CEU Central Continuing Education University

Presents

MEDICAL IDENTITY THEFT, CYBERCRIME & HIPAA

Contact Hours: 2

First Published: January 1, 2017

This Course Expires On: January 1, 2020

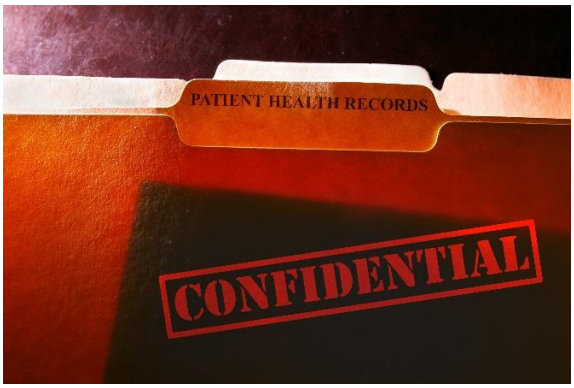
Course Objectives:

Upon completion of this course, the nurse will be able to:

1. Identify the purpose and components of HIPAA
2. Have knowledge of Medical Identity Theft
3. Identify information protected under the HIPAA privacy rules
4. Describe the responsibilities of healthcare providers / staff members / and facilities or healthcare organizations regarding HIPAA compliance

It was another ordinary day at work for Rachel, as she checked in yet another patient to the busy emergency department where she was employed as an admissions clerk. Towards the end of her shift, Rachel was approached by one of her co-workers who described an opportunity to "make easy money". All Rachel would have to do was print out the demographics sheet on each patient she admitted to the ER on her shift and she would be paid $100 in cash for each one. Rachel thought about it and decided to try it once, after all, she could certainly use the money.

Unfortunately for Rachel, she didn't realize that her co-worker was part of a medical identity theft ring that sells patient information to fraudulent individuals who use other's information to obtain medical care, buy drugs, or submit fake billings to Medicare or other insurance companies in the victim's name. Also unfortunately for Rachel, the FBI was conducting surveillance on Rachel's co-worker on suspicion of committing medical identity theft, and when Rachel turned over the first set of demographics, she was arrested for medical identity theft and HIPAA Violations.



The modern world is evolving and many laws coincide and interact with other types of laws. For instance, the Health Insurance Portability and Accountability Act is a law that can relate to certain computer crimes. **The Health Insurance Portability and Accountability Act, which is more commonly referred to as HIPAA, is often associated with the computer crime of *medical identity theft.*** HIPAA is related to the digital crime of medical identity theft because patients' personal medical information can be stolen from their medical records.

The Health Insurance Portability and Accountability Act is very important to the medical and health care system within the United States of America. According to David Kim and Michael G. Solomon, who authored the book *Fundamentals of Information Systems Security*, HIPAA is "a U.S. federal law requiring health care institutions and insurance providers to protect patients' private data and have proper security controls in place". Moreover, HIPAA mandates the establishment and distribution of all privacy policies that explain how all identifiable health information is acquired, utilized, and shared (Ferrera, et al., 2012, p. 374).

EDUCATION EDGE!

Everything written in green throughout this course is information you will need to know!

Additionally, the Health Insurance Portability and Accountability Act also develops stringent codes and regulations on how the private information and data is to be utilized and disclosed (Ferrera, et al., 2012, p. 374). This act is highly significant because everyone in the United States is required by law to be protected under the HIPAA law, because every American needs medical attention and care.

HIPAA has been protecting patients' private information for many years. However, computer criminals have been devising ways in order to circumvent this law, in order to ultimately steal patients' data and identities.

The United States of America has enacted a number of laws and regulations that are all designed to protect patients and safeguard their private information (Ferrera, et al., 2012, p. 374). In concerning the protection of patients' data and information, the Health Insurance Portability and Accountability Act is considered to be the most paramount law in protecting individual's health data and privacy in the United States (Ferrera, et al., 2012, p. 374).

Unlike other forms of computer crimes, which primarily focus on individual groups of people, like credit card holders and driver's licenses databases, the HIPAA laws affect everyone. This is because everyone at one point in time needs healthcare.

This problem is only going to become worse, because currently, the United States government is requiring that all healthcare providers need to have all medical information and records digital. Furthermore, this includes doctors' offices, hospitals, clinics, and healthcare agencies. People's most private information, both medical and personal, are at risked of being hacked. Moreover, everyone is at risk of becoming a victim of the computer crime of medical identity theft.

