



PAYCHEX[®] HR SERVICES CLIENT SEMINAR

Information for Managers and Supervisors

Health Insurance Portability and Accountability Act (HIPAA)

PAYCHEX[®]

TABLE OF CONTENTS

Objectives.....	3
Overview of the Health Insurance Portability Act (HIPAA)	4
HIPAA Title I.....	6
HIPAA Title II.....	10
Administrative Simplification Rules	13
Privacy Rule	17
The Security Rule.....	19
HIPAA Enforcement and Outreach.....	22
Summary	26
Additional Resources.....	27
Review Activity.....	28
Glossary.....	31

Professional Employer Organization (PEO) Services are sold and provided by Paychex Business Solutions, LLC and its affiliates.

The information in these materials, and that provided by the presenter, should not be considered legal or accounting advice, and it should not substitute for legal, accounting, and other professional advice where the facts and circumstances warrant. It is provided for informational purposes only.

If you require legal or accounting advice, or need other professional assistance, you should always consult your attorney, accountant, or other professional advisor to discuss your particular facts, circumstances, and business needs.

©2017 Paychex, Inc. All rights reserved.

#159971

OBJECTIVES

This seminar describes the laws and provisions of the Health Insurance Portability and Accountability Act (HIPAA), providing you with information and resources you can use to determine how HIPAA affects your business. You are encouraged to seek legal counsel for additional information and support.


During this seminar, we will:

- identify what the Health Insurance Portability and Accountability Act (HIPAA) is and how it protects workers and their dependents
- identify the purpose of Title I and Title II under HIPAA
- discuss the Administrative Simplification Rules in detail
- discuss the Privacy and Security Rules in detail
- discuss HIPAA enforcement
- examine the complaint process, and
- explore available resources to explain HIPAA and address major aspects of the rule.

Learning Objectives

During this seminar, you will:

- identify what the Health Insurance Portability and Accountability Act (HIPAA) is and how it protects workers and their dependents
- identify the purpose of Title I and Title II under HIPAA
- discuss the Administrative Simplification Rules in detail
- discuss the Privacy and Security Rules in detail
- discuss HIPAA enforcement
- examine the complaint process, and
- explore available resources to explain HIPAA and address major aspects of the rule.



Notes:

OVERVIEW OF THE HEALTH INSURANCE PORTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law that was enacted in 1996 to help protect millions of American workers by ensuring health coverage for those who change or lose their jobs and privacy for all individuals.

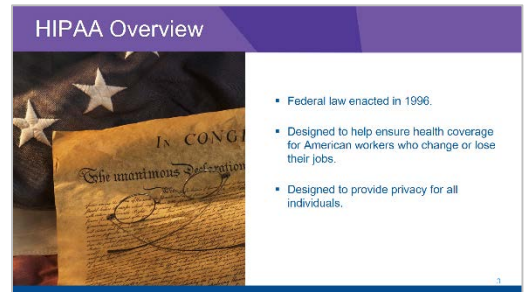
The need for privacy was realized as more and more health information was being recorded and exchanged electronically. Before HIPAA, there were very few laws in place to help ensure a patient's privacy when their medical records were stored on a computer, rather than in the once-standard paper charts.

HIPAA has two main sections:

- **Title I** – works with group and individual health insurance plans to ensure coverage for workers and their families when they change or lose their jobs.
- **Title II** – requires national standards for electronic healthcare transactions, and addresses the security and privacy of electronic medical records.

HIPAA protects workers and their dependent family members by:

- providing individuals additional opportunities to enroll in group health plans if they lose other coverage or experience certain life events
- ensuring that employers do not exclude new employees with pre-existing medical conditions from plan coverage
- prohibiting discrimination in enrollment and in premiums charged to employees and their dependents based on health status-related factors, including, but not limited to, previous medical conditions, previous insurance claims, or genetic information
- ensuring that certain individuals have access to individual health insurance policies
- requiring national standards for electronic healthcare transactions, and
- preserving the states' role in regulating health insurance, including the states' authority to provide greater protections than those available under federal law.



HIPAA Overview

- Federal law enacted in 1996.
- Designed to help ensure health coverage for American workers who change or lose their jobs.
- Designed to provide privacy for all individuals.

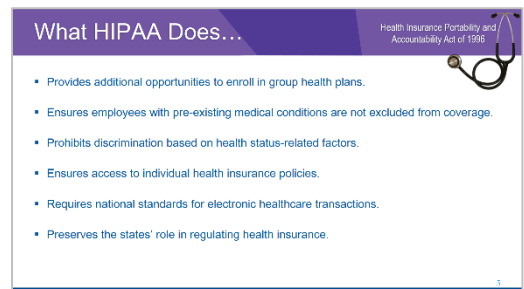
3



HIPAA's Two Main Sections

- **Title I** ensures health insurance coverage for workers who change or lose their jobs.
- **Title II** addresses national standards for healthcare transactions and the security and privacy of electronic medical records.

