

Welcome to the Hard Hat Training Series!



BUY THE COMPLETE
PRESENTATION HERE

Welcome to the Hard Hat Training Series. Today, we will talk about the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a federal law established to provide the portability of health insurance and improve the protection of patients' medical records. Although it may be extensive, understanding HIPAA is critical in providing individuals with a healthcare structure they can trust. Through this training, we will strive to provide the tools and information that will allow you to increase your knowledge, and help you maintain a safe and productive workplace.



HARD HAT
TRAINING SERIES

SAFETY
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.



HIPAA AWARENESS
TRAINING

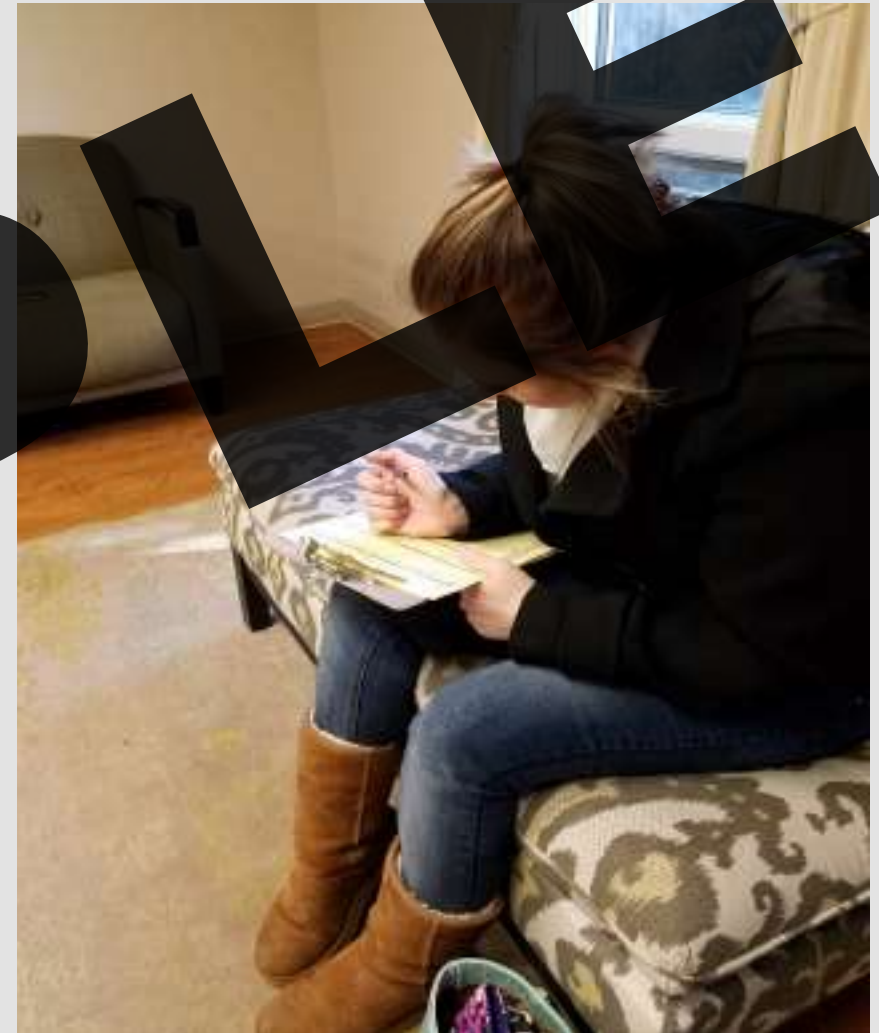
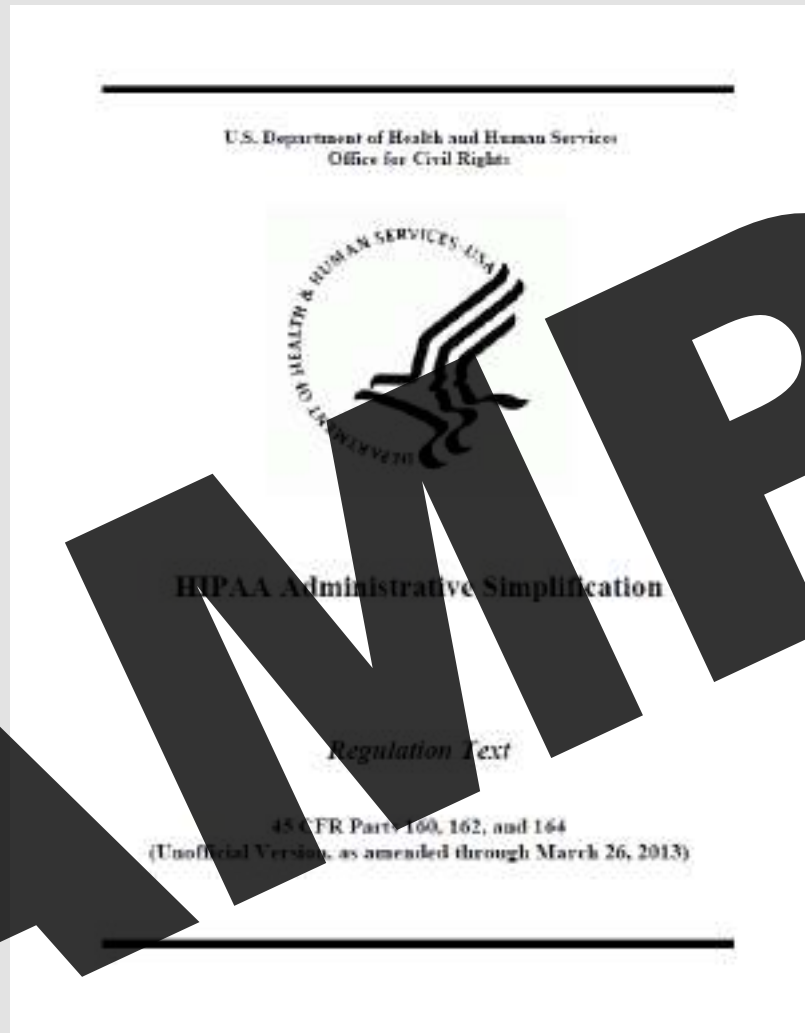


