual, or whenever there are substantial barriers to communication.

• Allowing the disclosure and use of the protected health information for health care operations, payment, or treatment by providers of health plans, health care, and health care clearinghouses holding indirect treatment relationship not needing to obtain a patient’s consent.

• Permitting the provider of health care to refuse treatment to the patient should the patient refuse to consent to disclosure or use of their protected health data to give health care operations, payment or treatment.

• Necessitating written consent needs to be obtained once by the provider.

• Utilizing a consent document which is written down in general terms and brief. The consent document should be written down in plain language, informing the individual that data may be disclosed and used to treat, pay, or give health care operations, and should state the rights of the patient to review the health care provider’s notice of privacy, to be able to request restrictions, be able to revoke consent, and should be signed and dated by the patient or her or his representative.

Consent rules include individual rights below:

• An individual should be given notice regarding the privacy practices of the covered entity and prior to signing consent may have the notice reviewed.

• An individual upon disclosures and uses, may request the restrictions of their health information utilized in health care operations treatment, or payment. The entity doesn't have to acquiesce to the restriction asked for. An individual, given in writing, may revoke consent.

Administrative issues observed in Consent Rules include:

• consents that are signed should be kept from when it was in effect last, for 6 years.
• a single joint consent can be procured by specific covered entities which are integrated for multiple entity use.
• Should a covered entity have procured consents and also gets authorization, the entity should disclose data compliant to the document with greater restrictions, except when the conflict is resolved between the individual and covered entity.

Frequently Asked Questions

Every one of the Rules discoursed over in Guidance, the Guidance contains responses to questions frequently asked with regard to the Rules. Answers provide to the covered entities, guidance and the public with regard to the manner of application of the rules. Summarized below are a few responses.

Are clearinghouses or health plans expected to procure a patient’s consent to disclose or use the protected health data to give health care operations, treatment, or payment?

They are not. The health plans and health care clearinghouses can disclose and use the protected health data without procuring consent for health care operations treatment, or payment. They can, however, procure consent should they choose to, if so, should procure consent according to Consent Rules.

May a pharmacist utilize the protected health data to have a prescription filled which is called in by the physician of the patient should the patient be new and has not yet given the pharmacy written consent?

Presently, this activity isn't allowed according to Privacy Rule. The HHS department's Secretary is cognizant that this could impair the normal activities of the pharmacist’s, and shall propose modifications to attend to this problem.
Will the requirement of consent restrict the providers' ability to communicate with other providers regarding a patient's condition?
It does not. The provider-patient direct treatment relationship should have consent to give treatment to patient. Consultation with different providers regarding a patient’s condition comes under the treatment definition. So long as the entity being consulted has no direct treatment relationship, it has no need to procure patient consent.

Can direct treatment providers, such as hospitals or specialists, the patient is referred to initially, use the protected health data to schedule surgery or set appointments or procedures prior to obtaining the written consent of the patient?
As written, Privacy Rule, requires prior consent to any routine activities occurring. This proves a problem should first contact with the provider not be in person. The HHS Secretary is cognizant of this issue, and proposes modifications to deal with it.

Is a pharmacist required to procure a consent according to Privacy Rule to give advice regarding over-the-counter medicines?
So long as he does not maintain records of the protected health data for this type of situation, a pharmacist need not have a customer’s consent to give this kind of advice. The pharmacist can not disclose or use the protected health data otherwise.

The rule gives an exception to requirement of prior consent in “emergency treatment situations.” How does an entity identify when a situation warrants the “emergency treatment situation” label and, thus, is exempted from Privacy Rules requirement of prior consent?
The entity should confirm if getting a consent would affect with delivery of required health care in time, using their professional judgment. Should it be so, the entity can use protected health information to give the treatment, the payment or the health care operations.

The provider should also attempt to get consent within reasonable time after providing care.
May a patient have her prescription for her picked up by friends or family members?
She may. The pharmacist can use his or her professional judgment along with experience to decide that the patient’s best interest is to permit someone apart from the patient, to get their prescription. It isn't necessary for the patient to give the names of such people in advance. Guidance gives the example that friends or relatives picking up a certain prescriptions is proof enough that the individual is concerned in the care of the patient.

The difference between “authorization” and “consent” according to Privacy Rule is?
The authorization is a further customized document providing the covered entities the permission needed to disclose or use the protected health data for certain purposes, usually apart from treatment, health care operations or payment. Treatment can't be conditioned upon the authorization obtained from the patient. An expiration date is set upon authorizations.
Examples given in Guidance of the instances where authorizations are required include selling a mailing list of patients, disclosing data for life insurance eligibility, and data disclosure for employment decisions by the employer.
A consent is a document which gives providers of health care that have a direct treatment relationship associated with patients, permission to utilize and disclose whole protected health records for the treatment, the payment and the health care operations. Permission to a provider, and none other. Consents do not require to delineate the specific utilization or disclosure of records, and can be utilized by the entity to cover any utilization and disclosure of information for the treatment, the payment and the health care operations. A provider may take consents as the condition of treatment.

Does the requirement of exception to consent with regard to substantial communication barriers with the individual change requirements according to the Americans with Disabilities Act or Title VI of the Civil Rights
**Act of 1964?**

It does not. Just because Privacy Rule makes an exception to consent because of substantial communication barriers does not change the obligations of covered entities according to these laws.

**Will providers of health care be expected to determine if another entity has a consent form with greater restrictions, prior to information disclosure to that entity to treat, pay, or carry out health care operations?**

They are not. The consent permits the covered entity only that which obtains the consent for disclosure or use of the protected health data for their own treatment, health care operations or payment. One covered entity isn't bound by terms of consents given to another entity, with the exception of the use of a joint consent, or the entities that are affiliated entities are using the same documents of consent.

**Can consent for the disclosure or use of the protected health data be given in an electronic format?**

Yes, ensuring that the consent conforms to all the requirements according to Privacy Rule, and has been signed by the individual.

**What is the connection between “notice” and “consent”?**

Consent refers to notice, and communicates to an individual he or she has a right, prior to signing the consent, to review the concerned notice.

**Would an entity ever require an authorization instead of a consent for or disclosures uses of the protected health data for treatment, health care operations, or payment?**

Yes it does, in circumstances when authorization is needed for treatment, health care operations or payment. Authorization is required for the disclosure of the protected health data in psychotherapy for treatment by health personnel apart from the notes originator, for purposes of health care operations or payment, apart from certain disclosures and uses exempted in Privacy Rules. A different type of circumstance is when the health plan seeks, for a specific service, payment from a secondary health plan, like in benefits coordination or a secondary payer circumstance, and requires protected health data from the physician who gave health care service to the individual. The provider of health care, who obtained consent, generally already has been paid in this type of circumstance, and transactions done are between the two health plans. An authorization should be used to request disclosure from a physician, instead of a consent.

**Should a covered entity affirm the signature on the consent form even if an individual is absent when it is signed?**

The covered entity does not have to.

**Can consent be gotten by a provider of health care only once if a single connected treatment course involving multiple visits is given?**

Yes it can. Should the course of the treatment not be a single connected treatment course, the health care provider is expected to get consent only once. A new consent will be required if the individual has revoked consents in between treatments.

**Should the individual consent to the disclosure or use of the protected health data for treatment, health care operations, or payment purposes, or gets health care service, revoking afterward the consent prior to the provider billing for the concerned service, is billing for the service by the provider precluded?**

It is not. Should the service be given after getting consent, the health care provider can bill for the provided service even if the consent is revoked right after the service is given. The revocation isn't effective to the magnitude that the provider of health care has acted dependent on the consent.

**Should a consent revocation be in writing?**

It should be in writing.

**If covered entities that are part of a health care arrangement that has been organized or affiliated are in different states along with differing laws with regard to disclosures and uses of health data like a pharmacy chain, should they obtain a consent within each state a patient gets treatment?**

No, they do not have to. Consent requires only to be gotten by the entity, or by the affiliated entities, once. The laws of the State can impose requirements additionally for the consent forms.
The Minimum Necessary
45 CFR §§ 154.502(b), 164.514(d)

A General Requirement
Privacy Rule requires covered entities to limit the disclosure, use and a request for protected health data to the standard minimum necessary to achieve the purpose intended for.
The requirement of the minimum necessary standard doesn't apply to:

- 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.

An entity is to formulate and implement the procedures and policies regarding the standard of minimum necessary which are appropriate for the organization of the entity, and that reverberates with the entity’s business practice and workforce.

Personal Health Information, Their Disclosures and Uses, Requests for It
Policies and procedures in the use of protected health data should identify the classes of persons or the persons in the covered entity who require access to the data to do the duties required. They should also identify types or categories of the protected health data required, and the conditions according to which access is proper. Guidance provides an example in which hospitals may implement protocols that permit nurses, doctors, or other personnel who are involved in the treatment to be able to access the complete medical record, as required. The policies and procedures should state when a complete medical record is required, including the justifications. Recurring or routine requests and disclosures can have standard protocol, policies and procedures and should limit protected health data to the minimum necessary disclosure.
Where disclosures of a nature that are not routine are involved, the procedures and policies should include reasonable criteria to limiting, and determining the disclosures to, only the least required protected health data required to achieve the purpose of disclosure of the information. Non-routine disclosures of information must be reviewed individually.

Disclosure and Use of Information and Reasonable Reliance
Privacy Rule permits the covered entity to depend on the judgment of the requesting party, in certain specific, regarding the least amount of information which is needed. These kinds of circumstances include when a requester is:

- The agency or public official for disclosure which relates to a compliance review or a complaint, as permitted for in Privacy Rules
- The researcher accompanied by appropriate documentation which is from a Privacy Board or IRB.
- Another covered entity
- The professional who’s a member of the workforce or a business associate of the entity which holds the data

A covered entity always keeps the discretion to arrive at its own disclosure of minimum necessary
determination, irrespective of the requesting party.

**Frequently Asked Questions**

Summarized questions and answers dealt within the Guidance with regard to the standards of the minimum necessary.

*How are the covered entities required to decide what the least necessary information is, which can be requested, disclosed, or used for a certain purpose?*

The covered entities are permitted under Privacy Rules to arrive at their assessment of what kind of protected health data is necessary within reason for a specific purpose, given the features of an entity’s workforce and business. The minimum necessary standard has flexibility, not a strictly rigid standard.

*Will the minimum necessary limitations impede quality health care delivery by hindering or preventing the required exchanges of the patient's medical record amongst health-care providers included in the treatment?*

It would not. Information disclosure between the providers of health care for the purposes of treatment is specifically exempt from minimum necessary rules.

*Does the minimum necessary rule prohibit medical residents, nursing stations, medical students, & other medical personnel from gaining access to the patients’ medical records during their training?*

It does not. “Health care operations” also includes in its definition, “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.” The access to medical information in training purposes, including accessibility to whole medical records, must be included within the procedures and policies for the minimum necessary disclosures & uses.

