Chapter 9 Key terms

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 printout showing who accessed a record

6. c must 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 hipaa

9.2

1. a. for as long as they are maintained

2. c premp 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. c. healthcare providers must still honor the request

6. b. not charge the individual

7. b organizations outside the covered entity’s workforce that use phi to perform functions on behalf ot he covered entity

8. b accomplish the intended purpose

9. a information system firm staff

10l. a does not id an individual

9.3

1. b must be posted in a prominent place where it is reasonable to expect the 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 disclosure of phi for treatment, payment or operations

6. c

7. d

8. d

9. c

10 d

9.4

1. b

2. a

3. d

4. c

5. b

6. b

7. a

8. a

9. d

10. c

2 Define:

Access report—report would allow an individual to see a record of every person who viewed the individuals’ drs during the previous three years

Administrative simplification—hipaa’s attempt to streamline and standardize the healthcare industry’s nonuniform business practices such as billing, including the electronic transmission of data.

ARRA—American recovery and reinvestment act provides significant funding for health information technology and other stimulus funding

Admissibility—what is admissible as evidence pertaining to how it was obtained and relevance to the case.

Breach—requirements that specify victims of breaches by notified an depending on the number of individuals affected the federal government and media outlets also be notified. Unauthorized acquisition access use or disclosure of phi that compromises the security or privacy of such info

BA—business associate is a person or organization other than a member of a covered entities workforce that performs functions or activities on behalf of or for a covered entity that involves the use or disclosure of phi

CLIA—clinical laboratory improvement amendments of 1988 regulates the quality of lab testing

Confidentiality—similar to privacy but it stems from the sharing of private thoughts in confidence with someone else.

Complaint—allegation about the entities policies and procedures, its noncompliance with them or its noncompliance with the privacy rule.

Consent—patient’s agreement to use or disclose personally identifiable info for treatment, payment and healthcare operations.

Covered entity—a person or organization that must comply with the hipaa privacy rule.

Deidentified information—does not id an individual because personal characteristics have been stripped from it in such a way that it cannot be later constituted or combined to re id an individual

HHS—department of health and human services primary federal entity responsibility for coordinating national efforts to implement and use health info technology

DRS—designated record set includes the health records, billing records, and various claims records that are used to make decisions about an individual.

E-discovery—same pretrial process as discovery but parties now obtain and review electronically stored data

Facility directory—directory of patients for person who ask for individuals by name and for clergy

FRCP—federal rules of civil procedure incorporated electronic information through the creation of e discovery tools.

FRE—federal rules of evidence governs admissibility in the federal court system

FTC—federal trade commission promotes consumer protection

HITECH—health info technology for economic and clinical health act

HIPAA—health insurance portability and accountability act part of privacy accountability laws

Hearsay—often excluded out of court statement used to prove the truth of a matter and it is inherently deemed untrustworthy because the maker of the statement was not cross examined at the time the statement was made.

Legal hold—a court order to preserve a health record if there is concern about destruction

Medical identity theft—is a crime that challenges healthcare organization and the health info profession healthcare fraud that includes both financial fraud and identity theft

Minimum necessary—requires uses, disclosures, and requests must be limited to only the amount needed to accomplish an intended purpose.

ONC—office of the national coordinator for health information technology was first established by presidential executive order

Personal representative—person who has legal authority to act on another’s behalf.

Preemption—means that federal law may supersede state law.

PHI—protected health information id’s an individual or provides a reasonable basis to believe the person could be id’d from the info given.

Red Flags Rule—consists of 5 categories of red flags that are used as triggers to alert the organization to a potential id theft.

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—act of destroying changing or hiding evidence intentionally

TPO—treatment payment and operations is an important concept because the privacy rule provides a number of exceptions for the phi that is being used or disclosed for tpo purposes.

Warrant—is a judges order that authorizes law enforcement to seize evidence and often to conduct a search as well.

Sale of information—prohibits a covered entity or ba from selling in exchange for an individuals phi without the individual’s authorization

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

  1. Review Breach Notification. Evaluate the information offered  and how to report a breach. When a breach happens, it is important to notify the person it happened to as soon as possible. It seems when a group is breached, that 60 days could be a long time. I do wish it was less time then this. I am not sure how it can be determined if it is an imminent misuse or not. That seems like it is subjective. I believe lots can happen in 60 days for those that are not on top of their credit and accounts. I do like that the type of breach is shared but it feel it can be equally important to know from whom the breach has happened.

   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>

HHs has adopted national standards for electronic healthcare transactions, code sets unique health identifiers and security. Congress has helped secure the rules and laws around this. There are 3 types of entities that must abide by this; health plans, healthcare clearinghouses, and providers. Compliance to the security rule was enforced in 2005. This was rules around confidentiality, integrity and electronic protected health information. The enforcement rule was implemented.

4. Visit the State of Maine website.

 What are the various state laws related to ownership of the health record?

* State of maine maintains the healthrecord of the foster child but it does follow them into the foster homes. There are no specific laws that I could find around the ownership specifically and the research I found states   
  No law identified conferring specific ownership or property right to medical record

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

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

This website focuses on civil rights around availability access to all HHS programs. It helps with how to report hipaa breaches when applicable. It is available in multiple languages and includes professionals as well as individuals.

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://www.ahima.org](http://www.ahima.org/)

[http://www.fierchealthcare.com](http://www.fierchealthcare.com/)

[http://www.healthcareitnews.com](http://www.healthcareitnews.com/)

[http://www.himss.org](http://www.himss.org/)

The trade-off to big data in healthcare: Privacy

The article states that big data has many advantages including helping with diagnosis but it does put the medical record at risk of a breach. They are working towards being able to predict who may be at risk. This includes in the algorithm, social media. For example, patient takes cholesterol meds, is over weight and has posted on facebook about a divorce. All this information is collected and used to devise a medical plan for the patient. The more information that can be included the more effective this system is but to what cost?

# ​Health care organizations face consequences if they fail to protect data

* **Although the book does state that with violations comes sanctions of some sort this article discusses some of the punishments handed down for not properly training their employees.**
* A $4.8 million fine against New York Presbyterian Hospital and Columbia University for poor server management that exposed protected health information,
* A $4.3 million fine against Cignet Health of Maryland for multiple HIPAA violations, including $3 million for willfully ignoring investigators,
* A $1.7 million fine against WellPoint Inc. for insecure servers and ineffective administrative and technical safeguards that left ePHI exposed,
* A $1 million fine against Massachusetts General Hospital after sensitive documents were left on a train by an employee.

Some of the issues are lack of education to the employee others are complacent employers.

7. Do you think there are problems with any of the HIPAA  Privacy rule's exceptions to the authorization requirement? I feel that information one does not want to get out could get out. It only takes one leak at the police department or hospital to leak this information.

Do the exceptions minimize patient privacy? The exceptions can minimize privacy but they are set into place to protect the patient/victim.

Are there too many exceptions? I do believe likely there are too many exceptions or not tight enough rules around them. How are the leaks taken care of?

Are there other exceptions that you would include if you were asked to become involved in revising the law? There are no more exceptions but likely I would remove some or change the process to make it more protected for the individual.