STANDARDS

- 45 C.F.R. Part 160: Privacy Rule (General Administration Requirements)
- 45 C.F.R. Part 162: Administration Requirements
- 45 C.F.R. Part 164: Security and Privacy Rules
- 45 C.F.R. Part 164.308 (a)(5) & 164.530 (b)(1): Training

Above is a list of areas you can find HIPAA standards and regulations. Be sure to reference these and all other Federal, State, and local laws as they may be more severe than the regulations established by HIPAA.

In this training, we will first take a look at the various legal regulations which lie within HIPAA. That will include a look into the portability of health insurance, the Privacy Rule, the Security Rule, and the Breach Notification Rule.





Recognizing the need for a more efficient medical industry and a secure way to store medical records, Congress agreed to lay the foundation for the proposal of a new federal law: HIPAA. This law sets detailed standards and regulations that protect medical information as it is stored, used, and disclosed.

In 1996, HIPAA was passed by the U.S. Congress, establishing standards and regulations with reference to the portability of health insurance plans (Title I). Although the law was passed, specific regulations were left out and were later addressed by Congress and the Secretary of Health and Human Services.

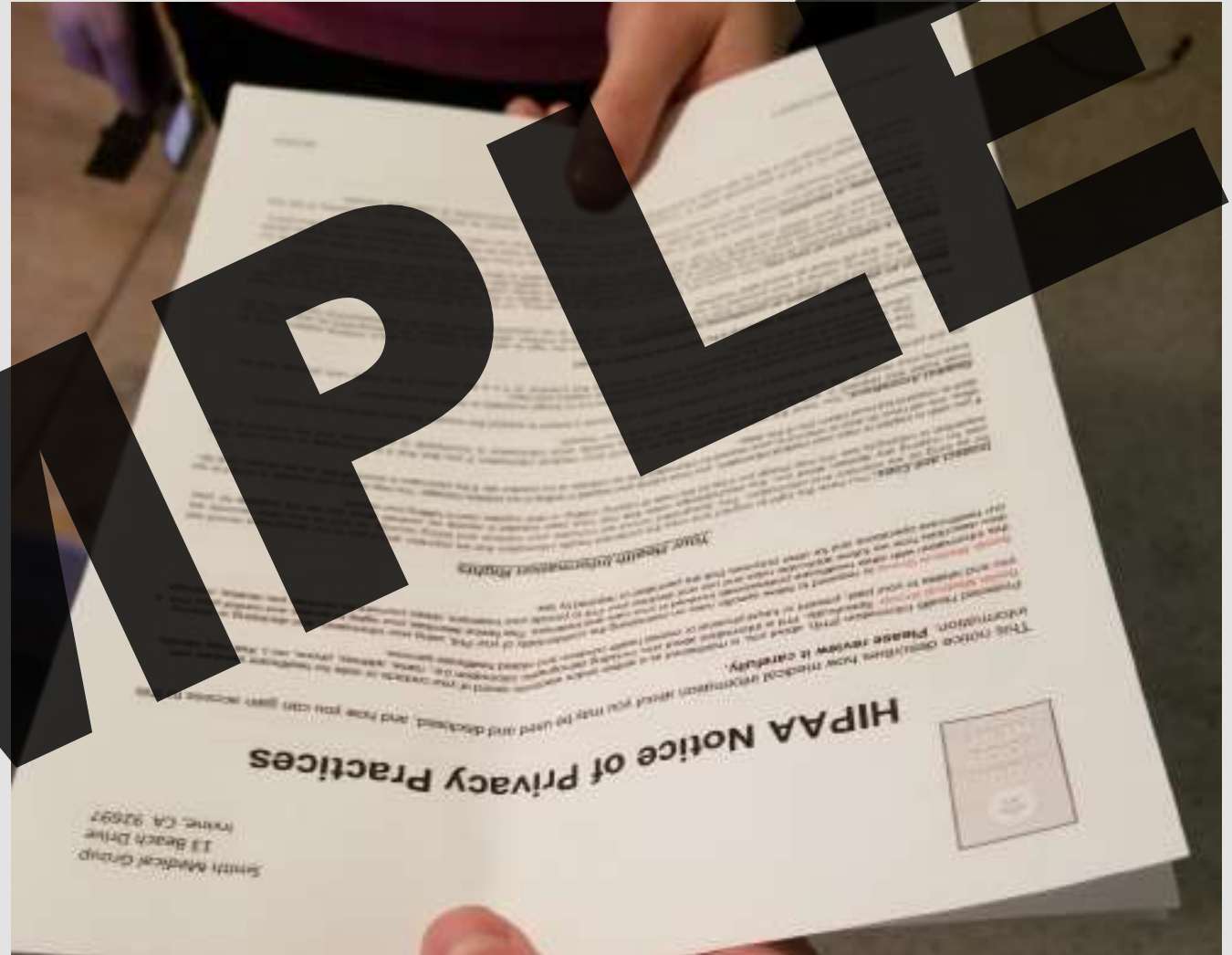


Since its initial installment, there have been many advancements within HIPAA in order to more effectively secure protected health information (PHI). Throughout this training, you will be able to gain a greater understanding of the various rules and regulations which have assisted in these advancements.



HIPAA

Health Insurance Portability
and Accountability Act



HARD HAT
TRAINING SERIES

SAFETY
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.



HIPAA AWARENESS
TRAINING



We will then learn about the details of who enforces HIPAA and how it is enforced if an organization does not comply with the regulations.



The most effective way to prevent HIPAA penalties is by consistently training your employees and documenting everything that involves the use or disclosure of PHI. Doing these two things can go a long way in protecting the information.



In 2017, four surveys were conducted by SecurityMetrics to analyze the various aspects of the rules within HIPAA. Over 300 healthcare professionals responded to the surveys, which uncovered the security habits within each organization. Among the different organizations, it was found that 26% of them do not have regular risk assessments, 16% send emails with unencrypted patient data, and only 34% train their staff on the Breach Notification Rule.



Below is a detailed chart containing the breach statistics of 2017 released by the HHS Office for Civil Rights. It shows the top ten breaches, which account for roughly 60% of all the patients affected by a breach that year. There were 297 total breaches reported to the HHS and over 4.5 million people were affected. It is important to note that only breaches affecting 500 patients or more must be reported to The Department of Health and Human Services.