HIPAA has a long and rich history. The Health Insurance Portability and Accountability Act can also be referred to as "Kennedy-Kassebaum," and this act was passed in Congress in 1996 (Pierce & Thomas, 2013). Then, it was later passed as the Health Information Technology for Economic and Clinical Health Act in 2009 (Kim & Solomon, 2012, p. 441).

Under the HIPAA act, "healthcare providers and organizations have strict guidelines that must be followed to remain within the law" (Pierce & Thomas, 2013). The passing of this act, established "a number of rules and requirements relative to the privacy and security of individually identifiable health information" (Ferrera, et al., 2012, p. 545). Specifically, these requirements, rules, and laws within the Health Insurance Portability and Accountability Act primarily deal with the security of patient records and the confidentiality and privacy of patients and patients' records (Pierce & Thomas, 2013).

The Health Insurance Portability and Accountability Act was originally designed to protect patients' private information. HIPAA laws are overseen and regulated by the Department of Health and Human Services. Specifically, HIPAA applies to protected health information, which is also known as PHI.

DID YOU KNOW?

Protected health information refers to any type of individually identifiable data based on a patient's health, which includes a patient's physical and mental health information.

If a patient's protected health information is stolen, it can translate into a cybercrime. This is because protected health information can be in digital form (Kim & Solomon, 2012, p. 442). This is significant because the data that is contained within a patient's protected health information includes numerous personal facts about the patient (Kim & Solomon, 2012, p. 442). These facts can include the following:

- Medical information
- Past health problems
- Present health ailments
- Billing information

Theft of information has always been a major cause of concern for health care providers. The crime of theft is normally defined as "the taking of property with the intent of permanently depriving the owners of their property or service" (Taylor, 2011, et al., p. 10). **Obviously, in concerning matters and crimes during the current digital age, theft in cyberspace is related to depriving a person of information.**

Clearly, the increased use of computers has enabled criminals to conduct more crimes and to be able to steal their victims' private property, data, and information. This is hugely significant because this is now linked to the evolving computer crime of medical identity theft.

As such, HIPAA violations can be associated with cybercrime. A computer criminal can take advantage of the digital age and can easily steal another person's medical information. Therefore, the HIPAA act is normally violated by digital criminals who commit the cybercrime of medical identity theft.

Thus, according to Robert C. Newman, who wrote the book *Computer Forensics: Evidence Collection and Management*, identity theft is defined as "the act of impersonating another, by means of using the person's information, such as birth date, Social Security number, address, name, and bank account information, usually to gain access to the person's finances or frame him or her for a crime" (2007, p. 348). Basically, this cybercrime occurs when a computer criminal steals another person's personal information in a way that usually involves the employment of deception or fraud (Vacca & Rudolph, 2011, p. 316).

Medical identity theft is a heinous computer crime. The digital crime of medical identity theft is such a deplorable and dangerous crime, because it involves the computer criminal acquiring a certain amount of a victim's personal medical information, so that the digital criminal could have the opportunity to pose as that victim.

The computer crime of medical identity theft is related to the HIPAA laws because a cybercriminal can use a patient's improperly discarded medical information in order to steal their identity. In turn, the cybercriminal's newly acquired stolen identity can then be used in order to make purchases or to conduct financial transactions (Easttom & Taylor, 2011, p. 479).

Another possibility is that the computer criminal can also sell the stolen identity to a fugitive who is on the run from the law. **An additional reason is that a criminal could steal another person's identity in order to ruin that person's reputation** (Easttom & Taylor, 2011, p. 479).

Even though the reasons can vary for a computer criminal to steal another person's identity, the threat of digital criminals actively pursuing the theft of people's private information from health care agencies and providers is a real and growing threat. Hence, the threat of cybercriminals committing the computer crime of medical identity theft and targeting health care providers, in order to obtain patients' private information, must be taken seriously.

Technically, when identity theft transpires within the healthcare system and medical field, it is normally referred to as medical identity theft (Chaput). Medical identity theft is considered to be a crime that takes place when a criminal utilizes another individual's personal information, which can include the individual's name and insurance card number (Chaput). Usually, the victim is not aware that their private information has been stolen until the criminal makes bogus claims for medical goods and services (Chaput).