*Should the minimum necessary apply to the disclosures to the third parties which are authorized by the individual?*

It does not. Most disclosures or uses which are authorized by the individual are exempted from minimum necessary requirements, which includes, as the Guidance states, the authorizations covered entities can receive from third parties directly, like life, casualty or disability insurers only after the patient’s claim under or application for the insurance policy. Guidance gives an example; an individual’s authorization that is being received by the health care provider to disclose medical data for underwriting purposes to an insurer. The health care provider is allowed to reveal the data requested without the minimum necessary determination, only when the authorization fulfills the Privacy Rule requirements within.

*Are providers expected to make the minimum necessary determination for disclosure to state or federal agencies, like the SSA or other affiliates, for applications of individuals for state or federal benefits?*

They are not. Since the disclosures are given the individual's authorized, they have been exempted from minimum necessary standard.

*Does the rule stop the disclosure, use, or requests of whole medical records without a justification done case-by-case?*

It does not. A covered entity can disclose, use, or even ask for the entire medical information if the entity documented its procedures & policies & it indicates that the medical record in its entirety is considered reasonably necessary for the concerned purpose. The justification doesn't have to be given with every distinct health record. No justification is required where minimum standard is inapplicable.

*Are covered entities, in limiting access, required to restructure the existing work flow systems which include the redesign of office space & upgradation of computer systems, to comply with minimum necessary*
requirements?

No. Covered entities should make reasonable efforts at limiting access to the protected health information only to those who require access which is based on the roles of those within the entity. Even though facility redesigns aren't generally necessary, the covered entity might need to bring in adjustments to the facilities, like isolating and locking record rooms or file cabinets, providing for additional security like passwords on computers that hold personal information.

What happens when an entity believes a certain request made is asking for information considered over the minimum required protected health information?

Covered entities should limit disclosure to the necessary minimum on its side, the disclosure which is determined by the entity. In case the circumstance falls under any of the circumstances in which the entity is allowed to rely upon a requesting entity to confirm what the least necessary is, the entity is entitled to do so.

Are physicians’ and doctors’ offices allowed to keep on using sign-in forms in waiting rooms?

The intention of the HHS was not to prohibit sign-in forms usage.

In minimum necessary requirements, are covered entities prohibited from maintaining bedside patient medical charts, requiring that empty prescription vials be shred, or require isolation of X-ray light boards?

No. The covered entities should take reasonable safeguards to prevent unnecessary or inadvertent disclosures. As an example, the Guidelines say that the rule doesn't require X-ray boards to be completely isolated from every other functions, but, it requires covered entities to take reasonable measures for the protection of X-ray boards from being publicly accessible.

Oral Communications

45 CFR §§160.103, 164.501

The Background

Privacy Rule is applicable to all oral communications, in addition to electronic, written or any other, regarding protected health information. Had Privacy Rule not been applicable to all oral communication, then health information of any kind could be disclosed, just as long as all disclosures were spoken.

The General requirements

General requirements regarding the oral communications as those stated within the Guidance are below:

- 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
Given is the summary of frequently asked queries with regard to orally communicated information found within the provisions of Guidance:

**Does the rule require the hospitals and the physicians’ offices to be provided for private rooms, soundproofing of walls to avoid possibilities of a conversation being overheard?**
No. Privacy Rule doesn’t require an entity to require access to private rooms, the encryption of wireless, soundproofing of rooms or any other emergency medical communications by radio which may be tapped by scanners, by telephone systems encryption. The covered entities should take fairly reasonable steps to safeguard a patient's information. Under the Guidance, reasonable safeguards also include:

- 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.

**Should the providers of health care employ confidential conversations along with other patients or providers, has violation of the rule taken place if the possibility exists that they may have been overheard?**
Privacy Rule isn't intended to forbid providers from talking between one another or their patients, and isn't intended to forbid providers to speak aloud to one another within a busy emergency department in order to make sure that appropriate treatment is meted out.
The Guidance expresses that the practices given below are permissible according to the Rule, as far as reasonable precautions have been taken to minimize chances of inadvertent disclosure to others nearby:

- 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.

**Are the covered entities required to give oral information access to patients?**
No. According to Privacy Rule, the covered entities are required to give individuals access only to protected health information contained in their own “designated record sets.” The oral information isn’t considered as part of designated record sets defined by the Rule.

**Did the HHS change its position, by covering all the oral communications within Privacy Rule, from proposed rule?**
No. The rule proposed would have encompassed information in any medium or form, provided it had been, at some point, transmitted or maintained electronically. If the information had been in electronic form, it would be covered, no matter which form it was being held by the entity. As an example, if one patient had a single bit of health information emailed to the clinic, which would have placed information in the patient’s health record, that portion of data would be under the jurisdiction of Administrative Simplification law, however, other records held in the clinic wouldn’t be within the same jurisdiction, possibly even the same patient’s records. It is extremely chaotic for a provider or clinic to confirm which records are under jurisdiction of Administrative Simplification law, the accompanying regulations and those which were not. Privacy Rule had the nexus of oral information to the electronic information removed, and also covers all the individually identifiable health information of covered entities.

**Are covered entities expected to document all the oral communication done?**

No. The rule doesn’t include the requirement of covered entities to document any information disclosed or used for payment, treatment or the health care operations, inclusive of all oral communication. That being said, certain oral communications must be documented according to the Rule, as an example, to meet the standards for providing disclosure history to the individual upon request of the same. When Privacy Rule has a requirement for documentation, it requires documentation for all the relevant communications, inclusive of oral communication.

The Guidance gives the example in a case where a physician discloses knowledge of an instance of tuberculosis to the concerned public health authorities. This disclosure should be recorded by the physician, regardless of whether the information was documented in writing or orally.

### The Business Associate

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

### The Background

These days, providers of most health care and health plans don’t carry out the entire gamut of health care activities they are involved in and functions by themselves. Instead they use a variety of business associates to implement specific tasks. According to Privacy Rule, plans and providers are allowed to provide the business associates protected information upon the receipt of acceptable levels of assurance that the contractor/business associate uses the data only for purposes for which the business associates were engaged for by the entity, and will protect the information from being misused, and shall assist the covered entity by complying with the entity’s duty to provide access to health data and history of specific disclosures to individuals. Protected health information disclosure may only be to a business associate who will help the plans and providers carry out functions of health care The business associate for independent use, may not.

### A Business Associate-What Is It?

Guidance provides the information below about what defines business associate:

- 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.

FAQs

Has the HIPAA authority been overstepped by the Secretary by the requirement that “business associates” must be in compliance with the Privacy Rule, although that requirement is via contract?
Business associates aren't subject to all of the provisions in Privacy Rule, only a small set of the provisions through contractual requirement. The Guidance highlights that, as an example, covered entities aren't required to have business associates consent to develop policies or to an appointed privacy office and procedures for disclosure and use of protected health information.

Has the Secretary overstepped statutory authority by the requirement of “satisfactory assurances” regarding disclosures to contractors/business associates?
The Secretary has not. HIPAA has given authorization to directly regulate the health plans, the health care providers, and clearinghouses. HHS has explicit authority in regulating the disclosures and uses of protected health information kept and transmitted by the covered entities. Thus, the Department holds the authority to mandate that a contractor or business associate must have a contractual relationship with a covered entity to have protected health information given to the concerned business associate.

Will it be reasonable that covered entities be liable for the violations of privacy of the contractors/business associates?
The Covered entities aren't held liable when violations of privacy of their business associates occurs. The covered entities aren't required to monitor or oversee in an active manner the methods used by the business associate/contractor carries out safeguards and aren't expected to oversee the extent the business associates/contractors abides by the of the contract requirements. If the entity gains awareness of a practice or pattern of the involved business associate that is a material violation or breach of the associate’s contractual obligations, it must institute “reasonable steps” to fix the breach or end the violation. Should such steps not be successful, the entity should terminate the contractual agreement, if feasible. If it is not feasible, the entity should report the issue to the HHS.

The Parent and the Minors
45 CFR §164.502(g)

The General Requirements in Parent and Minors involved

The parent usually has the authority with regard to making health care choices of a child who is a minor and is usually considered the “personal representative” according to Privacy Rule, and so can access health information regarding the child. This provision is also applicable to an individual acting as in loco parentis or other guardian of a child.
In certain circumstances, the parent is not considered a “personal representative” according to Privacy Rule, and thus would not exercise control over the child's protected health information concerned.

Guidance provides the following examples these types of situations:
- 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.

Guidance further provides circumstances in which Privacy Rule indicates the current kind of professional practice in confirming that the parent isn’t the child's personal representative and therefore would no longer have accessibility to health information of the minor’s. One situation is when a parent consents to a relationship of a confidential nature between the minor and the physician, an example would be when the physician asks the parent of a sixteen-year old if he or she can talk to the child confidentially regarding medical conditions and if the parent agrees, they would no longer control protected health information discussed in the confidential conference between minor and physician. A different circumstance would be if a physician has reasonable belief in her or his professional judgment that a minor may be or has been subjected to neglect or, abuse or in addressing parents as the minor's personal representative would endanger the minor. In some conditions, the physician may decide not to address the parents as personal representatives of the concerned child.

In Relation To the State Law

Privacy Rule doesn’t preempt state laws which specifically address health information disclosure of a child to the parents, whether the law prohibits or authorizes such disclosures.

Frequently Asked Questions

Guidance deals with the questions below regarding the regulations surrounding minors and parents:

If a child gets emergency medical care with no parental consent, may a parent get the entire information about the minor’s treatment and condition?

Usually, yes. According to Privacy Rule, parents are still the minor’s personal representatives, unless conditions meet one of two exceptions.

Will the Privacy Rule give rights for children treated without consent of the parents?

No. The Rule does not deal with consent to treatment, just the access to protected health information. Privacy Rule doesn’t preempt or change the state laws or others that deal with consent to the treatment.

Does Privacy Rule allow for parents rights to view their children’s health information?

Usually, yes. There are 2 exceptions which are

(1), when the parent has agreed, with the provider, to a relationship that is confidential, and (2) when the provider reasonably believes that her or his professional opinion with regard to the minor has been or can be subjected to neglect or abuse, and in addressing the parent as representatives of the child's would endanger the minor.
Marketing and Health-Related Communications
45 CFR §§ 164.501, 164.514(e)

Marketing-What is it?

Under 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.”

Communications Not Considered Marketing

The Guidance describes the activities not considered marketing according to Privacy Rule. Covered entities do not “market” when the entity:

- 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’s not considered “marketing” when covered entities use a patient’s protected health information to tailor health-associated communication to the concerned individual, provided the communication given is as:

- 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.