Breach Report Results

Name of Covered Entity *	State *	Covered Entity Type *	Individuals Affected *	Breach Submission Date *	Type of Breach	Location of Breached Information
Commonwealth Health Corporation	KY	Healthcare Provider	897300	03/01/2017	Theft	Other
Airway Oxygen, Inc.	MI	Healthcare Provider	800005	06/16/2017	Hacking/IT Incident	Network Server
Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300000	07/15/2017	Hacking/IT Incident	Desktop Computer, Network Server
Urology Austin, PLLC	TX	Healthcare Provider	279883	03/22/2017	Hacking/IT Incident	Network Server
Pacific Alliance Medical Center	CA	Healthcare Provider	266123	08/10/2017	Hacking/IT Incident	Network Server
Peachtree Neurological Clinic, P.C.	GA	Healthcare Provider	176295	07/07/2017	Hacking/IT Incident	Network Server
Arkansas Oral & Facial Surgery Center	AR	Healthcare Provider	128000	09/24/2017	Hacking/IT Incident	Network Server
McLaren Medical Group, Mid-Michigan Physicians Imaging Center	MI	Healthcare Provider	106008	08/24/2017	Hacking/IT Incident	Network Server
Harrisburg Gastroenterology Ltd.	PA	Healthcare Provider	93323	04/28/2017	Hacking/IT Incident	Network Server
VisionQuest Eyecare	IN	Healthcare Provider	85995	03/02/2017	Hacking/IT Incident	Network Server





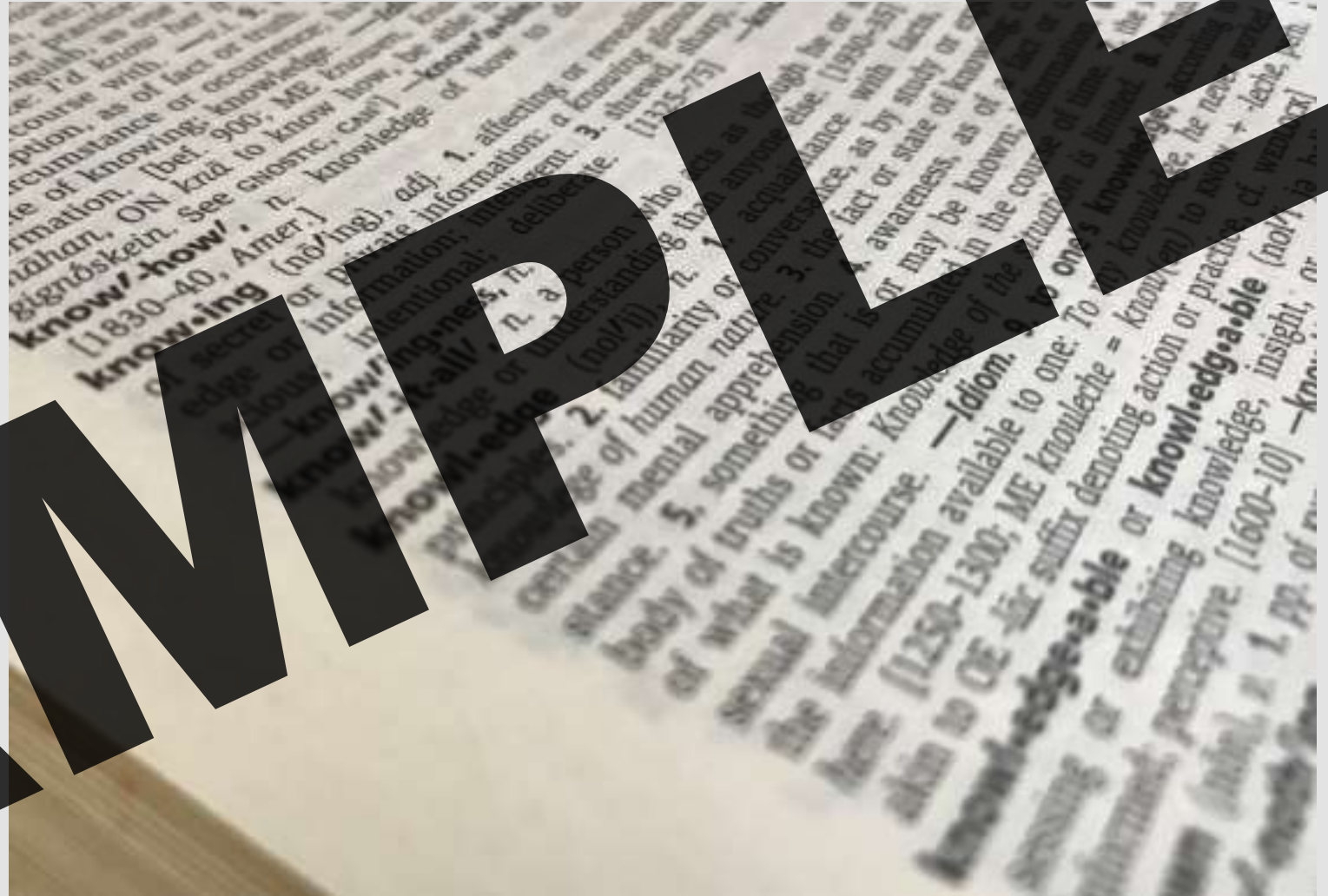
In an effort to stress the need for complete compliance to HIPAA and to decrease the number of PHI breaches, the U.S. Department of Health and Human Services (HHS) has established civil and criminal penalties. We will learn more about what the penalties are and when they are given to an organization later.