4



What HIPAA Does...

Health Insurance Portability and Accountability Act of 1996

- Provides additional opportunities to enroll in group health plans.
- Ensures employees with pre-existing medical conditions are not excluded from coverage.
- Prohibits discrimination based on health status-related factors.
- Ensures access to individual health insurance policies.
- Requires national standards for electronic healthcare transactions.
- Preserves the states' role in regulating health insurance.

5

Notes:

OVERVIEW OF THE HEALTH INSURANCE PORTABILITY ACT (HIPAA) – CONT.

Although HIPAA adds protections and makes it easier to switch jobs without fear of losing health coverage, the law has limitations. For example, HIPAA **does not**:

- require employers to offer or pay for health insurance coverage
- guarantee that all those in the workforce will get health coverage
- control how much an insurance company can charge for group coverage
- force group health plans to offer specific benefits
- allow individuals to keep the exact same health insurance plan they had at a previous job when going to a new job
- guarantee that any conditions an individual has (or has had in the past) are covered by the new employer's health plan, and
- prohibit an employer from imposing a pre-existing condition exclusion period if an individual has been treated for a condition during the past 6 months.

This list is not all inclusive. For more information, refer to the Health and Human Services (HHS) website at www.hhs.gov.

Notes:

HIPAA TITLE I

Title I under HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. HIPAA ensures that a group health plan cannot deny coverage or establish the amount of your monthly premium based on your health status, which includes your medical history, genetic information, or any disability you may have.

Secondly, Title I establishes rules on how a group plan handles *pre-existing conditions*. In the past, some employers' group health plans limited, or even denied, coverage if a new employee had such a condition before enrolling in the plan. People were completely denied health insurance based on chronic medical conditions, regardless of how well the condition was being controlled. Under HIPAA, that is not allowed.

Today, group health insurance plans must follow rules regarding what's considered a pre-existing condition and how long they can exclude coverage for these conditions. Because of the increased financial risk to the insurer, the list of pre-existing conditions can be long.

PRE-EXISTING CONDITIONS

Simply defined, a pre-existing condition is a health condition or illness that you have had before your first day of coverage on a new plan. This rather broad definition is just a small piece of the puzzle, and the actual health coverage for those with pre-existing conditions depends on a few factors, including:

- the type of health insurance plan
- the level of care needed for your pre-existing condition, and
- your health insurance history.

Because someone with a pre-existing condition could cost an insurance company millions, it would be in their best interest to exclude those who have them – but it's not that simple. The concept of excluding pre-existing conditions makes sense if you were talking about auto insurance. For example, if your windshield was cracked before you bought your coverage, you can't expect your new auto insurer to replace it after you buy a policy. But when it comes to someone's health, the idea of exclusion might be less clear cut.

HIPAA Title I

- Protects health insurance coverage for workers when they change or lose their jobs.
- Establishes rules on how group plans handle pre-existing conditions.

A group of diverse business professionals in a meeting, looking towards the right.

Pre-Existing Conditions

...a health condition or illness that you had before your first day of coverage on a new plan.

A woman in profile, holding her neck, suggesting a health condition.

Notes:

PRE-EXISTING CONDITION EXCLUSION

Now that we've defined pre-existing conditions, you may be wondering how a pre-existing condition could affect health care coverage. There really is no simple answer.

Some conditions will not affect coverage at all, but others could keep an individual from having coverage for a specific condition for up to a year. When an insurance company applies a *pre-existing condition exclusion*, it can limit or exclude coverage for that condition.

Under HIPAA, an insurer is only allowed to look back six months for a condition that was present before the start of coverage in a group health plan. Specifically, the law says that a pre-existing condition exclusion can be imposed on a condition only if medical advice, diagnosis, care, or treatment was recommended or received during the six months before the enrollment date in the plan.

For example, an individual may have had arthritis for many years before coming to his current job. If he didn't have medical advice, diagnosis, care, or treatment – recommended or received – in the six months before enrolling in the plan, then that condition cannot be subject to a pre-existing condition exclusion. If he did receive medical advice, diagnosis, care, or treatment within the past six months, then the plan may impose a pre-existing condition exclusion for arthritis. If he did receive medical advice, diagnosis, care, or treatment within the past six months, then, under HIPAA, the plan may impose a pre-existing condition exclusion for arthritis.

LIMITATIONS

The limitations HIPAA placed on the pre-existing condition exclusion help ensure that those with pre-existing conditions can get health care. So, although an individual might have to live with a pre-existing condition exclusion period, he can't be denied coverage in a group plan because of his health. In addition, he cannot be charged higher premiums than a co-worker who may be in perfect health.