Marketing Communications and the Limitations on Them

A covered entity can disclose or use protected health information within creating or making marketing communications, after obtaining the applicable consent, so long as the marketing done:

- Involves the services or products of minimal value, like, key chains toothbrushes or pens with the entity name or the manufacturer of health care product on it;
- Is face-to-face, like the patient being provided samples during a visit in office;
- Regards the products that are services of an entity and health-related or third party, and (1) identifies covered entities communicating so that consumers know the origin of materials or marketing calls (2) states that covered entities is compensated for the communication, if it is, (3) informs individuals how they can opt out of future marketing communications according what is stated within Privacy Rule, and also
(4) elaborates why individuals that have specific characteristics or conditions have been targeted, how the service or product relates with their health. Covered entities must determine service or product may be of beneficial use to persons with the characteristic or condition targeted.

Other marketing communications should be done after obtaining authorization from individuals to disclose or utilize protected health information for creation or making the marketing communication.

**Contractors/Business Associates of Covered Entities**

Protected health information used in marketing may be only disclosed by covered entities to the business associates/contractors that undertake marketing activity on the covered entities’ behalf. No other disclosures for the marketing communication are permitted according to Privacy Rule. Also, covered entities should procure authorization from every person that is on a enrollee or patient list before they can be sold or given away. The covered entity should obtain the business associates'/contractors’ agreement to only utilize protected health information for purposes associated with covered entities’ marketing. Covered entities should not give over protected information for the contractor/business associate to utilize for their own purposes.

**FAQs :**

**How can I differentiate between activities for payment, treatment or health care operations vs. marketing activity?**

Marketing may occur while treatment, health care operations, or payment and under definition of “marketing” within Privacy Rule, doesn't require making the distinction for purposes of determination when the marketing rules are applicable. If marketing communication doesn't fall under any one exception to needing authorization by the patient, the covered entity should obtain authorization, without regard, of the time when the communication took place.

**Can telemarketers gain accessibility to personal health data and call patients to market services and goods?**

Yes, if telemarketer was only hired to take up marketing by covered entities and has agreed contractually to utilize the data on behalf of covered entities for marketing, as a contractor/business associate. The individual should authorize any other utilization of their protected information.

**Does this rule amplify the ability of plans, providers, marketers and also others to utilize my private health information to sell their goods and services? Does the rule make it easy for businesses in health care to engage in sales door-to-door and efforts at marketing?**

It does not. Privacy Rule is more restrictive when limiting the disclosure and utilization of health information in marketing than those that exist in many states. The Guidance provides two examples in marketing which now require permission according to Privacy Rule that may have been permitted in many states before the Rule was enacted:

- **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.**
- **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.**
Privacy Rule also places limits on the marketing activity of the business associates/contractors that were nonexistent prior to the Rule. As an example, according to Privacy Rule, the covered entities cannot give out protected information to door-to-door salespersons, telemarketers or hired marketers without making sure that the marketer agreed contractually to utilize the information to only market on behalf of entities involved and not for the marketers' personal use, or the use of third parties. Contracted marketers should identify covered entities that are sponsors of the marketing communication and should provide patients the option to opt-out of more marketing.

Do health promotion, disease management, preventive care, wellness programs fall beneath the “marketing” definition?

The activities that fall beneath the "marketing" definition depend upon how the activities have been conducted. The covered entities should examine the process with which these activities are conducted, and compare it to the activities that have been exempted from that defined as marketing to determine if authorization must be procured from participants.

Can business associates/contractors use private health information to sell to individuals for the contractor's own business purposes?

The covered entities should not provide protected health information out to business associates for their business associate’s use unless authorization has been obtained from the patients.

Background

Covered entities may always be able to disclose or use protected medical information which has been de-identified.

Research

45 CFR §§ 164.501, 164.508(f), 164.512(i)

Research Rules

The research rules in the Privacy Rule put restrictions on the disclosure or use for purposes of research protected medical information that hasn't been de-identified. The rules also deal with how the research subjects have been informed of how their medical data will be disclosed or utilized and how the research subject may obtain access to information regarding themselves when the data is held by the covered entities. Privacy Rule protects privacy of individually identifiable health information, ensuring that the researchers do continue to have reasonable accessibility to medical information required to conduct significant research.

Disclosing and Using Protected Health Information within Research

Certain disclosures and uses of protected health data are allowed with no authorization in the Privacy Rule. All other disclosures and uses must be authorized.
Unauthorized Research Disclosure/Use

In order to disclose or utilize protected medical information unauthorized, by the research participant, covered entities must procure one of the accompanying statements, as stated within 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 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 covered entities 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.

Use/Disclosure in Research Along With Individual Authorization

The covered entities, along with individual authorization, may disclose and use protected health data for research purposes. Authorization to release patient information for a study in research including treatment should include the research-specific factors. As an example, if plans to charge the patient's health plan by the researcher/covered entity is for routine costs associated with treatment, the authorization should describe the kinds of data that are given to the specified health plan.

FAQs:

Guidance deals with the questions below:

*Will medical research be hindered by the rule by causing doctors and others unwilling and/or unable to share information regarding individual patients?*

No. The Department doesn't believe that medical research will be hindered by Privacy Rule. It believes that health plan members and individuals should be more encouraged to participate in a research study when they know their private data is protected. An example, the Guidance provides is the affirmation that genetic studies in the National Institutes of Health, almost 32 percent of eligible patients offered a test in breast cancer risk refuse to take it, also of those who decline the test, the major portion cite concerns about medical insurance discrimination and privacy loss as a reason.

*Are the covered entities required to create a privacy board/an IRB before disclosing or using protected health information within research?*

No they do not. The Privacy Board or IRB may be independent or created by the covered entities.

*Does the Rule forbid researchers from setting conditions participation in a clinical trial following an authorization for use or disclose existent protected health information?*

Privacy Rule doesn't address the conditioning a researcher may utilize to determine who can or cannot be enrolled in a study. Thus, a researcher may set conditions on participation on receipt of an authorization.

*Are the Rule's requirements with regard to patient accessibility in synchrony with the provisions in Clinical Laboratory Improvement Amendments of 1988?*

True. If the clinical laboratories are covered providers of health care as well are forbidden by Clinical Laboratory Improvement Amendment to provide individual access to data, the Privacy Rule provides an exception individual access rules which does not require individual access to be provided for.
What does the Rule say about the right of the research participant’s to access to records or results of research?

Privacy Rule accords the patients rights, with few exclusions, to inspect and acquire a copy of medical information regarding themselves kept in the “designated record set.” As an example, one permitted exception is suspension of the individual’s access rights during a clinical trial if the individual has agreed to denial of access while consenting to participate in trial.

How is patient access within the Privacy Rule in sync with the provisions under Clinical Laboratory Improvement Amendments-1988?

Similar. Where those clinical labs that are deemed covered providers of health care do not permit an individual to access personal information under the provisions of Clinical Laboratory Improvement Amendment, the Privacy Rule also exempts them from individual access rules.
Chapter 3 – Assessments

1. In a ________________ atmosphere, where no individual entity creates the medical record, it is ambiguous with whom the medical record's ownership lies. (Page 27, Para 5)
   a) Medical
   b) Clinical data management
   c) Legal

2. The physician is obligated to keep medical records of patients private & confidential, a practice derived from ancient physicians' ________________ presently retained at its core, & also, further recent legal acknowledgment that a patient has a right to keep that information private that he/she desires to be maintained private. (Page 28, Para 2)
   - oaths
   - Promise
   - Decisions

3. Which systems allow health care organizations, payers & employers, through a core data storage system, to deliver & manage better care to employees, patients, & the insured? (Page 28, Para 4)
   - ABM
   - BBG
   - IIMM
   - CDM
Chapter 4

THE NAIC: PROTECTING CLIENT PRIVACY

Understanding the National Association of Insurance Commissioners (NAIC):

What is the NAIC?
The NAIC is the organization of state insurance regulators for all 50 of the United States, Washington DC, and five US territories. The NAIC’s primary objective is to help insurance regulators at the state level provide fair and reasonable service to all insurance consumers.

How does the NAIC work?
The NAIC is guided by a set of regulations and procedures in the provision of this assistance to various states. These regulations are drafted by committees specially convened for the purpose at regional meetings that take place every quarter. All NAIC meetings are open to unrestricted to the public who are also invited to comment on draft regulations. Each set of regulations or model must then be approved by a parent committee, and finally, at the NAIC’s plenary session, after which it is formally adopted. All members of the NAIC may vote for or against a model at these sessions. The approved model may either be adopted in its original format by a state, or be modified to suit local need of the state.

Protecting the Privacy of Health Information
The NAIC’s Regulatory Framework Task Force is responsible for the drafting of a model regulation to address the issue of the privacy of health data. The task force is accountable to a parent committee, namely the Accident and Health Insurance (B) Committee.

The Health Plan Accountability Working Group was set up in 1993 and was tasked with putting into place a comprehensive regulatory framework to govern all managed care bodies. The primary focus of the task force was to investigate the practice of collecting and sharing of personal health data, and to put in place requisite regulations to protect patient confidentiality. Initial drafts of the model developed in 1993 and 1994, drew heavily from an existing NAIC model, the "NAIC Insurance Information and Privacy Protection Model Act." However, the task force soon realized the need to have a robust regulatory structure in place first, and abandoned these drafts in 1995. The focus on privacy issues resurfaced in 1996 with the release of the new "Protected Health Information Model Act." The statement on the "Principles for Model Act Addressing the Confidentiality of Health Information" served as a guideline to the working committee during the process of drafting. In 1997, the working group, now called the Health Information and Privacy Working Group, was tasked with putting in place a model act to regulate the privacy of health data.

The NAIC identified a few reservations with allowing federal legislations to lay down the standards, namely
a.) the possible preemption of state laws that regulate health data that can be identified individually
b.) preserving the access to such information by insurance regulators so they may continue with their regulatory functions
c.) preserving the ability of states to develop and implement benchmarks for insurance carriers to collect and use such information
Preemption

The privacy of individually identifiable data is addressed explicitly in HIPAA. The Secretary is given responsibility of putting together a detailed set of suggestions to Congress in consultation with the National Committee on Vital and Health Statistics. Additionally, the HIPAA-added Section 1173(d)(2) of the Social Security Act mandates that the Secretary assume and implement appropriate security norms for health data that "ensure the integrity and confidentiality of the information" and that "protect against any reasonably anticipated...unauthorized uses or disclosures of the information...."

Provisions in current state statutes already deal with these clauses, and therefore, Congress’s expressly directs that federal regulations refrain, as far as possible, from preempting state laws.

The HIPAA also states that federal regulations developed after Section 264 was put in place should not displace any provisions 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." These statements are a clear indication that Congress places adequate protections on states and their ability to retain or ratify additional provisions, and positions federal norms as regards individually identifiable health data as minimum requirements.