We will then conclude the training by going through a few case studies to apply what you have learned throughout the training. Remember, be thinking about your own workplace and in what ways it can improve its compliance with HIPAA.



Definitions

Before we progress any further, we will take a look at some key terms and acronyms that will be important for you to know and understand. Make sure that you take the time necessary to understand each before moving forward.



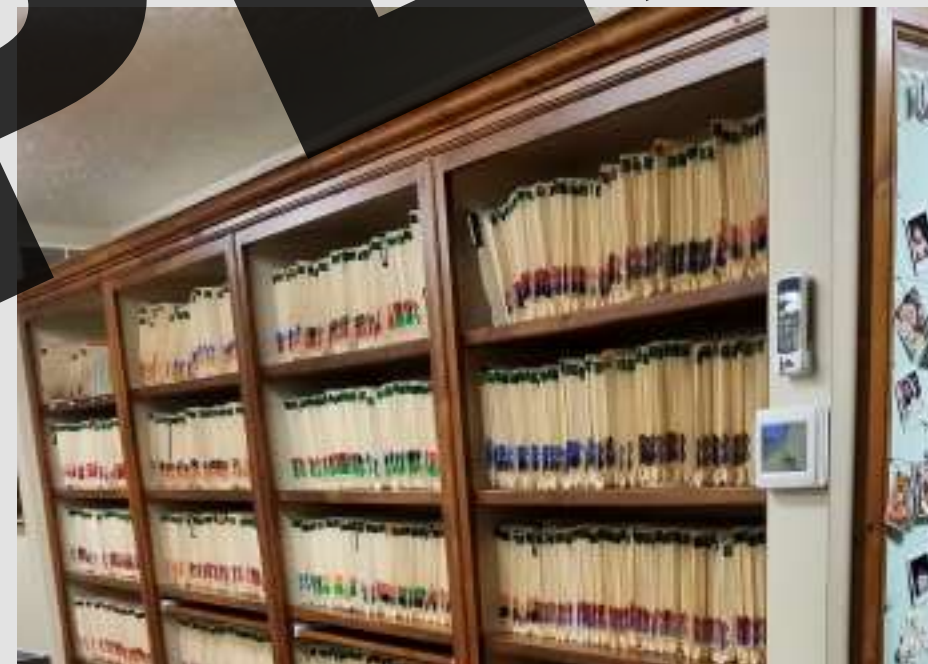


The United States Department of Health and Human Services (HHS) is a department of the U.S. federal government. Their responsibility is to provide essential human services along with protecting the health of all Americans. The HHS Office for Civil Rights (OCR) is the department responsible for the regulation and enforcement of HIPAA.





The **Privacy Rule** established national standards that were focused on assuring the security of protected health information (PHI). It also provides a smooth flow within the healthcare system when information needs to be transferred from one covered entity to another.



