Martha Herz
HIM
Chapter 9

**Chapter 9: Data Privacy and Confidentiality**

1. Check Your Understanding

9.1

1. B. Has been granted via court decisions

2. C. it is a pretrial process

3. B. deposition

4. B. Subpoena duces tecum

5. B. information that shows who accessed a record

6. C. must usually be accompanied by patient authorization

7. B. an individual appears at an appointed time and place to testify under oath

8. C. preserve information

9. C. it is destroying, changing, or hiding evidence intentionally

10. C. may be preempted by HIPPA

9.2

1. A. for as long as it is maintained

2. C. preempt less strict state statues where they exist

3. D. covered entities and their business associates

4. B. in any form or medium, including paper and oral forms.

5. D. Both health plans and healthcare providers may deny the request

6. A. Impose a reasonable cost-based fee

7. B. organizations outside the covered entity’s workforce that use phi to perform functions on behalf of the covered entity.

8. B. accomplish the intended purpose

9. B. volunteers

10. A. does not identify an individual

9.3

1. B. Must be posted in a prominent place where it is reasonable to expect that patients will read them.

2. A. an incidental disclosure

3. C. receive a copy of the notice of privacy practices

4. B. consent

5. D. they are not required to permit use and disclosures of PHI for treatment, payment or operations.

6. C. is subject to the patient having had the opportunity to informally agree or object.

7. A. Revoking an authorization in writing.

8. D. information provided to a treating physician

9. C. is public interest and benefit disclosure that does not require patient authorization

10. D. is not required if an IRB or privacy board alters or waives the authorization requirement

9.48

1. B. does not require written authorization for face to face communications with the individual

2. A. who committed the breach

3. D. encrypting all electronic PHI

4. C. it applies when one person’s PHI is breached

5. B. A signature and stamp by a notary

6. A. using another person’s name to obtain durable medical equipment

7. A. an account held by a person who is over 80 years old

8. A. every member of the covered entity’s workforce must be trained.

9. D. A minor’s [personal representative

10. C. individuals must be informed in the notice of privacy practices that their information may be used for fundraising purposes.

2 Define:

Access report- Report that provides a list of individuals who accessed patient information during a given period

Administrative simplification- As amended by HITECH. Authorizes HHS to: adopt standards exchange health data, to adopt standard identifiers and individuals for use on standard transactions, and to adopt stands to protect the security and privacy of personally identifiable health information.

ARRA-American Recovery and Reinvestment act- the purpose of this act include the following; to preserve and create jobs and promote economic recovery, to assist those most impacted by the recession, to provide investments needed to increase economic efficiency by spurring technological advances in science and health, to invest in transportation, environmental protection, and other infrastructure that will provide long-term economic benefits, to stabilize state and local government budgets, in order to minimize and avoid reductions in essential services and counterproductive state and local tax increases.

Admissibility- The condition of being admitted into evidence in a court of law.

Breach-Under HITECH, the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part that compromises the security or privacy of the protected health information.

BA- Business associate- a person or organization other than a member of a covered entity’s workforce that performs functions or activities on behalf of or affecting a covered entity that involve the use or disclosure of individually identifiable health information. As amended by HITECH with respect to a covered entity, a person who creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, and repricing or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

CLIA-Clinical laboratory improvement amendments of 1988- established quality standards for all laboratory testing to ensure the accuracy reliability and timeliness of patient test results regardless of where the test is

Confidentiality-A legal and ethical concept that establishes the healthcare provider’s responsibility for protecting health records and other personal and private information from unauthorized use or disclosure. As amended by HITCH, the practice that data or information is not made available or disclosed to unauthorized persons or processes.

Complaint- In litigation, a written legal statement from a plaintiff that initiates a civil lawsuit.

Consent- A patient’s acknowledgment that he or she understands a proposed intervention, including that intervention’s risks, benefits, and alternatives. The document signed by the patient that indicates agreement that protected health information (PHI) can be disclosed.

Covered entity-As amended by HITECH a health plan, a health care clearinghouse, a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Deidentified information- Information where personal characteristics have been stripped from it in such a way that it cannot be later constituted or combined to re-identify an individual. It is commonly used in research.

HIS- Hospital information system- the comprehensive database containing all the clinical, administrative, financial and demographic information about each patient served by a hospital.