Section 1178 of the Social Security Act, as added by HIPAA, also extends protection to state laws if they are determined necessary by the Secretary for the execution of any of the provisions set out in Section 1178(a)(2)(A). It also safeguards, without Secretarial intervention, any state law that "relates to the privacy of individually identifiable health data" and is therefore governed by HIPAA Section 264(c)(2). Section 1178 can also be seen as an expression of Congress’s aim that federal regulations not preempt the enactment of tougher state laws regulating confidentiality of individually identifiable health data. The objective is to allow state’s maximum flexibility in developing supplemental regulations to support HIPAA’s privacy benchmarks as they see fit. States should be allowed to develop local regulations that may even be more stringent for a couple of reasons:

· Several states already have in place strenuous measures to regulate the use and distribution of private health data. These laws may be more comprehensive than federal regulations, especially in the context of transactions as outlined in the Social Security Act. However, preempting these laws would actually result in downgrading the protection currently available to consumers in such a state.

· Where states are yet to develop comprehensive regulations to protect private health data, any federal preemption would work to limit a state’s ability to develop unique solutions to specific problems.

While carriers that operate in several states may benefit from having uniform privacy norms, the benefits are not necessarily passed on to a consumer, especially one from a state that already has comprehensive privacy protections in place.

Privacy and the Insurance Industry

State insurance departments also function as regulators of insurers in that state. These departments have access to highly confidential business, financial and personal data and therefore, substantial experience in safeguarding such information. This also includes proprietary information of insurance companies such as product and business practices information, actuarial formulas besides other financial data. While these departments are authorized to collect and assess confidential data in the performance of their regulatory duties, state laws prohibit the sharing of such information with other parties.
Federal privacy norms should not prevent insurers, health plan providers and other regulated bodies from sharing individually identifiable health data with state insurance regulators. Such information is vital to the successful regulation of such entities, without which consumers will remain unprotected.

State insurance departments usually access individually identifiable health data in the following scenarios:
· When investigating a complaint by a consumer
· When assessing the market conduct of an insurance provider or other regulated
· When assessing financial solvency
Federal legislation is expected to aid, and not impede, state regulators in the discharge of their duties.

Consumer Grievances
The state insurance department also investigates consumer complaints. When a complaint is filed against an insurer by a consumer, the consumer must also provide a written statement authorizing the investigating agency to procure the complainant’s medical records from the entity who is the subject of the complaint. Often, claims are rejected by an insurer claiming a benefit is not covered by the policy, or sometimes, that the treatment being claimed is an experimental one.

The investigating department needs to examine the consumer’s insurance policy as well as his/her medical records before determining whether the claim can be covered or not. Since the consumer has usually authorized access to their personal data, this doesn’t normally pose a problem. Such access also allows state regulators reliably identify problem insurers. Consumer complaints help regulators uncover unfair denials by insurers and recover millions of dollars each year, which eventually return to the consumer. In 1996, for instance, the Wisconsin Insurance Department investigated over 8000 consumer complaints, recovering over $2,300,000, over two thirds of which were from claims that had been denied.

Assessing Market Conduct
The state insurance department must also conduct assessments of an insurer’s market conduct in order to gauge the business practices of the insurer. These assessments include on site visits to the insurer’s office/s to review marketing practices, sales processes and claim payments, as well as a review of client complaints. Several states have regulations that allow the insurance commissioner to review this information. Regulators study individually identifiable health data in order to determine if a company uses similar standards of payments for comparable claims.

In conducting such assessments, regulators need to review files of several consumers. Usually, individual client consent for such access is not sought because it would slow down the assessments considerably besides making the task tedious. Sometimes, companies attempt to withhold client information claiming a potential violation of confidentiality. However, allowing a company to disguise client data such as names or addresses could also help companies deceive investigators by changing or fabricating claims. Federal laws that potentially diminish the powers of state insurance investigators would only hurt the consumer by giving companies more room to mismanage their operations.

As new norms for overseeing the functioning of managed care institutions get put in place, allowing state regulatory authorities a free hand in obtaining personal private information acquires greater significance. The NAIC recently implemented five model acts; these regulate the functioning of managed care providers across five broad areas, namely:
· the reach and spread of the health provider’s network, including additional contracts
· processes in place to address grievances
· procedures in place to regularly review utilization
· processes in place to monitor and ensure quality
· process of obtaining requisite credentials for employed health care professionals

Enforcing and monitoring each of these norms requires that the state insurance department be able to access individual records. This helps determine if regulated processes were followed; for instance, if required protocols were followed for utilization, or in complaint cases, how the process was followed from registration of the grievance, until how it was finally resolved or closed. Similarly, the effectiveness of a provider network may be determined by reviewing certain services and how clients who require those services access them. For instance, to decide if a health plan has an adequate number of geriatricians, a review of the clinical records of seniors in the plan would show how many times a geriatrician was visited or consulted, if each access happened in a timely manner and if overall, there had been adequate coverage for the needs of the seniors group.

Regulatory authorities need to periodically review individual records for another reason. The HIPAA explicitly prevents any insurer from determining eligibility for a health plan on the basis of "health status-related factors". Individuals that apply for a renewal of their policy cannot be refused if they meet the qualification requirements other than health status. Therefore, regulatory authorities must check random records to ensure that an insurer has not misused individual personal data in any way that is a violation of HIPAA norms.

Later amendments to the HIPAA such as the Newborns' and Mothers' Health Protection Act (1996) and the Mental Health Parity Act (1996) especially require that regulators have access to medical records to ensure that provisions laid down by the law are being followed, such as, for instance, norms pertaining to yearly and lifetime restrictions on mental health benefits.

State insurance departments follow confidentiality rules very diligently. Often, no copies are made of individual records being examined. In some states, the law mandates that these files be treated as confidential. These papers may not be subpoenaed or publicly disclosed until the review has been completed. Individual state departments additionally have confidentiality rules in place for employees to follow, modeled after NAIC’s Model Law on Examinations and the Market Conduct Examiners Handbook.

Assessing Financial Solvency

Besides market assessments, state insurance departments must also assess a provider’s financial solvency. This is done by reviews of financial statements to determine the ability of a provider to pay current and future claims. These reviews also require access to individual client records; for instance, the financial solvency assessment process requires cross-verification of claims against individual records in order to be able to evaluate compliance.

In summation, state insurance departments work to safeguard consumer interest by regulating insurance providers and ensuring that they comply with HIPAA norms. Without access to individual private records, such investigations or assessments of providers would not be possible. Federal laws should therefore be careful to not implement provisions that will seriously limit the ability of state regulators to fulfill their duties to consumer.

Health Information: Usage and Disclosure

State insurance departments also safeguard consumer interests by monitoring the compilation, use and sharing of confidential private information by insurance providers and regulated health care providers. The NAIC’s
“Insurance Information and Privacy Protection Model Act”, applies to any insurance agent, institution or support business. In addition to privacy regulations which govern managed care entities, there is a need to develop a set of regulations to govern health data for various reasons. For one, under the current model, private information can be disclosed under a general authorization. However, health data is not only confidential but also highly sensitive, and should be governed by more rigorous privacy rules. Also, the way managed care is provided has undergone huge changes over the past few years. As more health providers go online and access to patient data gets easier, maintaining confidentiality poses quite a challenge.

Any model the NAIC develops must be in accordance with standards set by the Secretary of Health and Human Services or adopted in federal legislation pursuant to HIPAA. In the course of developing a model, several issues have been raised, all of which are being reviewed by the NAIC’s working group. Feedback from interested parties such as HHS employees is also being considered. These include:

- Outlining the parameters of a model law. For instance, to whom will it be applicable – insurance providers, health providers, or both? How will it affect other second-hand users of the private information?
- Defining what the term "health data" refers to. Exactly what information will the law protect?
- How will the law define and treat disclosure? Will individual consent for disclosure be necessary? What processes will need to be put in place?
- How will an individual access his own information? What about changes to that information?
- Should any restrictions be put in place in allowing how an individual accesses his private information?
- How will any new law impact existing federal and state regulations?
- Defining violations and penalties.
- Determining if the regulations will be adequate for any electronic transactions involving individually identifiable health data
- Determining limitations, if any, to regulate the internal use and distribution of private data within a provider organization.

Some of the issues discussed above are also pertinent to HIPAA requirements which instruct the HHS Secretary to make appropriate recommendations to Congress. These recommendations should include counsel about individual rights in relation to individually identifiable information, processes required to ensure implementation of these rights, and authorizations required for the sharing or distribution of such information.

**Privacy Issues Working Group**

The NAIC Privacy Issues Working Group was re-constituted in a bid to encourage dialogue between regulators and anyone with an interest in the issue.

Most states already have privacy norms in place. As states move into the phase of interpreting and enforcing these protections, having a forum such as the Working Group to discuss issues and find resolutions is vital. The Working Group also serves as an overseer of sorts, trying to maintain some uniformity across all states. The Group’s responses will also serve as guidelines to NAIC members for the future.

The GLBA mandates all financial organizations, including insurance companies, have policies in place aimed at safeguarding the customer, especially with regard to the privacy, protection and integrity his or her private information. Regulators are mandated by the GLBA to similarly establish regulations to enforce these protections.

The Working Group has a draft model governing privacy standards in place which is being reviewed.
Task Force to Review Privacy Notices

This NAIC task force is concerned with the actual content of privacy notices that financial organizations provide their consumers, and to make sure that they are easily understandable to the average customer. The task force has also developed models or samples of such notices using ‘plain language’, that financial organizations are expected to emulate.

Model Insurance Information and Privacy Protection Act

The NAIC’s Model Insurance Information and Privacy Protection Act was first drafted in 1979, and has since been amended several times. The Act serves in part as an extension of the FCRA, as it was originally enacted, and includes provisions mandated by the GLBA and the privacy Rule. Covered by the Act are insurance providers, including agents, institutions, reinsurers, and other support businesses, and insurance lines including life, health, casualty and property insurance.

The Act aims 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.

The Act defines and regulates the following types of information:
1) information in medical-records
2) personal data
3) information classified as privileged

1. Medical-record information is defined as any information that is related to a individual’s physical or psychological health, medical history and/or treatment. Such information must also be procured from a qualified health care provider or institution. It may also be gotten from the individual's parent, spouse or legal guardian.

2. Personal information is defined as information that identifies the individual. It is any information that may be used to determine a person’s character, behavior, occupation, income, likes, health, reputation, etc.

3. Privileged information is defined as information that is associated with a particular individual and that is gathered specifically for an insurance claim, civil or criminal matter, or in reasonable anticipation of one.

Any of the above may be collected through a pretext interview as defined Under Section 3 of the model Act. This is an interview where a person attempts to procure personal data about another individual by

a) Posing as someone else
b) Falsely pretending to be a representative of someone
c) Misrepresenting the reason for the interview
d) Not providing proper identification

The Act permits such interviews to be carried out only if a reasonable basis for suspecting criminal activity, fraud, material misrepresentation, or material nondisclosure exists (usually in connection with claims). This reasonable basis must include specific information available for review by the insurance commissioner.