Protected health information (PHI) is defined under the Privacy Rule as any health-related information that can be linked back to a specific individual. This can include a variety of things such as medical bills, medical notes, conversations about the patient's condition or treatment, or any other personal information that is created, received, maintained or transmitted by a covered entity or business associate. PHI is not limited to any form or medium.



HIPAA De-identified Health Information Methods

Expert Determination

Apply statistical or scientific principles

Very small risk that anticipated recipient could identify individual with

Safe Harbor

Removal of 18 identifiers

No actual knowledge of residual information can identify individual

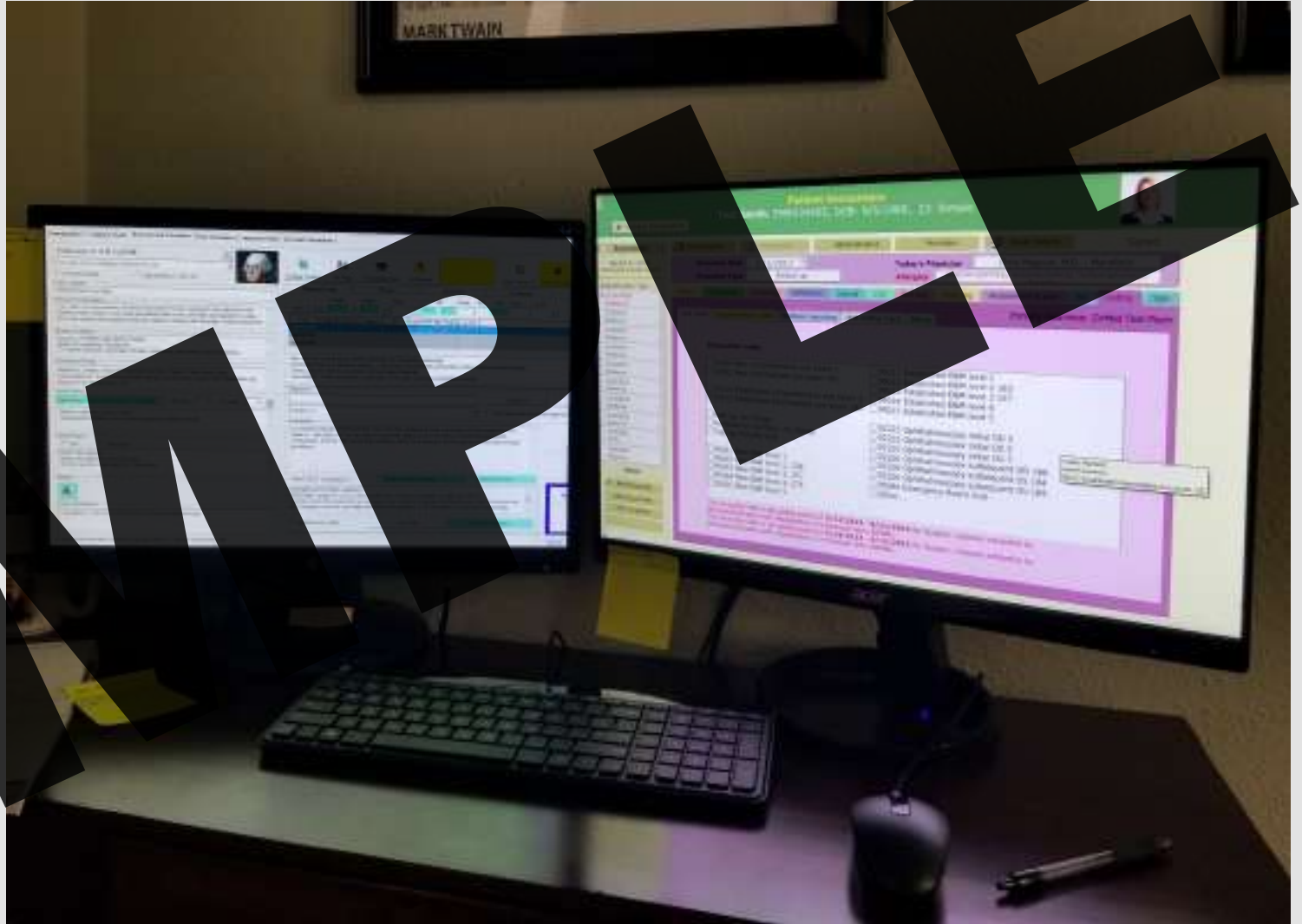
De-Identified health information does not provide any information that may reasonably be used to identify an individual. The use and disclosure of this information is not restricted. To the left are two methods that can be used to create de-identified information.