Notes:

CREDITABLE COVERAGE

Because 12 months is a substantial amount of time to wait for medical coverage, HIPAA uses what is known as *creditable coverage* to reduce, or eliminate, a pre-existing condition exclusion period. If an individual can prove that he had uninterrupted health insurance before the current plan, that coverage can be counted toward any pre-existing condition exclusion he may have.

In fact, if he had at least one year of group health insurance at one job and then received health insurance at a new job without a break of more than 63 days, the new health insurance plan cannot impose a pre-existing condition exclusion on him at all.



The waiting period imposed by a new employer's plan may not be counted toward a break in coverage.

However, if there was a break in coverage greater than 63 days, or if he doesn't have creditable coverage behind him when enrolling in a new group plan, none of the health insurance coverage he had is counted toward his pre-existing condition exclusion period.

Most United States health coverage is creditable. However, if you had coverage from an overseas health insurer, your new health insurer can refuse to pay for any of your existing medical conditions (except pregnancy, if the plan has maternity coverage), but only for a maximum of 12 months, or 18 months for those who don't enroll during the general open enrollment period.



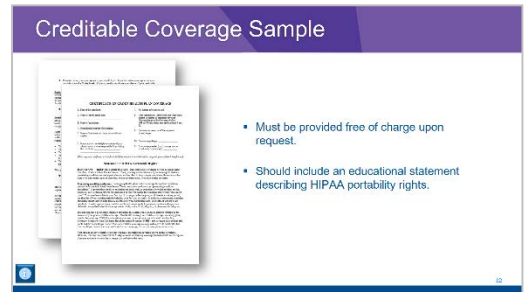
Notes:

CERTIFICATE OF CREDITABLE COVERAGE

A Certificate of Creditable Coverage must be provided free of charge upon request while the employee has health coverage or anytime within 24 months after coverage ends.

- Among other things, the certificate should contain information about coverage dates, policy identification number, the issuer's name and address, dependents, the length of time an individual or his dependents had coverage, as well as the length of any waiting period for coverage that applied. It should also include an educational statement that describes individuals' HIPAA portability rights.

If a certificate is not received after being requested, or the information on the certificate is incorrect, the individual should contact the prior plan issuer. If he cannot get a certificate, he has the right to show prior creditable coverage with other evidence, such as pay stubs, explanation of benefits, or letters from a doctor.



Notes:

HIPAA TITLE II

As most of us living in today's high-tech world have noticed, the use of technology permeates the healthcare system. On a recent visit to a healthcare provider, you may have seen computers used to access medical information, rather than using the traditional wall of file folders. Although electronic filing systems are generally efficient, they could pose a threat to patient privacy. HIPAA ensures privacy while allowing electronic access to protected health information.

Title II under HIPAA requires national standards for electronic healthcare transactions to be established, along with national identifiers for providers, health insurance plans, and employers. Although Title II lists health care system rules and penalties, it is known for its *Administrative Simplification Rules*. These rules are used to help make the exchange of electronic health information safe and efficient throughout the nation's healthcare system.

ADMINISTRATIVE SIMPLIFICATION RULES

The *Administrative Simplification* provisions of HIPAA required the U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions, unique health identifiers, and security. At the same time, Congress recognized that advances in technology could erode the privacy of health information, and therefore, incorporated HIPAA provisions that mandated the adoption of federal privacy protections for individually identifiable health information.

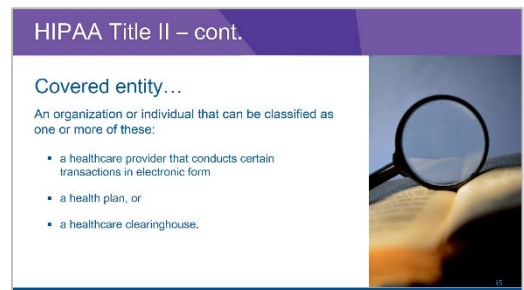
We'll take a closer look at these rules a little later in this seminar.

COVERED ENTITY

The Administrative Simplification Rules adopted by HHS apply to any entity that is:

- a healthcare provider that conducts certain transactions in electronic form
- a health plan, or
- a healthcare clearinghouse.

An organization or individual that can be classified as one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations, and must comply with those regulations.



Notes:

ARE YOU A COVERED ENTITY?

To determine if a person, business, or government agency is a covered entity, there is a tool posted on the Centers for Medicare and Medicaid Services (CMS) website:

<https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf>

Answer the appropriate questions that apply to the person, business, or agency. If you are uncertain about which chart to use, answer all of the questions.

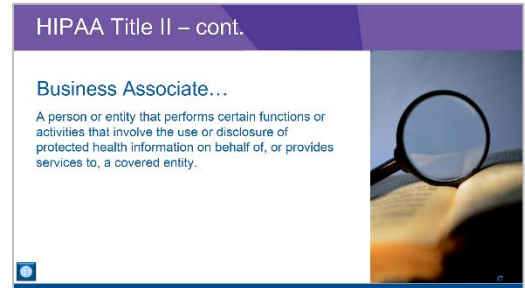
BUSINESS ASSOCIATE

A *business associate* is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not considered a business associate.