Section 4 of the model Act requires that anyone applying for insurance be provided with a written disclosure which describes how the insurer collects private and confidential information and how such data may be shared or used. The disclosure should also include information on privacy rights that the individual is entitled to under the Act.
Section 6 deals with authorization forms. These forms must include information on who within the provider’s organization will share or disclose personal data, and details on what type of information is most likely to be shared or disclosed within the organization and to any affiliates. Life, disability and health insurance disclosure forms are valid for a period of 30 months while disclosure authorizations for casualty and property insurance are applicable for a period of 12 months. Disclosure authorizations for claims-related information are applicable for the entire period of the claims process.

Section 7 of the Act details investigative consumer reports. Such a 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. The information thus collected; usually speaks about an individual's character, behavior, reputation, living habits, etc. Before an investigative consumer report is prepared, the individual concerned must be notified and given the option of requesting a copy of the report.

Section 8 concerns an individual’s right to access personal data about him or herself that has been collected by an insurer or other support business, and that can be reasonably retrieved. Any request to access such information must be in writing. The insurance provider, producer or other support business has up to thirty working days to respond to the request. The response must include information on the nature and substance of the information requested, how the individual can get a copy (in person or if a copy should be mailed), information about all others to whom this information has been disclosed or distributed, and information on the process to follow to update, correct or delete the existing private data.

An individual’s request for access may be denied if any information has been collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding.

Section 9 provides information on the process to follow to rectify, alter or erase disputed information. To begin with, all requests must be made in writing. The veracity of such requests must then be investigated by the insurer or other support business. If the request is found valid, appropriate action to modify or delete the information must be taken. In such cases, the individual must also receive notification of such action, as also

1) Any person specifically designated by the individual who may have received the information in the previous two years

2) Any insurance-support business that has systematically received such information over the preceding seven years, unless the organization no longer maintains information on the individual

3) Any insurance support business that supplied the information that has been changed.

If a change or deletion request if denied by the insurer, producer or support business, the individual may file a concise statement questioning the accuracy of the information. Anyone that subsequently accesses the personal data must then also be provided a copy of the concise statement.

Section 10, 11 and 12 discuss adverse underwriting decisions. These are defined as any denial of insurance, a termination of coverage, or the failure of an agent to apply for a coverage that the applicant requested. In casualty and property insurance, the definition extends to include coverage that has a residual market mechanism or coverage with an insurer that specializes in substandard risks, or when the information provided is different from that the applicant gave resulting in an increased rate of coverage. In life, health and disability insurance, this can include an offer for insurance at rate that is higher than standard rates.

Section 10 also mandates that an individual be notified of his or her rights to request further information in the event of an adverse underwriting decision. Further, the individual may also request specific information and its sources that directly resulted in the adverse decision. Complete information on the rights to dispute such information must be provided as well.

Section 11 provides insurers, insurance producers and other support businesses, the right to access information
about any prior adverse underwriting decisions in an individual's history, or any coverage the person may have received because of a residual market mechanism, as well as the reasons for such actions.

Section 12 provides that an insurer or insurance producer not make decisions about an insurance applicant because of a previous adverse underwriting decision or because he or she received insurance through a residual market mechanism. Further, no underwriting decision may be made on the basis of information procured primarily from insurance institutions. Instead, the insurance provider is expected to authenticate the information before using it to make an adverse underwriting decision.

Under Section 13, an insurance provider must necessarily obtain the individual's written authorization before sharing or distributing any private or confidential information. Information may be divulged if it will be used to avert fraud, or if it is being provided to state regulators or other government groups, or for a sale, merger, consolidation or transfer, and/or other business transactions. Where personal private information is being utilized for research, no identifying information may be included in the report. Where the information is used for marketing, all personal, privilege and medical information must be included. Individuals may also choose to deny the use of their personal data for marketing.

A cease and desist order may be issued by the state insurance commissioner in the event that any provisions of the Act have been flouted. The penalty can range from a $500 fine for each violation, to a maximum fine of $10,000. Insurers and insurance producers are also liable to a suspension or revoking of their license. If the order itself is defied, then the penalty may be re-assessed.
Assessment: Chapter 4

1. The NAIC’s primary objective is to help _____________ provide fair and reasonable service to all insurance consumers. (Page 1, para 1)
   a. insurance regulators at the state level
   b. insurance providers at the state level
   c. managed care entities at the state level

2. Which government body is responsible for investigating consumer grievances?
   a. NAIC
   b. State insurance department
   c. Privacy Issues Working Group

3. The _____________ Act aims to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance support businesses.
   a. Model Insurance Information and Privacy Protection Act
   b. HIPAA
   c. GLBA
Chapter 5

INSURANCE AGENTS AND CLIENT PRIVACY

Respecting Confidential Information

A major priority in the insurance industry has always been the protection of confidentiality of their clients’ personal data. As an insurance agent, you will be expected to balance the consumer’s desire to protect private information with your ability to provide the latest insurance products at competitive rates. In simple terms, the more information that you can get from the consumer, the better will be your product offering. The only way to achieve this is to gain the clients’ confidence that you will respect the confidentiality of any personal data provided by them.

It is important to make a distinction between public and non-public personal data. In the context of insurance, non-public personal data consists of any information shared by a consumer with an agent or broker. This includes personally identifiable information, lists of potential customers, or descriptions of consumer groupings. The GLBA defines a consumer as any individual dealing with an insurance firm, while a customer is a consumer who has entered into a business relationship with a particular firm. As an insurance agent, you will need to follow GLBA guidelines for both consumers and customers. This includes the requirement of providing information about your privacy policies to all customers, but providing them to consumers only if you intend to share any non-public personal data with a third party, unaffiliated organization.

The best approach is to clearly state your confidentiality policies and practices to the customer from the beginning of any business relationship and provide annual updates. These policies need to clarify that customers have the right to limit distribution of any financial data they share with you. Specifically, they need to know that you will not be using the information for any marketing purposes other than those related to your insurance products. An exception could be products or services that are offered by an affiliated organization. Such policies also include clauses that permit customers the right to access and update their information, if required. Other clauses are needed to allow insurance firms the right to share the same information when it may be required for the purpose of issuing contracts or servicing customers.

When it comes to medical information about a customer, there is general agreement that greater confidentiality is required. The life insurance industry has a strong professional history of handling and protecting its customers’ sensitive medical information. This has enabled it to draft and adopt a wide-ranging statement of principles that safeguard the confidentiality of medical records related to customers.

Impact of Privacy Laws

In addition to implementing their own confidentiality policies, insurance firms need to follow new privacy laws and rules. These rules apply to all individuals or business entities that are licensed or authorized by the local State Department of Insurance. In general, insurance companies need to find an approach that balances the customer’s right to privacy with business requirements. This can avoid a situation where your customer will be snowed in under tones of updated notices and your agents will spend valuable hours away from the field. Since the industry consists of a range of firms that offer different products and deal with distinctive types of personal data, federal law does not stipulate any one privacy policy. Each firm is responsible for adopting policies that honor the requirements of the privacy laws.

The best method seems to make a definite determination whether the agent or the insurance company is responsible for providing the required confidentiality notices. For example, under privacy laws an agent or broker who collects protected financial data for a particular insurance firm is not liable with notice and opt-out
requirements, as long as the information is shared only that particular firm. In this case, the company itself needs to comply with the requisite privacy requirements.

However, there may be instances where the agents shares a customer’s information with third-parties, or where the agent accepts a fee for additional advisory services, such as investment, economic, or financial advice. In these instances, the agent is clearly required to provide all the necessary confidentiality notices, including opt-out clauses.

Certain insurance companies allow the agent to directly hand over the initial notice at the start of a relationship with a new customer. However, it is then the company’s responsibility to follow-up with the required annual notices as per the GLBA and privacy rules.

An interesting variation in applying privacy laws is the case of independent insurance agents.

Mr. Axel Cummins, an independent agent, prided himself on doing the best for his clients. “Come to me,” he would declare, “and I can guarantee you the best insurance policy your dollar can buy!” To keep his promise, Cummins would personally visit each client and obtain detailed information. This helped him get a better idea of the needs and requirements and suggest individualized insurance products. Once he and the client were in agreement, he would visit at least three competing insurance firms. “Of course, I had to share my clients’ information with them,” he stated, “otherwise it was difficult to get quotes for the relevant products!”

In most cases, the client would select from among the insurance companies and things would end well. However, in the fall of 2006, Cummins was startled when he received a breach of clause notice from an erstwhile client. It turned out that Cummins had recommended company XYZ to the client in 2004, and the necessary papers were signed. However, the client claimed that Cummins had not followed up the first confidentiality notice with any further updates.

“My husband was lawyer,” she sniffed, “Don’t think Mr. Cummins can pull a fast one on me! I was his client, and he should have kept me informed. That’s the Law!”

In the fictitious scenario given above, Mr. Cummins may have been sharing his client’s information with several insurance companies. However, it is the responsibility of each of those insurance firms to apply the privacy laws applicable for both consumers and customers. Thus, Mr. Cummins was not responsible for the annual updates, but company XYZ certainly was! The exception is, of course, if the independent agent plans to disclose the client’s information to parties other than the insurance firms; here, he is responsible for providing the client with confidentiality notices and opt-out opportunities.

Potential Conflicts

As stated earlier, federal law has no single stipulation for all insurance companies, and each firm is responsible for drawing up suitable policies and guidelines. As new privacy rules are developed, you as an agent may face some areas of potential conflict. For instance, HIPAA clearly states that information such as names, addresses, social security numbers, and payment histories fall into the category of protected private health data, which is subject to an opt-in standard. This would mean that you cannot share any of this information with another party without express written permission from your client. However, many state privacy laws consider the exact same information as “financial data” that is subject to standard opt-out standards. So you could potentially find yourself in a situation where your confidentiality policy is in alignment with your state law, but in breach of
HIPAA!

You could face certain hurdles even in situations where you are clearly attempting to help your client. For example, you may have to share certain personal data with third-parties (such as pharmacies or out-sourced companies) while processing a client’s claim. Privacy laws require that you keep your client informed of your intentions or obtain permission to do so. Language too can play a part in creating scope for legal conflicts. Consider the fact that some privacy rules require you to obtain “client consent” while others require “client authorization” before sharing non-public information. The difference may be minor, but it could mean you are in breach of law! (See page 96).

Another semantic minefield is in the laws that deal with exemption from disclosure. Some of the privacy laws appear to exempt who are hired by a compliant carrier. However, DHHS regulations imply that any assessment of providing exemption is less a function of definition and more of use. For example, DHHS will exempt you from disclosure for sharing client information for the purpose of treatment and health care operations, or payment. However, the critical subject of underwriting has been left out!

All of these areas of potential conflict (and they may grow!) make it an urgent necessity that you invest time, effort, and commonsense towards drafting a robust privacy policy.

Creating an Effective Privacy Policy
It is imperative to remember that your privacy policy constitutes a contract linking the insurance company and the customer. As such, it needs to ensure that all legal requirements towards GLBA privacy rules dealing with non-public personal data are satisfied, both for consumers and customers. However, as seen earlier, there are many potential conflicts in implementing privacy rules. Hence it makes good sense to include comprehensive alternative dispute resolution clauses. This can help you reduce costs associated with any legal processes arising from future conflicts.