DRS- Designated record set- as amended by HITECH a group of records maintained by or for a covered entity that is, the medical records and billing records about individuals maintain by or for a covered health care provider, the enrollment, payment claim adjudication and case or medical management record systems maintained by or for a health plan, used in whole or in part by or for the covered entity to make decisions about individuals.

E-discovery- refers to amendments to federal rules of civil procedure and uniform rules relating to where in audit trails, the source code for the program, metadata and any other electronic information that is not typically considered the legal health record is subject to motion for the compulsory discovery.

Facility directory- a directory of patients being treated in a healthcare facility.

FRCP-Federal Rules of Civil procedure- rules established by the US supreme court setting the “rules of the road” and procedures for federal court cases. FRCP include electronic records and continue to be very important as benchmarks in how these records can be used in courts, not only federal, but state and other courts as well.

FRE- Federal Rules of evidence- rules established by the us Supreme Court guiding the introduction and use of evidence in federal court proceedings that are an important benchmark for state and other courts. FRE governs what and how electronic records may be used and the roles of record custodianship.

FTC- Federal Trade Commission- an independent federal agency tasked with dealing with two areas of economics in the United States, consumer protection and issues having to do with competition in business.

HITECH-Health information technology for economic and clinical health- Legislation created to promoted the adoption and meaningful use of health information technology in the United States. Subtitle D of the act provides for additional privacy and security requirement that will develop and support electronic health information, facilitate information exchange and strengthen monetary penalties.

HIPAA-Health Insurance Portability and Accountability Act- The federal legislation enacted to provide continuity of health coverage, control, fraud and abuse in healthcare, reduce healthcare costs and guarantee the security and privacy of health information, limits exclusion for pre-existing medical conditions prohibits discrimination against employees and dependents based on health status, guarantees availability of health insurance to small employers regardless od size, requires covered entities (most healthcare providers and organizations) to transmit healthcare claim in a specific format and to develop, implement and comply with the standards of the privacy rule and the security rules and mandates that covered entities apply for and utilize national identifiers in HIPPA transactions.

Hearsay- A written or oral statement made outside of court that is offered in court as evidence.

Legal hold- A communication issued because of current or anticipated litigation, audit, government investigation, or other such matters that suspend the normal disposition or processing of records. Legal holds can encompass business procedures affecting active data, including, but not limited to, backup tape recycling the specific communication to business or IT organizations may also be called a “hold” “preservation order” “suspension order” “freeze notice” “hold order” or “hold notice”

Medical identity theft- The fraudulent use of an individual’s identifying information in a healthcare setting.

Minimum necessary- Requires that uses disclosures, and request must be limited to only the amount needed to accomplish an intended purpose.

ONC- The Office of the National Coordinator for Health Information Technology- the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information. The position of National coordinator was created in 2004, through an executive order and legislatively mandated in the HITECH act of 2009

Personal representative- Person with legal authority to act on a patients behalf.

Preemption- In law, the principle that a statue at one level supersedes or is applied over the same or similar statue at a lower level.

PHI- Protected health information- as amended by HITECH, individually identifiable health information; except as provide in paragraph of this definition, that transmitted dby electronic media, maintained in electronic media or transmitted or maintained in any other form or medium.

Red Flags Rule- consists of five categories of red flags that are used as triggers to alert the organization to a potential identity theft, the categories are alerts, notification or warnings from a consumer reporting agency. Suspicious documents, suspicious personally identifying information such as a suspicious address; unusual use of or suspicious activity relating to, a cover account; notices from customers; victims of identity theft, law enforcement authorizes or other business about possible identify theft in connection with an account.

Right to request amendment- One may request that a covered entity amend PHI or a record about the individual in a designated record set.

Spoliation- The act of destroying, changing, or hiding evidence intentionally.

TPO- Treatment, payment and operations- the privacy rule provides a number of exceptions for PHI that being used or disclosed for TPO purposes. Treatment means providing, coordinating, or managing healthcare or healthcare-related services by one or more healthcare providers; payment includes activities by a health plan to obtain premiums, billing by healthcare providers or health plans to obtain reimbursement, claim management, claims collection, review of the medical necessity of care, and utilization review; the privacy rule of care and utilization review; the privacy rule provides a broad list of activates that are healthcare operations that includes quality assessment and improvement, case management, review of healthcare professionals qualifications, insurance contracting legal and auditing functions, and general business management functions such as providing customer service and conducting due diligence.