A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as those particular services that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information.

The types of functions or activities that may make a person or entity a business associate include payment for health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions/activities:	Business associate services:
<ul style="list-style-type: none"> • claims processing • claims administration • data analysis • utilization review • quality assurance • billing • benefit management • practice management, and • re-pricing. 	<ul style="list-style-type: none"> • legal • actuarial • accounting • consulting • data aggregation • management • administrative • accreditation, and • financial.



Notes:

BUSINESS ASSOCIATE – CONT.

Examples of a business associate might include:

- A third-party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a healthcare provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearing house that translates a claim from a non-standard format into a standard transaction on behalf of a healthcare provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

Business associates of covered entities are responsible for compliance with the HIPAA Privacy and Security Rules' requirements related to PHI and the activities and functions they perform.

Notes:

ADMINISTRATIVE SIMPLIFICATION RULES

STANDARDS FOR ELECTRONIC TRANSACTIONS

The first section of the Administrative Simplification Rules involves implementing national standards for electronic healthcare transactions, including:

- plan enrollment
- health claims
- eligibility determination
- claim status verification, and
- care and premium payments.

While these transactions may be available on some healthcare systems, HIPAA intends for all transactions to be processed using the same electronic format so that your protected health information can be shared, when you request it to be, with providers across the country.

STANDARDS FOR UNIQUE HEALTH IDENTIFIERS

Next, there are the standards for Unique Health Identifiers. This requires a *national provider identifier*, or NPI, for all healthcare providers that transmit health information in electronic form.

This NPI is a 10-digit number used by HIPAA covered entities (e.g., health plans, health care clearinghouses and some health care providers) to identify health care providers in HIPAA standard transactions. This requirement is intended to improve the efficiency and effectiveness of electronic transmission of health information.

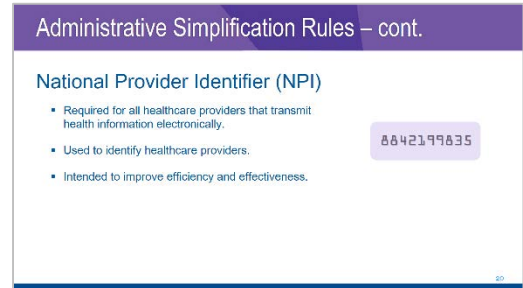


Administrative Simplification Rules

National standards for electronic healthcare transactions...

- plan enrollment
- health claims
- eligibility determination
- claim status verification
- care and premium payments

49



Administrative Simplification Rules – cont.

National Provider Identifier (NPI)

- Required for all healthcare providers that transmit health information electronically.
- Used to identify healthcare providers.
- Intended to improve efficiency and effectiveness.

8842199835

50

Notes:

PRIVACY RULE

The Privacy Rule establishes minimum federal standards for safeguarding the privacy of individually identifiable health information, also known as Protected Health Information, or PHI.

PROTECTED HEALTH INFORMATION

PHI is information about health status, provision of health care, or payment for health care – whether oral or recorded in any form or medium – that can be linked to a specific individual. This includes information that relates to:

- the individual's past, present, or future physical or mental health or condition
- the provision of health care to the individual
- the past, present, or future payment for the provision of health care to the individual, and
- that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Examples of PHI include many common identifiers (e.g. name, address, date of birth, social security number) along with: diagnoses (for yourself, family members, or friends), medications, names of doctors, dates of treatment, etc.

Unlike other sections of Title II, the Privacy Rule applies to protected health information in any form, be it paper, electronic, or oral communication. When people in the medical field mention HIPAA, the Privacy Rule is generally what they're referring to.

Administrative Simplification Rules – cont.

Privacy Rule...
Establishes minimum federal standards for safeguarding the privacy of individually identifiable health information.



Administrative Simplification Rules – cont.

Protected Health Information (PHI)...
Information about health status, provision of health care or payment of health care that can be linked to a specific individual.



Notes:

SECURITY RULE

The Security Rule establishes national standards to protect individuals' protected health information that is created, received, maintained or transmitted in an electronic form by a covered entity. It is intended to protect the confidentiality, integrity, and availability of electronic protected health information.

ELECTRONIC PROTECTED HEALTH INFORMATION

Electronic protected health information refers to any protected health information that is covered under HIPAA's Privacy Rule that is created, received, maintained or transmitted in an electronic format.

There are different types of electronic protected health information, including information in a patient's medical record at a doctor's office, documentation of conversations a doctor may have had with others about a patient's care or treatment, patient information in a health insurer's computer system, or patient billing information, among others. In addition, any past medical records or payment information is subject to the same degree of privacy protection.

Regardless of the type of electronic device -- PC, tablet, or smartphone -- used to access electronic protected health information, users must abide by HIPAA Security Rule guidelines when handling both information at rest and that which is being transferred electronically, via email, or file transfer.