Often, an insurance company may be dealing with a range of similar products. In such cases, it may be a good idea to consolidate all the multiple privacy policies and put out a single, comprehensive policy. This will greatly reduce any conflicting obligations and confusions, both for agents and customers. Many companies find that a quality assurance program helps to ensure that all customers receive notices well in time, and all follow-up maintenance activities are organized and followed by all employees. Remember that any lapses may reflect on the company’s public image. An adequate errors and omissions insurance will also help to cover any potential liabilities arising from the privacy policy.

Scope of Marketing Personal Information
As you have already seen, your company’s privacy policy needs to include opt-in or opt-out standards to enable consumers and customers to decide whether their information is shared for marketing purposes. The goal of these privacy laws is to protect the confidentiality of non-public private information from being used without the client’s express permission. However, these regulations in no way are meant to inhibit insurance companies from providing clients with the best possible products and services, or to prevent medical professionals from disease management activities and mailing helpful information such as appointment reminders.

Misrepresentation
So far, we have covered your obligations as an insurance agent or broker while dealing with confidential information. However, note that information obtained by individuals who represent themselves as someone other than who they are can be considered an infringement of privacy laws! This can invite penalties associated with deceptive trading principles and violation of the Insurance Information Privacy Act.
A group of insurance agents in California wanted to sell senior citizens annuities. However, the process of collecting information about potential customer assets was proving to be a tedious process. Then they hit upon what they considered was an innovative marketing idea called a “living trust mill”. The agents organized seminars exclusively for senior citizens with the stated purpose of sharing information and knowledge about setting up living trusts. During the course of these seminars, they obtained detailed private financial data from a large number of senior citizens.

However, the regulatory bodies took a dim view of this scheme and the agents were found culpable of misrepresenting themselves as authorities in real estate planning.

Global Privacy Concerns
In this century, the internationalization of economy and growing development of e-commerce has brought forth new challenges for the insurance agent. You may find that you need to develop specific privacy policies to deal with international clients. For instance, many foreign nations have privacy laws and rules that are more restrictive in imposing specific privacy obligations when compared to the United States. Often the key difference lays in the fact that American economic sectors are comfortable with self-regulation, while other countries have statutory or administrative guidelines and obligations.

Principles of Safe Harbor
Looking at the international economy, the European Union (EU) privacy rules have generated some interesting debate in the United States insurance industry. In effect, EU rules prohibit transfer of any EU citizen’s data to any nation deemed to have inadequate privacy protection, including the United States. This has placed two choices in front of American insurance companies: either modify their company privacy policy to conform to EU directives, or confirm with the safe harbor principles.

These principles are being specifically created to create uniform standards that can allow American insurance companies to receive data under EU privacy rules.

Notice ~ All individuals must be informed about the purpose(s) for which their information is being collected by an insurance company. This notice must include contact information for the insurance firm, provisions for complaints or inquiries, nature of third parties that may obtain access to the individuals’ private information, and extent and means of choices to limit use and disclosure of the information. The notice has to be in clear and conspicuous language and should be provided when personal data is requested or soon thereafter. Under all circumstances, the individuals need to be provided the notice before any information is disclosed to third-parties or used for purposes other than originally stated.

Choice ~ Insurance companies need to include the opportunity (opt-out) for individuals to select both how and whether any personal data is shared with third parties, in cases where the disclosure is unconnected from the purpose for which it was collected (or purpose that was stated in any notice communicated to the individual). Information about readily available means to exercise this opt-out opportunity must be communicated in clear and conspicuous language. Certain types of sensitive information will require affirmative or explicit opt-in options. This will include medical or health data, race or ethnicity related data, political opinions, trade unions membership, religious or idealistic beliefs, and sexual preferences.

Onward Transfer ~ Insurance companies may disclose personal data to third parties only within the framework
of the principles of notice and choice. However, even when information is shared with a third party within the guidelines of these principles, the insurance companies need to ensure that the third parties are also compliant with the safe harbor principles. If not, it is obligatory for insurance firms to enter into a written agreement with third parties to ensure that the privacy protection offered remains consistent with the appropriate safe harbor principles.

**Security** ~ Any private information collected from individuals needs to be stored under reasonable measures to protect it against loss, misuse or unauthorized access, alteration, disclosure, and destruction. Insurance companies also need to create, maintain, and use systems that assure reliability for intended purposes, as covered under the principles of notice and choice.

**Data Integrity** ~ Insurance agents should only process information in a manner consistent with the purpose(s) for which it had been gathered. They need to take reasonable action to make sure that the data remains correct, absolute, and up to date.

**Access** ~ Individuals who have provided personal data to an insurer should have reasonable means to access that information. This includes the right to correct or modify that data to ensure its accuracy. In this case, reasonable means will depend upon the nature of information, intended usage, sensitivity of data, and the associated expenses and difficulties of providing access.

**Enforcement** ~ Every insurance company that wishes to comply with the safe harbor principles needs to include relevant mechanisms in its own unique privacy policies. This will include clauses providing recourse for individuals who have provided information, in the case of any non-compliance or potential conflict. Recourse should include the consequences for insurance firms that fail to follow the safe harbor principles.
1) An agent working exclusively for a single insurance firm collects some non-public information from a client for the purpose of quoting potential insurance products. Under which of the following circumstances would the agent be responsible for providing privacy policy notices? (Page 2, paragraph 3)

a) The agent shares the client’s information with his insurance agency
b) The insurance firm shares the information with an affiliated organization
c) The agent accepts an advisory fee for financial counseling
d) The insurance firm markets the client’s information to a third-party

2) While drafting privacy policies, an insurance firm needs to consider the impact of potential liabilities due to conflicts with various privacy laws. Which of the following can help mitigate the risk of such liabilities? (Page 3, paragraph 4)

a) Errors and omissions insurance
b) Conflict resolution clauses
c) Privacy and security insurance
d) Third-party liability clauses

3) The compliance of third-parties is covered under which of the safe harbor principles? (Page 6, paragraph 4)

a) Notice
b) Onward Transfer
c) Security
d) Data Integrity
Chapter 6

PRIVACY DISCLOSURE REQUIREMENTS

Common Terms and Definitions

As an insurance agent, you carry a serious duty to ensure that your client’s privacy is respected and maintained. This includes understanding the exact disclosure requirements where data can be shared with other parties in an open, ethical manner. The first step is to familiarize you with commonly used terms and definitions in disclosure regulations:

**Affiliates:** These are two business entities where either has the power to control the other, or both are under the common control of a third entity. For example, an insurer and a bank could be affiliates under the terms of the GLMBA.

**Consumers:** In the insurance industry, consumers are individuals who want to acquire a product or service offered by an insurance company. For instance, any person who fills an application towards an insurance policy is treated as the consumer of the company offering the policy. In addition, the beneficiaries and claimants on an insurance product are also defined as consumers.

**Customers:** Once consumers get a product or service from an insurer, they are deemed to have initiated a business relationship with the company and are known as customers. This includes individuals who have paid you a fee for investment, financial, or economic advice.

**Covered Entity:** The regulations of the financial privacy rules state that any “covered entity” needs to either issue or supply privacy disclosures, as applicable. Such an entity includes any business or individual who have obtained authorization issued by the Department of Insurance.

**Insurers:** This term covers all the entities that are required to follow privacy regulations, including insurance firms and financial organizations.

**Licensees:** This refers to all individuals who are duly regulated by the Department of Insurance, and are required to provide privacy disclosures, unless specifically exempt.

**Nonaffiliated third party:** This is any company or individual who do not share an affiliation with an insurance agent, agency, or company.

**Nonpublic personal data:** This can be defined as any private information that can specifically identify an individual person. In most cases, this includes basic information such as names, addresses, telephone numbers, and social security numbers. In addition, nonpublic personal data could include ownership of insurance products, details related to service provisions of such products, and figures related to payment for insurance products or services. Commonly accepted exceptions include openly accessible information or statistical data that cannot identify individual people.

**Opt-Out:** In general, information about a person can be shared or communicated with others, if there is no specific notification from the individual requesting protection of the information. In insurance, an “opt-out” allows the customer to prohibit agents or companies from sharing personal data with non-affiliated third parties.

**Opt-In:** In this case, express permission in the form of permission or consent is required from an individual...
before his information can be communicated to any third party.

**Privacy Policy Statement:** This is a disclosure form that can be handed over in printed format, or put up on a website, clearly stating the insurance agency’s intentions regarding nonpublic personal data obtained from customers. This needs to stipulate if any information will be shared with affiliates or unaffiliated third parties, along with details of any “opt-out” clauses. Such privacy policy statements may include a list of non-affiliated entities, a description of the nature of information that is typically shared information with them, disputes resolution clauses, the agency’s right to sell the information if the business is put up for sale or transferred, and the right to modify the policy in the future. Finally, there needs to be a mechanism that allows the customers to acknowledge receipt of the policy statement.

**Universal Client Privacy Rules**

These are some of the privacy rules that should be addressed in any policy statement, irrespective of the specific nature of business of an insurance firm.

**Regarding Consumers:**

Licensees may disclose a consumer’s nonpublic personal data to a nonaffiliated third-party ONLY if the consumer grants permission.

Licensees need to provide consumers with a privacy policy, including an opt-out notice, in such time that there is a reasonable opportunity opt-out prior to any sharing of information.

Licensees may disclose a consumer’s nonpublic financial or health data to a non-affiliated third-party only if:

- The consumer receives a notice prior to any disclosure
- The consumer receives clear details of the opt-out opportunity and procedure
- The consumer has reasonable time to exercise the opt-out before disclosure and
- The consume selects not to opt-out

Under the GLBA, all insurance entities (including agents) and financial organizations are obligated to create and provide a notice of their privacy policies and practices to customers in understandable language. This first mandatory notice has to be sent out when a business relationship is established with the customer, with follow-up notices on an annual basis. The GLBA does not mandate any information handling practices, but it does expect that these practices, as followed, be disclosed in the notice. In essence, most agents can meet the GLBA client privacy requirements with an uncomplicated disclosure form.

**Regarding Customers:**

Customers need to be provided with annual notices regarding the licensee’s privacy policies up to the point when the business relationship ends. That is, licensees are not obligated to provide notices to former customers.

A licensee may disclose a customer’s nonpublic personal data to a non-affiliated third-party only after providing a suitable notice to the customer.
A privacy notice needs to provide comprehensive information about the licensee’s privacy processes and procedures, details of opt-out notice and procedures, and a reasonable time limit to exercise the opt-out clause before any disclosure of information.