Warrant-A judge’s order that authorizes law enforcement to seize evidence and conduct a search.

Sale of information-Addressed specifically by ARRA, which prohibits a covered entity or BA from selling (receiving direct or indirect compensation) in exchange for an individual’s PHI without that individual’s authorization; the authorization must also state whether the individuals permits the recipient of the PHI to further exchange the PHO for compensation.

3**. You should always have the actual language of the HIPAA privacy regulation at your fingertips should questions about interpretations arise**.

1. **Review Breach Notification. Evaluate the information offered and how to report a breach.**

Originally when implanted HIPAA required that covered entities lessen the harmful effect of wrongful use or disclosure of PHI but disclosure is optional. With the changes made by the ARRA breach notifications are now required and have set guidelines. Victims must be notified without delay, meaning no more than 60 days after the breach was discovered or first known. The notification must include and brief description of the breach, what information was disclosed, what steps they should take to protect themselves and what the covered entity is doing to lessen the harm of the breach, and prevent further breaches. It also needs to include a contact number if they have any further questions. It also requires that if more than 500 individuals are effected than they must be notified individually and the media outlets but be notified as well. In addition to the victims and the media covered entities must also notify the Secretary by filling out and electronically submitting a breach report form.

   2**. Review Special Topic and choose Health Information Technology.   Visit the various sites and summarize your findings as they relate to this chapter.**

 <http://www.hhs.gove/hipaa/for-professionals/index.html>
When HIPAA was first established health records were still mostly paper and it was written with that in mind. These various articles and links describe how the health information technology and work with the guidelines of the right of access and privacy requirements established by HIPAA.

**4. Visit the State of Maine website.**

 What are the various state laws related to ownership of the health record?
Maine does not have any laws that identify specific ownership or property rights to medical records. They do have medical record retention polices, but nothing that states who owns the medical record.

**5. Evaluate/summarize the following website and information that is offered.**

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

The Office for Civil Rights portion of the HHS.gov website gives information relating to the civil rights and privacy laws as they relate the health records. It has links that explain what is protected by law and how the record can be used and disclosed. It is a good resource for anyone who would like to be educated on the subject and especially those that may believe their rights have been violated.

**6.Retrieve 2 articles from the internet that have been written in the past year on privacy compliance. Summarize the important concepts. What have you discovered from this search that is not addressed in this chapter?**

<http://searchhealthit.techtarget.com/blog/Health-IT-Pulse/Health-data-breaches-down-in-October>

 <http://healthitsecurity.com/news/cyberattack-causes-healthcare-data-breach-at-mainegeneral>

In December 2015 information was released about a large cyber-attack that caused data breach at Maine General Medical Center here in Maine. That articles talks about how the Senate recently passed the Cyber security Information Sharing Act that will help create a framework for sharing information regarding cyber security threats across the healthcare industry. This act will help healthcare professionals connect with each other to share their experiences, best practices and other information regarding security.
In the other article I read from searchhealthIT published in November of 2016 it states that breaches have decreased for the month of October. It says that only 35 breaches occurred last month of those 35 40% of them were caused by hacking, malware or ransomware and 664,548 patients’ records were affected. This articles talks about how the abundance of health records available to be bought by criminals and the increased in attention by law enforcement has brought the price of black market health records down significantly. The article cautions that they do not know how criminals will respond to this price drop. They also caution that just because the number have breaches are on the decline and the price has dropped that it does not mean that healthcare organizations should stop being vigilant. Healthcare organizations should work to prevent future breaches by monitoring their internal systems for weird data transfers and implement strong password rules.

**7. Do you think there are problems with any of the HIPAA Privacy rule's exceptions to the authorization requirement? Do the exceptions minimize patient privacy? Are there too many exceptions? Are there other exceptions that you would include if you were asked to become involved in revising the law?**

I think that the biggest problem with HIPAA regarding patient’s privacy is that there are too many exceptions. The long list of exceptions create too many loop holes in patient privacy that allow the sharing of PHI for commercial use but on the other hand the strong rules of HIPPA and confusing misinterpretations cause healthcare organizations to be afraid of breaches to the point that they are not sharing information with family members or for treatment purposes to avoid the possibility of a breach. I think there is more than enough exceptions in the way HIPAA is written I would not include any more if I were asked to become involved in the revising of the law.