The Security Rule involves safeguards used with each individual's electronic protected health information. Basically, it deals with the various security standards each provider should follow to ensure the highest level of confidentiality of all the electronic protected health information that he creates, receives, maintains or transmits. It requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. In addition, providers are expected to protect their entire system from any threats to its security, such as computer hackers or even indiscreet office personnel.

Administrative Simplification Rules – cont.

Security Rule...

- Establishes national standards to protect individuals' protected health information.
- Intended to protect the confidentiality, integrity, and availability of electronic protected health information.



Administrative Simplification Rules – cont.

Electronic Protected Health Information...

Refers to any protected health information that is covered under HIPAA's Privacy Rule that is created, received, maintained, or transmitted electronically.



Notes:

ENFORCEMENT RULE

The Enforcement Rule, also part of HIPAA's Administrative Simplification Rules, became effective in March 2006. This rule involves compliance, procedures for hearings, and the imposition of civil monetary penalties against those who violate any of the Administrative Simplification Rules.

Before the Enforcement Rule came into effect, these civil penalties were only applied to those who were non-compliant with the Privacy Rule. Now, violators of any rule in the Administrative Simplification process can be punished. This rule also details how an investigation should take place, how the penalty is determined, and how to appeal a ruling.

Administrative Simplification Rules – cont.

Enforcement Rule...

Involves compliance, procedures for hearings, and the imposition of civil monetary penalties against those who violate any of the Administrative Simplification Rules.



Notes:

PRIVACY RULE

The provisions of the Privacy Rule apply to health plans, healthcare clearinghouses, and health care providers that conduct certain health care transactions electronically. The Privacy Rule protects all protected health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

The Rule requires appropriate safeguards to protect the privacy of protected health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. In addition, the amount of protected health information that is shared is kept to the minimal amount needed for treatment or business operations.

Because of the importance of the Privacy Rule, comprehensive compliance requirements are involved for both employees and patients of any healthcare facility. If you aren't in healthcare, you might have been exposed to this rule when a healthcare provider asked you to sign a HIPAA release form. This form is used to prove that you've been advised of your healthcare provider's privacy practices with regards to your protected health information.

PATIENT RIGHTS

Under the Privacy Rule, (*individuals*) patients have the following rights:


- *Access to Medical Records* – Patients generally should be able to see and obtain copies of their medical records and request corrections. Patients may be charged for the cost of reproducing and mailing the records.
- *Notice of Privacy Practices* – Patients must be notified regarding the use of personal medical information and patient rights under the Privacy Rule. Patients should be asked to sign, initial, or otherwise acknowledge the receipt of the notice.
- *Limits on Use of Personal Medical Information* – To encourage the best quality care, the Privacy Rule does not restrict doctors, nurses, and other providers from sharing information needed to treat their patients. Protected health information may only be shared for purposes related to healthcare.
- *Prohibition on Marketing* – The Privacy Rule restricts and limits the use of patient information for marketing purposes. Covered entities must get an individual's specific authorization before disclosing patient information for marketing purposes.

The Privacy Rule

Electronic



Paper



Verbal



Protects all protected health information held or transmitted by a covered entity or its business associate, in any form or media.

- Protects the privacy of protected health information
- Sets limits and conditions on uses and disclosures
- Minimizes the amount of protected health information that can be shared

The Privacy Rule – cont.

Patient Rights...

- Access to medical records
- Notice of privacy practices
- Limits on use of personal medical information
- Prohibition on marketing
- Confidential communications



Notes:

PATIENT RIGHTS – CONT.

- *Confidential communications* – Under the Privacy Rule, patients can request that their doctors, health plans, and other covered entities take reasonable steps to ensure that their communications with the patient are confidential.

Consumers may file a formal complaint regarding the privacy practices of a covered health plan or provider. Such complaints can be made directly to the covered provider or health plan or to The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR).

In addition to protecting patient privacy, covered entities are responsible for:

- *Written Privacy Procedures* – Covered entities are required to have written privacy procedures, including a list of staff that can access protected health information, how the information will be used, and when it may be disclosed. Covered entities generally must ensure that any business associates who have access to protected health information agree to the same limitations on the use and disclosure of that information.
- *Employee Training* – Covered entities must train their employees in their privacy procedures, designating an individual to ensure the procedures are followed. If a covered entity learns that an employee failed to follow privacy procedures, they must take appropriate disciplinary action.
- *Public Responsibilities* – There are limited circumstances, in which the Privacy Rule permits – but does not require – covered entities to continue certain disclosures of health information for specific public responsibilities. The Privacy Rule generally establishes new safeguards and limits on these disclosures. Where no other law requires disclosures in these situations, covered entities may continue to use their professional judgment to decide whether to make such disclosures based on their own policies and ethical principles.