Licensees may disclose a customer’s nonpublic personal data to a non-affiliated third-party only if:

- The customer receives a clear notice prior to any disclosure
- The customer receives a valid description of the opt-out clause and procedure
- The customer has reasonable opportunity and time to exercise the opt-out clause before disclosure and
- The customer does not choose to exercise the opt-out opportunity

**Exemptions**

While most regulation laid down in federal and state policies apply to all agents, there can be certain exceptions. In these cases, an agent may not have to comply with opt-out requirement and special disclosures when:

- The agent is selected by an insurer or designated agency that provides and complies with all the privacy notifications as required by privacy regulations, and
- He shares personal financial data only with his company (agency) or affiliated entities.

If the agent wishes to share an individual’s personal data with any entity other than his own, he will then need to provide a copy of the privacy notice and offer the individual the opportunity of prohibiting any disclosure to third parties.

While these generally accepted principles of exemptions appear to cover all the bases, there are some hindrances. For example, an agent may not provide a customer with a disclosure privacy policy in good faith, thinking that his agency will follow up. However, the agency may not follow through with annual notices, as required under regulations. Staff changes, business shutdowns, and sheer oversight may leave your customer dangling. Perhaps the only solution is for an agent to personally follow up on every consumer and customer to avoid falling short of regulatory practices.

**Essential Recipients**

If your agency or insurance company does not offer to provide due notices, it becomes your responsibility to provide suitable policy statements to your customers who purchase any insurance product or service. This includes the initial notice at the start of the business association (as stipulated under GLBA) and annual follow-up notices. For consumers, a notice must be provided only in cases where you have an intention of sharing or selling nonpublic information to a non-affiliated third party.

**Mandatory Disclosure Information**

In general, federal and state privacy laws simply stipulate the nature of facts that need to be disclosed to consumers and customers. There are no legal requirements as to the exact design of the privacy policy used by an insurance company. It is mandatory that certain facts are clearly stated in understandable language, and
displayed in a manner that makes them easily noticeable. You will find it good practice to use short, clear sentences in simple language. Usage of bullets also helps to present information in discrete installments.

Some of the features you might want to include in a privacy notice are:

- **Categories of**
  - Nonpublic personal financial data.
  - Nonpublic personal financial data.
  - Affiliates and nonaffiliated third parties with whom information is shared (except as part of an insurance transaction).
  - Nonpublic personal financial data disclosed about former customers (with details of parties who received the information).
  - Information disclosed due to contractual relationships, servicing or marketing (with details of parties receiving the information).

- **Explanation of the consumer’s opportunity to opt-out of disclosure to nonaffiliated third parties (with details of procedures and methods).**

- **Processes and procedures followed for protection of confidentiality of nonpublic personal financial data (including secure storage).**

- **If any information is disclosed as part of insurance transaction, it is made to other affiliated or nonaffiliated third parties as permitted by law.**

An important aspect of a privacy policy statement is that it includes some general description of the type of information you might expect to collect from an individual. This can include the manner of data collection (such as interviews, forms, or websites) and practices followed to ensure information is stored confidentially, with polices designed to ensure the veracity and excellence of the data. You also need to provide comprehensive details of the kind of data that may be potentially shared with affiliated and non-affiliated third parties. This includes any information-sharing agreements with third-party service providers, marketers, and other entities. Of course, the policy statement needs to clearly communicate the individual’s right to opt-out of disclosure of any nonpublic private information with third-parties.

**Regular Follow-up**

Once you enter a business relationship with a customer, it is obligatory to give a privacy policy statement at the start, and to follow up with annual notices, provided that the relationship is maintained. The initial notice may be given in many different forms. In some cases, the agency and insurance company may prefer to provide separate notices to the customers. In other instances, a joint notice may be created, or the insurance company’s notice may suffice by itself.

Note that this initial notice (which states the intention to provide the disclosure policy) can be provided with the delivery of the actual insurance policy, while the actual notice may be grouped with other official communication, such as billing for premiums. A similar mechanism can be used for the annual follow-up notices.

An important exception is the case of title insurance and similar real estate related services where there is only a one-time interaction with the insured party. Here, there is no mandatory requirement for annual notices.

Group cover are also regulated slightly differently. Here, the obligation of providing notices is limited to the plan sponsor, and individuals need not be notified. However, if there is an intention to share the participant’s
personal data with non-affiliated parties, the privacy policy needs to be made available to all individuals.

**FAQs on Financial Privacy**

The following list of frequently asked questions attempts to provide you specific answers to situations that you may face on a day-to-day basis in the insurance industry. However, these should be treated as guidelines rather than hard and fast rules. Always ensure that your state’s privacy laws are honored and any updates to federal and state laws are factored in. In most instances, your company’s senior officers should be able to give you the best possible advice.

**Does every agent need a privacy policy?**

Very much so. Under law, an agent is considered to be a financial organization, which obligates him to comply with the privacy policies outlines in GLBA. However, an agent can consider himself exempt if his company or agency is responsible for distributing privacy policies.

**As an independent agent, I represent many insurers. What responsibilities do I have under the privacy rule?**

Even independent agents are subject to the regulations. However, you do not need to comply with the requirements related to notices and opt-out clauses if:

- Your company (companies) or your designated agency is in compliance with the regulation; and
- You don’t intend to share protected information with any entity other than that company (companies), agency or any third-party affiliates of the company (companies) or agency.

**I am an autonomous agent. I usually share my consumers’ information with several companies in order to obtain the best prices on insurance products and services. Can I continue this practice under the privacy regulations?**

Yes, you can, since the regulations allow you to share nonpublic personal financial data with several companies for the express purpose of comparing prices. This has to be done at the consumer’s request. Your clients will be treated like consumers for each of the insurance firms, and are therefore entitled to complete privacy and opt-out notice from the respective companies.

**In my capacity of an independent agent, I get paid for servicing and dispensation functions by multiple insurers. Do I need to provide any notice when exchanging private information?**

Not really. The regulations allow an insurer to share nonpublic financial data with service providers that function for the company. You certainly qualify on that point. The only mandatory requirement is for the company, which must give an initial notice to consumers before sharing the data. In addition, the third-party (you) must have a written agreement that safeguards the privacy of the information from use in any purpose other than intended. In addition, re-use and re-disclosure provisions are also applicable to the company.

**I represent several companies. How do I know which of these send out notices and which don’t?**

The answer is simply good communication. When you are engaged in any business relationship with an insurance company or agency, it is essential to have clear channels of communication to address all aspects of
compliance with regulatory requirements.

**I am a paid agent of an insurer and deal exclusively with the product line offered by that organization. What is the extent of my responsibilities under the new privacy rule?**

As an agent, you are subject to all the regulations in the new privacy rule. However, you do not need to comply with the requirements related to notices and opt-out clauses if:

- Your company is in compliance with the regulation; and
- You do not intend to share protected information with any entity other than that company and its third-party affiliates.

**I am an agent who has absolutely no intention of ever sharing my client’s private information with anyone but my company? Does this exempt me from requiring a privacy notice?**

You could be exempt if your company does provide notices on policies and procedures, as per GLBA guidelines. However, there is no reason why you should not give a basic policy statement that lets your clients know that their privacy will be completely protected. After all, this little step can go a long way towards building trust and goodwill in a long-term business relationship with your client.

**What are the guidelines on disclosure of personal health data?**

In almost all states, disclosure of an individual's nonpublic personal health data is not allowed, even to an affiliated third-party. Express authorization from the concerned individual is required. This must include:

- The individual’s identity.
- Description of the nature of information to be revealed.
- Descriptions of third-parties who would receive the information.
- The person’s bona fide signature.
- The time limit for which the authorization is applicable.
- The process for revoking authorization.

**Since there is now a new privacy rule, am I obligated to visit all my existing clients to inform them of the development?**

In some cases, you may have to. If your clients are also customers, then they need to be sent mandatory privacy policies and opt-out notices. However, if the company (companies) that appointed you is in compliance with the regulations, you may be exempt. It would be best to get the required information from the concerned insurers.

**One of my clients didn’t get any notice or privacy policy from my company. Can I be held responsible?**

In the eyes of the Department of Insurance, any failure to give a mandatory notice is a clear violation of the regulations. This may even attract prosecution under unfair trade practice laws. If any personal data has been shared without providing an opt-out notice, this leaves open the possibility of a civil action.

The best solution for you is to start using your own simplified privacy notice. In the future, if the insurer may be in any violation of compliance, at least you can prove that it is was not your responsibility.

**My agency receives several requests for information over the phone related to insurance products. Do all of
**these callers qualify for receipt of my agency’s privacy policy?**

It all depends how far the phone call goes. If the person is simply requesting information, then he is a consumer. However, if you collect private information over the phone and then intent to share it with non-affiliated third-parties, you will need to provide your privacy policy, with an opt-in notice. If the phone caller goes further and actually buys a product over the phone, then he is a customer and you are obligated to provide the necessary notices.

**I work as an agent for a single company. With reference to the privacy laws, can I be considered as an associate of the company?**

Not at all; the definition of affiliate clearly states the parameters of the relationship and you do not qualify.

**I work for an insurer that deals in several types of products and services. Can my company share information with me for strictly marketing purposes?**

Yes, it can. The regulations allow companies to share an individual’s information for promotional purposes with the agent who is acting in the capacity of the individual's agent.

**Am I allowed to share my client’s information with my own company for marketing purposes?**

Only in cases where the individual has been made aware of the intent to distribute the information in a valid privacy notice.

**My company provides my clients with its own privacy policy statement and opt-out notices. Recently, I disclosed information about an existing customer with a non-affiliated third-party. Does this mean I have lost the exemption under the “licensee” definition? Do I have any new notice and opt out responsibilities to the customer?**

It depends on the exact situation. If your disclosed information to a third-party that was mentioned in the privacy policy, for purposes outlined in that document, then you have no fresh obligations. However, if you have disclosed information to some other third-party, or for your own purposes, you have lost the exemption and regulations apply to you.

**What is the duration of a customer’s “opt-out” request?**

In the eyes of the law, it is literally until infinity, or until the customer provides a written statement revoking the opt-out.

**As a broker, am I subject to the same exemption as an agent under the definition of “licensee”?**

Many states consider brokers to be equivalent to agent when it comes to privacy regulation. Hence, if you can demonstrate that you are a representative of the insurer (principle), you are subject to agent exemption.

**As an independent adjuster, will I be treated like an agent under the new privacy law?**

Yes, you will share the same responsibilities and exemptions as any agent.

**I heard that agent exemption applies in instance of business conducted through a clustered agreement or broker. Is this true?**
Yes.

*Recently, my agency sold its assets, but not the company. Does agent exemption still apply?*

Yes.

*Can I share with associates and affiliates? Is the sharing only limited to associates of the principal? What if a bank is an affiliate?*

If you are benefiting from the exclusion as defined in the “licensee” definition, you are not allowed to disclose nonpublic personal financial data except to the principal and it’s affiliates. If you choose to disclose this data to other associates, then you must provide the required notices.