Identity theft can also be called identity fraud (Vacca & Rudolph, 2011, p. 20). Fraud is "a crime that involves intentional deception for personal gain or to cause other damage to an individual or company" (Vacca & Rudolph, 2011, p. 315). Typically, in concerning matters in cyberspace, the digital crimes of identity theft and identity fraud normally intercede with each other. As such, the United States Department of Justice claims that "identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (Easttom & Taylor, 2011, p. 5). Furthermore, any time a criminal attempts to utilize another person's personal information, in order to commit any kind of deception or fraud, is categorized as identity theft (Easttom & Taylor, 2011, p. 5).

More importantly, "unlike financial identity theft, medical identity theft can harm its victims by creating false entries in their medical records at hospitals, doctors' offices, insurance companies, and pharmacies" (Chaput). Furthermore, these fake changes that are made to victims' medical histories and files can potentially remain on record for years, without anyone discovering it or trying to correct it (Chaput).

Additionally, medical identity theft can also be referred to as health care fraud. According to the Federal Bureau of Investigation, "health care fraud costs the country an estimated $80 billion a year". The FBI further claims that health care fraud is a threat that will continue to increase (www.fbi.gov).

The FBI is in charge of investigating health care fraud cases. **One criminal case that the FBI investigated took place in New York. In this health care fraud case, a woman named Helene Michael was arrested for committing acts of health care fraud and identity theft. Helene Michael was the officer and owner of Medical Solutions Management Inc., and specifically, she was convicted of "conspiracy to commit health care fraud, health care fraud, and HIPAA identity theft crimes".**

In this case, Helene Michael took advantage of her role as an owner of a medical equipment company, and she was able to enter nursing homes in numerous counties throughout the state of New York. During the trial, it was discovered that Helene Michaels entered these nursing homes in order to access and later steal many patients' health care records. During her trial, Helene Michaels was found guilty of violating the Health Insurance Portability and Accountability Act. As a consequence, Helene Michael was sentenced to 12 years in prison (www.fbi.gov).

The crimes of medical identity theft and health care fraud can be committed by many different types of people (Chaput). Some of these various kinds of individuals can include:

- **Nurses**
- **Doctors**
- **Receptionists**
- **Lab technicians**

Most of the time, the crime of medical identity theft is usually an inside job (Chaput). For instance, employees working in hospitals, clinics, and doctors' offices can copy patients' private data and information and later give the private information to medical identity theft gangs (Chaput). Medical identity theft gangs are guilty of stealing hundreds of medical records and billing codes over the years (Chaput).

An example of an inside job is the following case from the FBI. In this criminal case, a doctor and two hospital employees were found guilty of violating the rules and regulations outlined within the HIPAA laws. In this case, a doctor, named Dr. Jay Holland, was found guilty, along with two hospital employees, named Candida Griffin and Sarah Elizabeth Miller (www.fbi.gov).

According to the FBI, Holland, Griffin, and Miller pleaded guilty in 2009 "to misdemeanor violations of the health information privacy provisions of the Health Insurance Portability and Accountability Act based on their accessing a patient's records without any legitimate purpose". As a direct result of their blatant violation to the Health Insurance Portability and Accountability Act, Griffin and Holland were sentenced to one year probation, and they both had to pay fines (www.fbi.gov). In addition to the sentence of probation and fines, Dr. Holland was additionally sentenced to serve community service, where he was ordered to educate and teach other healthcare professionals on the Health Insurance Portability and Accountability Act (www.fbi.gov).

There are also other examples of inside jobs in concerning the crime of medical identity theft for instance, sometimes medical identity theft can be committed by a patients' friends and family members. Friends and family members can assume the identity of a patient in order to receive that patient's health insurance benefits (Chaput).

Fortunately, the rules and regulations under the Health Insurance Portability and Accountability Act states covered entities are only allowed to utilize a patient's protected health information in a very specific way (Kim & Solomon, 2012, p. 442).

Some of these covered entities are as follows:

- **Health care clearing houses,**
- **Health care providers that send PHI in digital form**
- **Health plans (Kim & Solomon, 2012, p. 442).**

Covered within the Health Insurance Portability and Accountability Act, the Privacy Rule deciphers how covered entities must protect patients' privacy. As a consequence of this rule, covered entities must actively protect and safeguard all patients' protected health information. The Privacy Rule was established in 2000 and by spring 2003, all covered entities were required by law to follow this new rule (Kim & Solomon, 2012, p. 442).

Subsequently, the creation and the enforcement of this rule, was the first time in the history of the United States, where the federal government specified privacy protections for patients' protected health information. Moreover, according to the Privacy Rule under HIPAA, covered entities are not allowed to disclose any patient's protected health information without that patient's written consent (Kim & Solomon, 2012, p. 442).