The **Security Rule** is essentially a subdivision of the Privacy Rule. Like the Privacy Rule, it sets national standards for the protection of personal health information. However, it does not apply to any other form of PHI apart from electronic PHI.



Electronic protected health information (e-PHI) is identical to PHI, however it strictly refers to the electronic form of all individually identifiable health information.



The **Breach Notification Rule** states that covered entities must inform the HHS and affected individuals of breaches that occur to any form of PHI. Depending on the extent of the breach, some cases require the covered entity to notify the media of the breach.



The **Health Information Technology for Economic and Clinical Health Act (HITECH)** was enacted as part of the American Recovery and Reinvestment Act of 2009. It was established to help incorporate electronic medical records (EHR), with the goal of providing better care for individuals while ensuring security for all medical information. This Act also led to changes within HIPAA with regards to the Privacy Rule, Security Rule, Breach Notification Rule, and the enforcement of HIPAA. These changes were included in the HIPAA Final Omnibus Rule.

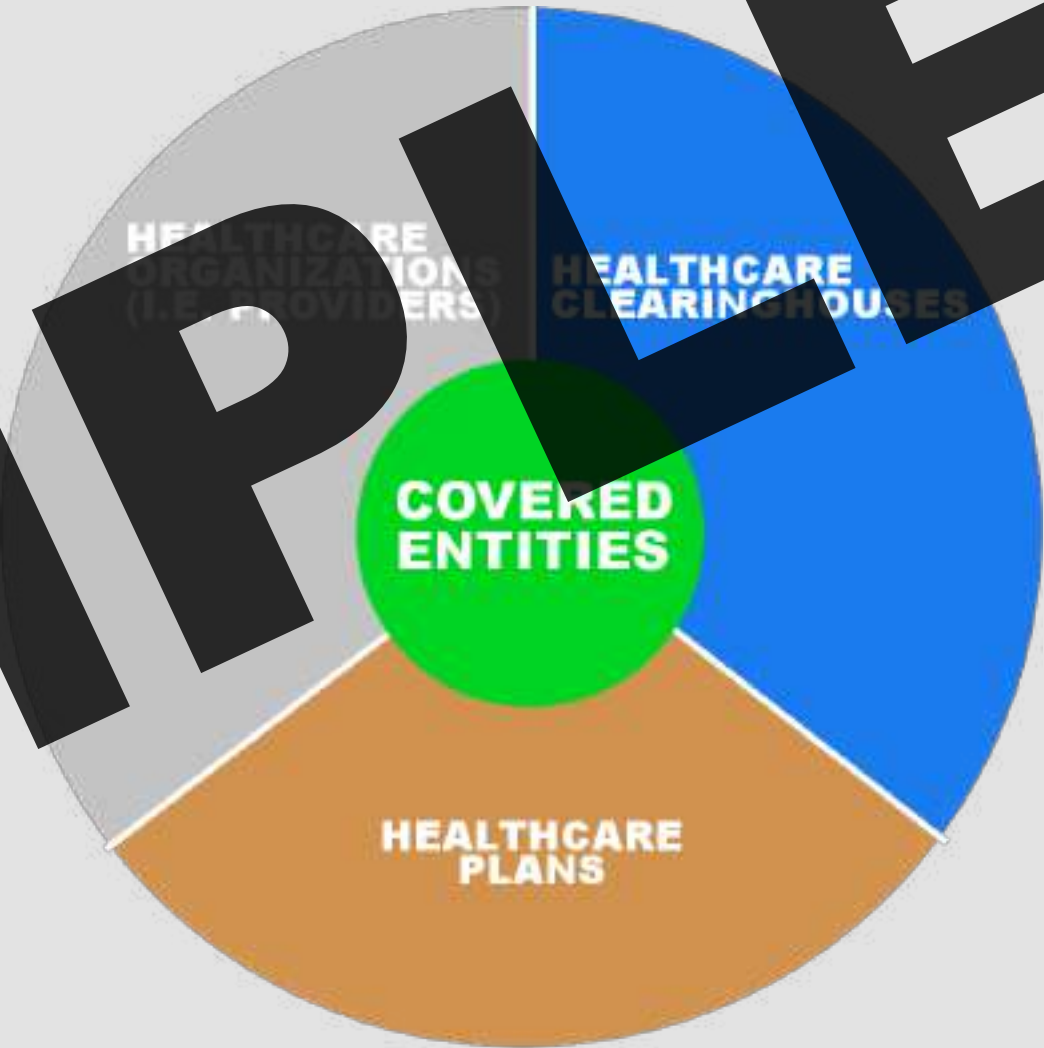


**HIPAA****OMNIBUS****HITECH**

The HIPAA Omnibus Final Rule (Omnibus Rule) became effective March 2013 and is known for connecting portions of HITECH to HIPAA to increase its regulations. The changes in regulations from this Rule will be included throughout the training.

**HARD HAT**
TRAINING SERIES**SAFETY**
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.HIPAA AWARENESS
TRAINING

Covered Entities (CE) are health plans, healthcare clearinghouses, and healthcare providers who transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.



A **health plan** is defined as a personal or group plan that provides or pays for the various costs of medical care. To the right is a chart which shows all health plans that are considered a covered entity under HIPAA.

Health Plan Covered Entities

Health Plans
Dental Plans
Vision Plans
Prescription Drug Insurers
Health Maintenance Organizations (HMOs)
Medicare
Medicaid
Medicare+Choice
Medicare Supplement Insurers
Long-term Care Insurers
Employer Sponsored Health Plans
Government Health Plans
Church Sponsored Health Plans
Multi-Employer Health Plans

Healthcare clearinghouses process non-standard health information, which they obtain from other entities. The clearinghouses take this medical information and convert it into a standard format or vice versa. To the right is a table which shows what entities could be categorized as a healthcare clearinghouse.