Notes:

THE SECURITY RULE

The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must implement to secure individuals' electronic protected health information (ePHI).

Before HIPAA, there were no generally accepted security standards or general requirements for protecting health information. At the same time, new technologies were emerging, and the healthcare industry began to move away from paper processes, relying more on the use of electronic information systems to pay claims, answer eligibility questions, share health information, and other administrative functions. Today, providers are using applications such as computerized physician order entry systems, electronic health records, and radiology, pharmacy, and laboratory systems.

Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient, the increase in adoption rates of these technologies increases the potential security risks.

Although the main purpose of the Security Rule is to protect the privacy of individuals' health information, it is also designed to allow covered entities to adopt new technologies that improve the quality and efficiency of patient care. The Security Rule is designed to be flexible so a covered entity can implement policies, procedures, and technologies that are appropriate for his particular size, organizational structure, and risks to his patients' electronic protected health information.

GENERAL RULES

The Security Rule requires covered entities to maintain reasonable and appropriate *administrative*, *physical*, and *technical safeguards* for protecting electronic protected health information.

Specifically, covered entities must:

- ensure the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted
- identify and protect against reasonably anticipated threats to the security or integrity of the information
- protect against reasonably anticipated, impermissible uses or disclosures, and
- ensure compliance.

The Security Rule

Addresses the technical and non-technical safeguards to secure electronic protected health information.



The Security Rule – cont.

General Rules...

Maintain reasonable and appropriate safeguards for protecting electronic protected health information.

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Notes:

GENERAL RULES – CONT.

Under the Security Rule, electronic protected health information must not be made available or disclosed to any unauthorized persons. The confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of protected health information.

In addition, the Security Rule promotes maintaining the *integrity* and *availability* of electronic protected health information. This means that electronic protected health information cannot be altered or destroyed in an unauthorized manner, and the information must be accessible and usable on demand by an authorized person.

Covered entities must review and modify their security measures to continue protecting electronic protected health information in an ever-changing environment.

ADMINISTRATIVE SAFEGUARDS

Covered entities must:

- identify and analyze potential risks to electronic protected health information, and implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- designate a security official who is responsible for developing and implementing its security policies and procedures.
- implement policies and procedures for authorizing access to electronic protected health information when such access is based on the user or recipient's role.
- provide for appropriate authorization and supervision of workforce members who work with electronic protected health information.
- train all workforce members regarding security policies and procedures.
- have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

The Security Rule – cont.

General Rules...

Maintain reasonable and appropriate safeguards for protecting electronic protected health information.

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

The slide features a background of blurred code on the left and a central graphic of a padlock with a keyhole, symbolizing security.

Notes:

HIPAA ENFORCEMENT AND OUTREACH

The Health and Human Services' Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules.

OCR enforces the Privacy, Security and Breach Notification Rules in several ways, such as:

- investigating filed complaints
- conducting compliance audits to determine if covered entities are in compliance, and
- performing education and outreach to foster compliance with the Rules' requirements.
- Investigating reported breach incidents

OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

Enforcement of the Privacy Rule began in April 2003 for most HIPAA-covered entities. Since that time, OCR's enforcement activities have yielded significant results and have improved the privacy practices of covered entities. The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve.

HIPAA covered entities were required to comply with the Security Rule beginning in April 2005. OCR became responsible for enforcing the Security Rule in July 2009.

DEFINITION OF A BREACH

The HIPAA Breach Notification Rules, HITECH, requires HIPAA covered entities to provide notification following a breach of PHI. Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. Any breach that falls under this definition is subject to the HITECH breach notification rules.

If an exception to the definition of a breach does not apply, the only way for a covered entity to avoid having to provide notifications to affected individuals (and in certain circumstances HHS and the media) in the event of a breach is to perform a risk assessment demonstrating that there is a low probability that PHI was compromised. The assessment must be made based on the following four factors:

- The nature and extent of the PHI involved (including identifiers and the likelihood of re-identification)
- the unauthorized person who obtained the PHI
- whether the PHI was actually acquired or viewed
- the extent to which the risk has been mitigated.

HIPAA Enforcement and Outreach

HHS.gov
Office for Civil Rights

- Responsible for enforcing the Privacy, Security, and Breach Notification Rules.
- Works in conjunction with the Department of Justice.

Enforcement of Privacy Rule begins 2003 HIPAA covered entities required to comply with Security Rule 2005 OCR for enforcing responsible Security Rule 2009

HIPAA Enforcement and Outreach

Breach...