Furthermore, covered entities must also acquire a person's written consent in order to use that person's protected health information. One of the only times where a covered entity is not forced by law to obtain a person's written consent, is when the covered entity shares the patient's protected health information with a doctor or health care provider (Kim & Solomon, 2012, pp. 442-443). This is because it is usually presumed within the medical and health care fields that patients generally desire to have their health care providers use their protected health information in order to provide them with the proper medical treatment (Kim & Solomon, 2012, p. 443).

Today, the patients' personal data and billing information is digital, so this can be problematic for many covered healthcare providers who use electronic medical records. This is because the healthcare providers are at risk of having their computer networks and systems hacked and having patient's vital information stolen. *As a result of these cyber risks, healthcare providers must not only strictly adhere to the HIPAA rules, laws, and regulations, they must also have certain security measures in place on their computers and servers.* So, healthcare providers that employ the use of protected health information must closely follow the privacy and security rules under the Health Insurance Portability and Accountability Act (Kim & Solomon, 2012, p. 442).

REMEMBER

Basically, no one is allowed to look at a patient's records unless they have permission from the patient. If someone accesses a patient's records without consent, then that person is in violation of HIPAA laws.

An example of this type of situation is a criminal case from the FBI. In this one particular case, Huping Zhou, who was an employee at UCLA Healthcare System, was found guilty of "illegally reading private and confidential medical records, mostly from celebrities and other high-profile patients" (www.fbi.gov). Huping Zhou admitted to these charges, and he was consequently found guilty of violating rules and regulations within the Health Insurance Portability and Accountability Act. As a result, Huping Zhou was sentenced to four months in prison for violating the Privacy Rule of HIPAA (www.fbi.gov).

IMPORTANT

HIPAA also contains a Security Rule. The Security Rule under HIPAA consists of three specific components of matters of security. These three security components are as follows:

1) Physical Safeguards – which includes the protection of equipment, data, and electronic systems.
2) Technical Safeguards – this includes the "authentication and encryption used to control data access".
3) **Administrative Safeguards – which consists of the assignment of a security compliance team.**

Covered entities must follow all of these security components within the HIPAA Security Rule.

Today, cybercriminals are able to apply the use of the Internet in order to steal information and private data. This correlates to the Health Insurance Portability and Accountability Act because HIPAA extends to information that is in digital form (Kim & Solomon, 2012, p. 445).

As such, electronic protected health information, which is also referred to as EPHI, is a rule within the Health Insurance Portability and Accountability Act that is designed to preserve and protect all electronic and digital forms of protected health information and data (Kim & Solomon, 2012, p. 445).

"Basically, electronic protected health information is protected health information that is stored in digital form. Furthermore, within this rule, covered entities must protect all electronic protected health information. Hence, covered entities must safeguard all electronic protected health information that they maintain, receive, or create. Also, they must actively and routinely protect and keep safe all electronic protected health information that they might transmit. More importantly, covered entities must additionally protect all electronic protected health information from potentially anticipated threats" (Kim & Solomon, 2012, p. 445).

In order to safeguard all electronic protected health information, covered entities must establish and engage in certain security measures (Kim & Solomon, 2012, p. 445). Therefore, covered entities must develop an information security program.

Ultimately, in order for a covered entity to develop and build an information security program, they must consider certain factors.

These factors are as follows:

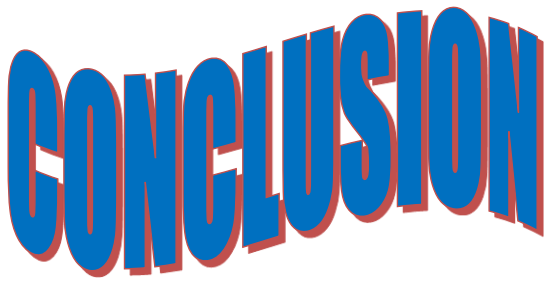
- **The potential risks to electronic protected health information**
- **The complexity and size**
- **The total cost of the security measures**
- **The technical infrastructure, which includes software and hardware security resources (Kim & Solomon, 2012, p. 445).**

Bottom line, covered entities must create and establish an information security program because cybercriminals are constantly devising new ways and methods to hack into computer systems and networks, in order to steal private and valuable data.