Health Care Clearinghouses

Billing Services

Repricing Company

Community Health Management Information System

Value-added Networks



Healthcare providers are recognized as institutional providers (hospitals), non-institutional providers (practitioners), and any other person or organization that offers, bills, or is compensated for healthcare services.



HARD HAT
TRAINING SERIES

SAFETY
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.



HIPAA AWARENESS
TRAINING



Who does HIPAA cover?

Healthcare Provider

Covered Entities



Billing Company

Business Associates

Law Firm

Subcontractor



A **business associate (BA)** is a person or organization who acts on behalf of a covered entity to complete activities that contain the storage, use, or disclosure of PHI. The Omnibus Rule recently made BA liable to all of HIPAA regulations. It also included organizations or persons who store PHI into the BA category. It is extremely important to know that if you do store PHI, even if it is not accessed at any point, you are still classified as a BA and can be held liable under HIPAA.



HARD HAT
TRAINING SERIES

SAFETY
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.



HIPAA AWARENESS
TRAINING





A **subcontractor** is a person or business that is contracted by a Business Associate to provide services or materials needed to fulfill the BAS contract with a CE. It is the responsibility of the business associates to ensure that they are following HIPAA regulations.



Three years after the HIPAA Omnibus Rule went into effect, a non-profit organization had a breach in which 412 patients were affected. In that same year, there were 328 breaches which involved more than 500 patients. Although the number of people affected by this breach was not substantial, the HHS Office for Civil Rights showed that the time for HIPAA enforcement had begun. The business associates were fined \$650,000.

What are the chances of...

Getting struck
by lightning



1 in 960

Dating a
millionaire



1 in 220

Experiencing a
data breach



1 in 4

A DATA BREACH WILL COST MORE
THAN YOU THINK



HARD HAT
TRAINING SERIES

SAFETY
PROVISIONS, Inc.
Copyright Safety Provisions, Inc.



HIPAA AWARENESS
TRAINING



We will begin our discussion with a quick look into **portability** within HIPAA in the next section. Portability is the capability of moving or carrying something easily. In reference to HIPAA, portability refers to the ability of an individual to retain their health insurance plan when moving from one employer to another.



Portability

SAMPLE



BUY THE COMPLETE
PRESENTATION HERE