*What are the acceptable channels for disclosing privacy policy statements to my clients?*

Your best bet is to get a clarification from the local regulator, who can help you understand the applicable state laws. Note that you may have to modify your manner of distribution from state to state. In general, you can disclose the notice in a brochure or newsletter. Other valid options include any renewal notices, direct mailers, and opt-out notices.

*To reduce overheads, I often send out privacy notices and opt-out notices in the same mailing as health data authorizations. Is this in compliance with regulations? What about combining notices from affiliated companies in the same mailing?*

In general, you are allowed to mail out privacy policies, opt-out notices, and health data authorizations jointly. It is also permissible for affiliates to share the same mailing. However, regulations do state that each notice must clearly identify the company that sends it out. In addition, all information must be accurate, easy to understand, and easy to find.

*Recently, a customer called me from his lawyer’s office and requested me to fax a duplicate of his policy on the attorney’s number. Does this qualify as an agent exception?*

In this case, it does since you shared information at the express desires of your client. However, you may want to update your client’s file with details of the request.

*One of my customer’s policies is coming up for renewal. I think I may be able to find her a better deal with a new product. Do I need to provide any notice to the customer before using her information to get quotes from other insurance companies?*

If your customer has not specifically requested any quotes, you will need to provide the necessary privacy notice and opt-out notice. If she has requested you for the quotes, you have no such obligation.

*Is it okay to share my clients’ personal financial data with the Department of Insurance?*

Yes, since it is a regulatory body with jurisdiction over insurer or agent disclosures.

*Recently, a fellow agent told me that she often requires her clients’ social security numbers if they wish to exercise the opt-out option. Is this standard procedure?*
Not really. The language and content of the regulations do not show any intention that a client should have to share her social security number in order to opt-out. Compliance with any such request will be purely up to the client. This optional choice should be communicated to the client if a social security number is requested. In short, any client’s opt-out is completely valid without the social security number.

**In policies where the insured party and the policy holder are two different individuals, who should I send out all notices and policy statements?**

It all comes down to the definitions of terms commonly accepted in the insurance industry. Your policy holder is a ‘customer’ who has a business relationship with the insurer. This entitles him to all the mandatory initial and annual notices. The insured person is a consumer when the insurer has any intention of sharing personal data with a non-affiliated third party.

**What impact does the new rule have on the disclosure of beneficiary information?**

Private information about a beneficiary is also protected by the new regulation. In simple terms, if you have any intention of disclosing nonpublic information about a beneficiary to a non-affiliated third-party, she is then considered as a ‘consumer’ and will need to be sent the mandatory notices and opt-outs.

**My insurance company often provides me with access to third-party claimant information. Does this put me under any privacy obligations?**

Insurers often provide their agents with such access. You have no specific privacy obligations other than the commonly accepted obligation to maintain the privacy and security of the claimant’s personal data. Under the new regulation, a claimant has the same rights to a notice as any other consumer, only in cases where you have the intention of divulging the information to non-affiliated third-parties.

**My insurance company offers on-going settlement options to beneficiaries and claimants. If a person submits a claim to this option, is he a consumer or customer?**

All beneficiaries and claimants in an insurance policy are considered as consumers under the new regulation. This obligated your company to provide notices and opt-out opportunities as per the guidelines.

**Is it mandatory for HMOs to send initial notices and opt out communication to subscribers and dependents?**

All HMOs are treated as ‘licensees’ by federal regulations. Thus, they have the same obligations as any other insurer when it comes to privacy policies and opt-out notices. Even group HMO coverage is treated similar to that of a group insurance plan. Basically, HMOs need to send mandatory communication to all their individual customers and to the group policyholder in any group plan. If the HMO intends sharing personal data about the individuals in a group plan, then all individuals will need to be sent privacy policy and opt-out notices.

**My agency deals in many single premium policies and paid-up policies. I wanted to know if the regulatory notice and opt out requirements apply to such policies.**

It all depends on the calendar. If you have had no contact with policy holders of single premium and paid-up policies for a period of twelve months before July 1, 2001, then you are not required to send any privacy communication. Essentially, the policies will be considered dormant. In all cases of purchase or contact post July 1, 2001, normal regulations do apply.

**I deal only in variable annuities. What impact do the new regulations have on my business?**
You are subject to all the mandatory requirements and disclosures as any other licensee.

*If a health insurer has only basic identifying information, such as names and addresses, but not financial or health data, is it still covered by the new regulatory privacy requirements?*

The issue here is how to separate purely identifying information from nonpublic private information. For example, an unlisted telephone number could be considered as nonpublic personal data. It is best to provide privacy policies and opt-outs in every case where any information could be shared with a non-affiliated third party.

*I deal in some large employer groups, defined under ERISA as 50+ plans. What privacy obligations am I under?*

You will need to follow the guidelines for any group insurance plan. The new regulation is not preempted by ERISA.

*This is a question about group plans. If I want to share information about individuals from the group, I know that I need to send out privacy policy information and opt-out information to all the policyholders. However, if I am unable to find contact information about a particular person, what should I do? What about the same situation in regard to claimants or beneficiaries?*

While this is an interesting scenario, it is also highly unlikely considering the level of information collected during the policy creation. on the other hand, if you are unlucky enough to run into this situation, you can rely on the group policyholder to take sound measures to obtain additional contact information about any individual.

*In a workers’ compensation policy, who receives the privacy notices?*

In a workers’ compensation plan, the participants are also the policyholders (customers). Hence, notices will need to be sent out to all such policyholders.

*There are so many different institutions and individuals in the industry. How can it be clear when the new privacy regulation is applicable, and when they are not?*

The answer lies in the definition of licensee. If an individual or institution is offering an insurance product or service to a consumer, it is a licensee and is covered by the regulation. Evening cases where an individual cannot be clearly identified as a consumer, any nonpublic personal data about the individual is still protected by the regulation.

Some specific exceptions to the regulation are viatical settlements, business auto policies, key man insurance, personal umbrella policies, and professional liability coverages. Such exceptions are generally commercial products that are not for personal or family coverage. Any nonpublic personal data collected while underwriting such policies is not covered by the new regulation.

*I know of a case where a TPA that is not mandated to be a licensee is also providing stop-loss reinsurance to a somewhat self-funded group. The stop-loss reinsurance is provided by an insurer who claims that it is not a group plan. Who is responsible for sending out any notices? And to whom should it be sent?*

It all comes down to who can access any nonpublic personal data. If the insurer providing the stop-loss policy...
has such data about the covered individuals, then it needs to treat this as any other group insurance plan and follow the specific guidelines. Since the TPA is not required to be licensed, it is exempt from the regulations.

_I am an independent agent. Recently a broker approached me to find coverage for a client of his, a trust that wants group health insurances for its employees. In this case, can I be classified as a service provider?_

No.

_Often, underwriting a specific policy can involve a sub-producer, general agent and an insurer in the placement of a risk. Do all these parties need to provide privacy notices?_

In such a case, the agent exception rule in the definition of ‘licensee’ is applicable to identify the party responsible for issues policy and opt-out notices.

_Will a licensee be considered as agent, employee, or representative of another licensee? Who issues the privacy notices?_

It all depends on the service being provided by the first licensee in the role of an agent, employee, or representative of the second licensee. In general, the agent exemption rule in the ‘licensee’ definition does hold true, but a case-to-case determination will be advisable.

_Is it permitted for a licensee to share health data with an affiliate in cases where both the parties are working on same claim?_

Of course. This is limited to health data required strictly for processing the claim, though.

_I am an independent agent offering health insurance in several states. In one state, I can across a situation where insurers were withholding certain claim information from hospitals. They claimed that such a disclosure was prohibited under new regulation. Are they correct?_

It all depends on the reason why a hospital may request the information. It is good policy to get authorization from your clients to forestall any complication.

_This query is in regard to HHS privacy regulation. If a licensee complies with HHS regulations, is it no longer subject to state regulations?_

In cases where a licensee is obligated to comply with HHS privacy regulation, it is under the jurisdiction of both the state and HSE. In cases where the licensee may be complying with HSE regulation even though it is not obligated to, the state has clear jurisdiction.

_I deal with affinity plans. Am I permitted to disclose account numbers used by the companies in an affinity plan?_

Yes, you are.

_Is it permitted for a company to share nonpublic personal financial data for the purpose of risk management? What about policyholder service functions?_

The answer lies in the details provided in the company’s privacy policy. If the nature of information and reason for disclosure is clearly communicated to the customer, then such a disclosure would be permissible. In any
case, risk management and loss control are covered by general servicing and processing exceptions.

I recently received nonpublic personal data from another body. What, if any, are my obligations under the privacy regulations?

Your main obligation is protect the confidentiality of the information. You may use or share the information only with the entity that provided you with the data, or affiliates of that entity.

Banks and securities firms share certain types of private information with me. Since they are already governed by privacy regulations, do I also need to follow any rules?

You must follow the regulations related to reuse and re-disclosure of confidential information. This means you can only share the information with the bank or securities firm that provided you with the information.

If a policyholder is cooperative and allows me to share nonpublic private information, am I permitted to charge him a lower premium rate?

Never. The regulations do not allow determination of premium rates based on the customer’s choice regarding disclosure of private information. This could be construed as discriminating against customers who may not want to agree to disclosure. However, there are several discounts that are permitted for other reasons. Who the company offers the discounts to is completely their choice.

What does a typical privacy notice look like?

Below are two indicative samples – these should be reviewed by an expert prior to use. The notice must be written in easy-to-understand language, provide clear information about the information being collected from your client, how it may be used and disclosed or shared, and also include information on how the client can opt-out.
Sample Disclosure #1

Purpose of This Notice
As provided by law, we are generally prohibited from sharing nonpublic personal data 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 data 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 data 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 data, 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 data 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 data relating to your character, personal habits, mode of living or general reputation

Right to access and amend your personal data:

You have the right to request access to the personal data 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 data 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 data. 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 data 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 within the requirements of these laws. We may disclose the following kinds of nonpublic personal data 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 data 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 data.

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 data 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 data 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 organizations 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 organizations 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 data 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
Assessment - Chapter 6

1) Who is a licensee? (Page 1, paragraph 7)
   a) An individual who purchases a policy on behalf of another
   b) Entities that provide marketing services for a specific insurer
   c) Entities regulated by the Department of Insurance
   d) An individual who has access to nonpublic private information

2) In which of the following circumstances is an agent not covered by the disclosure exemption and has to provide privacy policy and opt-out notices? (Pages 7 & 8, last and first paragraphs)
   a) Customer information is shared with a non-affiliated third party
   b) The agent’s company shares the information with a service provider
   c) The agent’s company provides privacy and opt-out information
   d) Consumer information is shared with an affiliated third party

3) Under the new privacy regulation, how are HMOs classified? (Pages 11 & 12, last and first paragraphs)
   a) Personal umbrella policy provider
   b) Group policy insurer
   c) Personal liability cover provider
   d) Self-funded trust