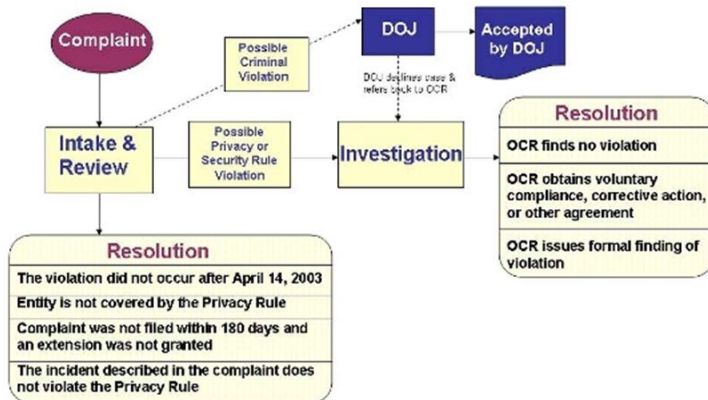
Generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information, such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Notes:

THE COMPLAINT PROCESS

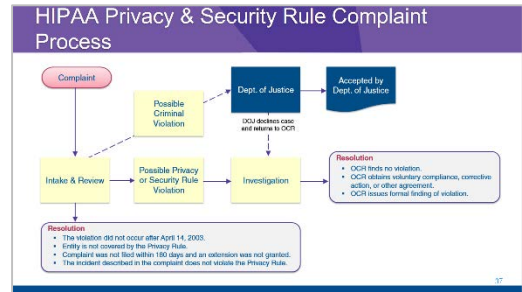
One of the ways that OCR carries out this responsibility is to investigate complaints filed with it. OCR may only take action on certain complaints. For more detailed information on the types of complaints, go to: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html>.

HIPAA Privacy & Security Rule Complaint Process



If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the covered entity named in the complaint. Then the complainant and the covered entity are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations.

For information on how complaints are filed, go to: <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>.



Notes:

OUTREACH AND EDUCATION

Led by the Office for Civil Rights, HHS has issued extensive guidance and technical assistance materials to make it as easy as possible for covered entities to comply with HIPAA requirements. Key elements of OCR's outreach and education efforts include:

- HHS has issued extensive guidance and technical materials to explain HIPAA, including an extensive, searchable collection of frequently asked questions that address major aspects of the rule. HHS will continue to expand and update these materials to further assist covered entities in complying.
- HHS has participated in hundreds of conferences, trade association meetings, and conference calls to explain and clarify the provisions of HIPAA. These included a series of regional conferences sponsored by HHS, as well as many held by professional associations and trade groups. HHS will continue these outreach efforts to encourage compliance with the privacy requirements.

To help covered entities find out information about the privacy regulation and other administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, OCR and HHS Centers for Medicare & Medicaid Services have established a toll-free information line: (866) 627-7748.



The slide features a purple header with the text "Outreach and Education". On the left, there is a blue box with the text "HHS.gov" and "Office for Civil Rights" below it. To the right of this box is a bulleted list of three items: "Extensive guidance and technical materials", "Extensive, searchable collection of frequently asked questions", and "Participation in hundreds of conferences, trade association meetings, and conference calls". Below the list is a fourth bullet point: "Toll-free information line". A small "08" is visible in the bottom right corner of the slide.


Notes:

SEEKING LEGAL COUNSEL

Seek legal counsel when:

- you need to determine your covered entity status
- you need your business practices analyzed to determine what to do to be in compliance with HIPAA, or
- you are named in a complaint.

Legal Counsel



Seek legal counsel:

- to determine your covered entity status
- to have your business practices analyzed, or
- if you are named in a complaint.

29

Notes:

SUMMARY

This seminar described the laws and provisions of the Health Insurance Portability and Accountability Act (HIPAA), providing you with information and resources you can use to determine how HIPAA may affect your business.

During this training, we:

- identified what the Health Insurance Portability and Accountability Act (HIPAA) is and how it protects workers and their dependents
- identified the purpose of Title I and Title II under HIPAA
- discussed the Administrative Simplification Rules in detail
- discussed the Privacy and Security Rules in detail
- discussed HIPAA enforcement
- examined the complaint process, and
- explored available resources to explain HIPAA and address major aspects of the rule.

You are encouraged to seek legal counsel for additional information and support.

Summary

During this training, you:

- identified what the Health Insurance Portability and Accountability Act (HIPAA) is and how it protects workers and their dependents
- identified the purpose of Title I and Title II
- discussed the Administrative Simplification Rules
- discussed the Privacy and Security Rules
- discussed HIPAA enforcement
- examined the complaint process, and
- explored available resources to explain HIPAA and address major aspects of the rule.

Notes:

ADDITIONAL RESOURCES

HIPAA FAQs

<http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>

NOTICE OF PRIVACY PRACTICES FAQs

http://www.hhs.gov/ocr/privacy/hipaa/faq/notice_of_privacy_practices/index.html

UNDERSTANDING HEALTH INFORMATION PRIVACY

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

BREACH INFORMATION

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

DISCLOSURES FOR WORKERS' COMPENSATION PURPOSES

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/workerscompensation.pdf>

HIPAA EMPLOYEE TRAINING

<https://www.hhs.gov/hipaa/for-professionals/training/index.html>

Notes:

REVIEW ACTIVITY

1. What is HIPAA?

2. Describe the two main sections of HIPAA.

3. List some of the issues HIPAA does not address.

4. What is a pre-existing condition?

5. Under HIPAA, how far can an insurer look back for a condition that was present before the start of coverage in a group health plan?

