Check Your Understanding

9.1:

1. B 2. C 3. B 4. B 5. B 6. C 7. B 8. C 9. C 10. C

9.2:

1. A 2. C 3. D 4. B 5. D 6. A 7. B 8. B 9. B 10. A

9.3:

1. B 2. A 3. C 4. B 5. D 6. C 7. A 8. D 9. C 10. D

9.4

1. B 2. A 3. D 4. C 5. B 6. A 7. A 8. A 9. D 10. C

2 Define:

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

Administrative simplification-Adopt standards for transactions and code sets that are used to exchange health data, adopt standard identivfers for health plans, health care providers, empolyers, and individuals for use on standard transactions, adopt standards to protect the security and privacy of personally identifiable health info.

ARRA: American Recovery and Reinvetment Act: To preserve and create jobs and promote economic recovery, assist those most impacted by recession. Provide investments needed o increase economic effecincy Invest in trasportation, environmental protection, and more.

Admissibility: The Condition of being admitted into evidence in a court of law.

Breach: The acquisition, access, use or disclosure of proected health info in a manner not permitted under subpart E.

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.

CLIA: Clinical Laboratory Improvement Amendments of 1988: Established quality standards for all lab 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 providers responsibility or protecting health records and other personal and private info from unauthrized use.

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

Consent: A patient’s acknowledgeemtn that he or she understands a proposed intervention including the risks, benefits and alternatives.

Covered entity: A health plan, health care clearing house.

Deidentified information: Information where personal characteristics have been stripped from it in such a way that it can not be latter constituted or combined to reidentify an individual.

HHS: Department of Health and Human Services: The Cabinet level federal agency and principal agency for protecting the health of all Amerians and providing essentional human services, especially for those who are at least able to help themselves

DRS: Designated Record Set: A group of records maintained by or for a covered entity that is the medical records and billing records about individual lmaintained by or for a covered health care provider, the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health pan.

E-discovery: The amendments to federal rules of civil procedure and uniform rules relating to Discovery of Electronically Stored Information that is subject to motion for ompulsory discovery

Facility directory: A directory of patients being treated in a healchcare facility.

FRCP: federal rules of Civil procedure: rules established by the U supreme court settting the rules of the road and procedures for federal court cases.

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.

FTC: An independent federal agency tasked with dealing with two areas of economics in the US. Consumer protection and issues having to do with the competition in business.

HITECH: Health information technology for economic and clinical health act: Legslation created to promote the adoption and meaningful use of health info technology in the US.

HIPAA: Health insurance portability accountability act: federal legislation enacted to provide continuity of health coverate, control fraud and abuse in healthcare, reduce healthcare costs and guarantee the security and privacy of health info.

Hearsay: A written or oral statement made outside of court that is offerend 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 dispotion or processing of records. Legal holds can encompass business procedures.

Medical identity theft: the fraudulent use of an individuals identifying info in a healthcare setting

Minimum necessary: Requires that uses, discloures and requests must be limited to only the amount needed to accomplish an intended purpose.

ONC: Office of the National Coordinator for Halth Info: the principal federal entity charged with coordination of nationwide efforts to iplement and use the most advanced health information technology and the electronic exchange of health information.

Personal representative: Person with legal authority to act on a ptient’s behalf.

Preemption: the principle that a statute at one level supersedes or I applied over the same or similar statute at a lower level.

PHI: Protected Health information: Individually identifiable health information

Red Flags Rule: 5 categories of red flags that are used as triggers to alert the organiztion to a potential identity 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: 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 is being used or disclosed for TPO.

Warrant: a Judges order that authrizes law enforcement to seize evidence and conduct a search.

Sale of information: Prohibits a covered entity from selling in exchange for an individuals PHI without that individual authorizing the exchange.

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.

A breach is when protected health information is used, shared, acquired, or disclosed without permission. When the discovery is made that a breach has occurred, every individual that was included in the breach must be notified. If there are less than 500 individuals affected, they are to be notified in by mail or phone within 60 days of the breach discovery. If more than 500 individuals are affected mail and phone are still required. However, now, media outlets must be used. The Secretary of HHS is to be notified when a breach is discovered too. In the breach report to individuals there is a description of what happened, date of breach, and date of discovery. The types of unsecured PHI what were involved, as well as steps the individual may want to do to ensure their personal identity safety. There is also a notification of who is investigating, mitigatign and how prevention will happen for the future.

   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.gov/hipaa/for-professionals/index.html>

I’m not sure if I made it to the correct website. It seems to bring me to an error. The website I went to is HHS.gov and it is a page that listed off the Privacy rules, security rules, enforcement rules, final omnibus rule, and breach notification rules. This website helps professionals stay up to date on the HIPPA rules and requirements. There are PDF documents explaining new provisions or updates and the dates are shown to ensure it is all current.

4. Visit the State of Maine website.

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

Maine allows health facilities to share health record informaton for public health safety. It can’t be disclosed, used or received any information regarding the health file without authorization. The records that are acquired for public health can only be used for that reason. Personal information isn’t able to be shared.

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

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

This link led me to Civil rights and how HIPPA protects our Nondiscrimation and health information privacy and patient safety. It educates our local service workers about our civil rights, health informatin privacy, and patient safety confidentiality laws. It also educates cummunities. This website/program, will investigate civil rights, health information privacy, and patient safety infomatin to ensure discrimination and violation of the law hasn’t occurred. If so, they take action to correct the problem. This website informs people of their rights and allows you to file with the office of civil rights if you feel you’ve been discrimated or a violation of the law occored to you.

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 2 articles I retrieved from the internet that have been written in the past year on privacy compliance are:

<http://www.himss.org/news/white-house-releases-presidential-policy-no-41-united-states-cyber-incident-coordination>

<http://www.himss.org/news/himss16-industry-perspective-it-s-all-about-privacy-and-security-education>

The first article is a brief review about how cyber secruity is important. The Presidential Policy Directive No 41 is a set of principles that the government will use to respond to cyber security incidences. The PPD focus in on “significant cyber incident” that demonstrates harm to national security, foreign affairs, civil liberties, economic security, or public confidence. There are now 5 guiding principles that the government will follow when a major cyber security incident occures. There are 3 lines of effort the governement will do: threat response, asset response, and intelligence support.

The second article is about the importance of security education. This article states the better edcuation and awareness of PHI security is important. One issues is that data needs to be easier to access for the individual and the government. The article also states cybersecurity is extremely important and that more security needs to be put into place. There should be more education on how to protect patient data and how to protect shared data. They also want to create apps to allow patients to access their record easily but also ensuring patient record safety. This article also states that, even though HIPPA policies occurred before electronic data, it doesn’t get in the way because it is just a basic set of standards that can be adaptable.

7. Do you think there are problems with any of the HIPAA  Privacy rule's exceptions to the authorization requirement?

Hippa Privacy rule allows patients the right to privacy regarding their health information. I believe that unless I choose to share my information publiicly regarding diseases I have or issues with the FDA, it shouldn’t be shared. I believe that it can be accessible if required by law. A couple of problems is for research, where a board alters or waives an authorization requirement. I don’t like how someone can dictictate the importance of sharing my information based on their research needs or for public safety.

Do the exceptions minimize patient privacy?

The exceptions may lead to patient information leaks/breaches.

Are there too many exceptions?

There are too many exceptions, especially for public safety.

Are there other exceptions that you would include if you were asked to become involved in revising the law?

I already feel there are too many exceptions. However, if a person is deceased, I feel it is ok for a direct spouse to know the health information of their loved one.