Essentially, encryption is a way for users to protect data and information. Encryption is basically defined as the method of converting plaintext into ciphertext (Elmasri & Navathe, 2011, p. 863). According to Ramez Elmasri and Shamkant B. Navathe who authored the book *Fundamentals of Database Systems*, "encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized persons".

However, sometimes digital information is not stolen by computer criminals. **Sometimes, digital information could be misplaced accidently or lost**. For example, in 2009, it was discovered that an external hard drive, which contained over 1 million patients' health records, was missing (Kim & Solomon, 2012, p. 441). This was a major problem for these unfortunate patients because the data on the missing hard drive was not encrypted (Kim & Solomon, 2012, p. 441).

"Consequently, the method of encrypting data and information vastly improves security and privacy. This is due to the fact that when data is lost or stolen, the encrypted information will not be able to be easily read by computer criminals (Elmasri & Navathe, 2011, p. 862). This is why the method of encryption must be utilized by all covered entities. Ultimately, the use of encryption will improve the security measures of the covered entities, because it will aid in safeguarding patients' private information and data.



The Health Insurance Portability and Accountability Act was created to protect patients' privacy and security. Also, HIPAA can play a major role in certain computer crimes. Often these computer crimes include identity theft and medical identity fraud. Even though there are many ways a person can violate the laws within the Health Insurance Portability and Accountability Act, the use of the Internet has aided cybercriminals in being capable of committing the computer crime of medical identity theft. So, in order to defend against threats in cyberspace, all health care providers must strictly adhere to all of the laws, codes, and regulations that are outlined within HIPAA.

REFERENCES

Chaput, Bob. About HIPAA. http://abouthipaa.com/. HIPAA Security Reminder – Knowing Identity Theft. Retrieved from http://abouthipaa.com/hipaa-and-it-security/hipaa-security-reminder-knowing-identity-theft/.

Easttom, Chuck & Taylor, Jeff. (2011). *Computer Crime, Investigation, and the Law*. Boston, MA: Cengage Learning.

Elmasri, Ramez & Navathe, Shamkant B. (2011). *Fundamentals of Database Systems*. Boston, MA: Pearson Education, Inc.

Federal Bureau of Investigation. www.fbi.gov. (April 2010). Ex-UCLA Health Care Employee Sentenced to Federal Prison for Illegally Peeking at Patient Records. Retrieved from http://www.fbi.gov/losangeles/press-releases/2010/la042710a.htm.

Federal Bureau of Investigation. www.fbi.gov. (April 2013). Long Island Health Care Provider Sentenced to 12 Years in Prison $10 Million Medicare Fraud and HIPAA Identity Theft. Retrieved from http://www.fbi.gov/newyork/press-releases/2013/long-island-health- care-provider-sentenced-to-12-years-in-prison-for-10-million-medicare-fraud-and-hipaa-identity-theft.

Federal Bureau of Investigation. www.fbi.gov. (October 2009). Doctor and Two Former Hospital Employees Sentenced for HIPAA Violations. Retrieved from http://www.fbi.gov/littlerock/press-releases/2009/lr102609.htm.

Federal Bureau of Investigation. www.fbi.gov. Health Care Fraud. Retrieved from http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud.

Ferrera, Gerald R., Reder, Margo E., Bird, Robert C., Darrow, Jonathan J., Aresty, Jeffrey M., Klosek, Jacqueline, & Lichtenstein, Stephen D. (2012). *Cyberlaw Text and Cases*. Mason, OH: South-Western, Cengage Learning.

HIPAA Guidelines. www.hipaaguidelines101.com. HIPAA Security Rule and Compliance. Retrieved from http://www.hipaaguidelines101.com/hipaa-security.htm.

http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx

https://oig.hhs.gov/fraud/medical-id-theft/

https://privacyruleandresearch.nih.gov/

https://www.ama-assn.org/practice-management/hipaa-compliance

https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/fact-sheets/hipaa

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

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Kim, David & Solomon, Michael G. (2012). *Fundamentals of Information Systems Security*. Sudbury, MA: Jones & Bartlett Learning.

Newman, Robert C. (2007). *Computer Forensics: Evidence Collection and Management*. Boca Raton, FL: Taylor & Francis Group.

Taylor, Robert W., Fritsch, Eric J., Liederbach, John, & Holt, Thomas J. (2011). *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ: Pearson Education, Inc.

Vacca, John R. & Rudolph, K. (2011). *System Forensics, Investigation, and Response*. Sudbury, MA: Jones & Bartlett Learning.