6. Under HIPAA, what is the maximum amount of time that an individual might have to wait to get coverage for a pre-existing condition?

Notes:

REVIEW ACTIVITY – CONT.

1. What is creditable coverage?

2. True or false: The waiting period imposed by a new employer's health plan can be counted toward a break in coverage.

3. What is a covered entity?

4. What is a healthcare clearinghouse?

5. What is a business associate?

6. List some functions or activities that may make a person or entity a business associate.

Notes:

REVIEW ACTIVITY – CONT.

7. What is a national provider identifier?

8. What is protected health information?

9. What rule establishes minimum federal standards for safeguarding the privacy of PHI?

10. What is electronic protected health information?

11. The Security Rule requires covered entities to maintain reasonable and appropriate _____, _____, and _____ safeguards for protecting individuals' EPHI.

12. What is a breach?

Notes:

GLOSSARY

ADMINISTRATIVE SIMPLIFICATION RULES

The *Administrative Simplification* provisions of HIPAA required the U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions, unique health identifiers, and security. At the same time, Congress recognized that advances in technology could erode the privacy of health information, and therefore, incorporated HIPAA provisions that mandated the adoption of federal privacy protections for individually identifiable health information.

BREACH

An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

BUSINESS ASSOCIATE

A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

COVERED ENTITY

Any entity that is a healthcare provider that conducts certain transactions in electronic form, a health plan, or a healthcare clearinghouse.

CREDITABLE COVERAGE

Uninterrupted health insurance before the current plan that can be counted toward any pre-existing condition exclusion waiting period. This means you can count any health insurance you had before your new insurance plan as long as it was uninterrupted for at least 63 days.

ELECTRONIC PROTECTED HEALTH INFORMATION

Any protected health information that is covered under HIPAA's security regulations and is created, received, maintained or transmitted in an electronic format.

GROUP HEALTH INSURANCE

Health insurance carried through an employer or other organization. Employers or other organizations can get better insurance rates because they have a large number of people to cover.

Notes:

GLOSSARY – CONT.

HEALTHCARE

Healthcare includes care, services, or supplies related to the health of an individual. Healthcare includes, but is not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body, and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

HEALTHCARE CLEARINGHOUSE

A public or private entity that performs either of the following:

- processes or facilitates the processing of health information received from another entity in a non-standard format or containing non-standard data content into standard data elements or a standard transaction, or
- receives a standard transaction from another entity and processes or facilitates the processing of health information into a non-standard format or non-standard data content for the receiving entity.

HEALTHCARE PROVIDER

Entities that transmit information in an electronic form, in connection with a transaction for which Health and Human Services has adopted a standard, including, but not limited to: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies.

HEALTH INFORMATION

Any information, whether oral or recorded in any form or medium, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and 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.

HEALTH PLAN

Entities including health insurance companies, HMOs, company health plans, and government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' healthcare programs.

Notes:

HIPAA

The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law that was enacted in 1996 to help protect millions of American workers by ensuring health coverage for those who change or lose their jobs and privacy for all individuals.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009 to promulgate regulations, developed by OCR, to require HIPAA covered entities to promptly notify affected individuals, and HHS and the media under certain circumstances, of a breach of PHI.

INDIVIDUAL HEALTH INSURANCE

A much more expensive health insurance option for people who don't have coverage, or don't have *enough* coverage through employers. Physical exams and questionnaires are usually a part of the application process, so poor health can really make a difference in the cost and eligibility.

NATIONAL PROVIDER IDENTIFIER

This NPI is a 10-digit number used by HIPAA covered entities (e.g. health plans, health care clearinghouses and some health care providers) to identify health care providers in HIPAA standard transactions. This requirement is intended to improve the efficiency and effectiveness of electronic transmission of health information.

PRE-EXISTING CONDITION

A health condition or illness that you have had before your first day of coverage on a new plan.

PRE-EXISTING CONDITION EXCLUSION

Some conditions could keep an individual from having coverage for a specific condition for up to a year. When an insurance company applies a *pre-existing condition exclusion*, it can limit or exclude coverage for that condition.

PROTECTED HEALTH INFORMATION

Information about health status, provision of health care, or payment for health care – whether oral or recorded in any form or medium – that can be linked to a specific individual.

Notes:

GLOSSARY – CONT.

TITLE I

Title I works with group and individual health insurance plans to ensure coverage for workers and their families when they change or lose their jobs.

TITLE II

Title II requires national standards for electronic healthcare transactions, and addresses the security and privacy of electronic medical records.

Notes:

NOTES:

