1. Check Your Understanding

 9.1

B,C,B,B,B, B, B,C,C, B

9.2

A,C,D,B,D,A,B,B,B,B

9.3

B,A,A,A,D,B,A,A,C,A

2 Define:

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

Administrative simplification- to adopt standards for transactions and code sets that are used to exchange health data; adopt standard identifiers for health plans, healthcare providers, employers, and individuals for use on standard transactions.

ARRA- American Recovery and Reinvestment Act; to preserve and create jobs and promote economic recovery; to assist those most impacted by the recession.

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

Breach- 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 preforms 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; 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 providers responsibility for protecting health record and other personal and private information from unauthorized use and disclosure.

Complaint- in litigation, a written legal statement form a plaintiff that initiates a civil lawsuit

Consent- a patient’s acknowledgement that he or she understands a proposed intervention, including the interventions risks, benefits, and alternatives.

Covered entity- a health plan, a health care clearing house, or a healthcare provider who tranmits any health information in electronic form in connection with a transaction covered.

Deidentified information- information where personal characteristics have been stripped from it in such a way that it cannot be later constituted or combined to reidentify and individual; it is commonly used in research.

HHS- The department of Health and Human Services

DRS- Designated Record Set; a group of records maintained by a covered entity

E-discovery- refers to amendments to federal rules of civil procedure and uniform rules relating to discovery of electronically stored information.

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

FRCP- Federal Rules of Civil Procedure; rules established by the Supreme Court setting the rules of the road for federal court cases.

FRE- Federal Rules of Evidence; rules established by the supreme court guiding the introduction and use of evidence in federal court cases.

FTC- Federal Trade Commission; an independent federal agency tasked with dealing with two areas of economics in the US

HITECH- Health Information Technology for Economic and Clinical Health; legislation created to promote the adoption and meaningful use of health information technology in the US

HIPAA- Health Insurance Portability and Accountability Act; federal legislation enacted to provide continuity of health coverage, control fraud and abuse in healthcare, reduce costs, and guarantee the security and privacy of health information

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.

Medical identity theft- a type of healthcare fraud that includes both financial fraud and identity theft, it involves either the inappropriate or unauthorized misrepresentation of one’s identity, or the falsifying of claims for medical services in an attempt to obtain money

Minimum necessary- requires that 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; 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

Personal representative- person with legal authority to act on a patient’s behalf

Preemption- the principle that a statute at one level supersedes or is applied over the same or similar statute at a lower level

PHI- Protected Health Information;  any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity and identifiable to a patient

Red Flags Rule- consist of 5 categories; alerts, notifications, or warnings from a consumer reporting agency; suspicious documents; suspicious personally identifying information such as a suspicious address; unusual use of a covered account; and finally notices from customers about possible identity 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; providing, coordinating, or managing healthcare, obtaining premiums, billing, reimbursement, claims management and collection, case management and quality assessment.

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

Sale of information- prohibits a covered entity or BA from selling in exchange for an individual’s PHI without the individual’s consent

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.

   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>

 HIPAA has many requirements, which are all necessary to protect PHI. HIPAA strivs for openness and transparency when it comes to policies and procedures about privacy. HIPAA also wishes to put part of the decision making in the patients hand, decision on the collection, use, and disclosure of their identifiable health information.

4. Visit the State of Maine website.

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

 I had a hard time collecting laws that have to do with ownership of the health record in Maine, but I did find laws on retention, collection, and regulation of the health record. https://www1.maine.gov/sos/arc/records/local/healthrec.pdf

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

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

 The website above is the Department of Health and Human Services site for finding and comparing available health plans. The laws and regulations hospitals and health organizations must follow can also be found off a link on the home page, the site is also a platform for DHHS to discus their strategic plan for the health of America.

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

Many organizations do not understand the their compliance scope, they also put compliance before security.  They also do not conduct risk assessments. I had not previously thought of compliance before security because I believed they were one in the same. It is rather concerning that they put compliance over security. <http://www.healthcareitnews.com/sponsored-content/top-five-compliance-mistakes-healthcare-it>

<http://www.healthcareitnews.com/news/texas-hospital-hacked-affects-nearly-30000-patient-records> 30000 patient records were compromised after a hack. They have decided to ramp up their security following the incident. My question is why do people hack hospitals, they should be a safe place free from hacking attacks. I understand no social security numbers were compromised but is that what these hackers are always after?

7. Do you think there are problems with any of the HIPAA  Privacy rule's exceptions to the authorization requirement? No.

Do the exceptions minimize patient privacy? I do not believe so, I believe the patient has the maximum privacy while still being workable for the organization.

Are there too many exceptions? The only exception I would be concerned about is the business exception.

Are there other exceptions that you would include if you were asked to become involved in revising the law? I do not believe so, if there were anymore exceptions then it would not have much privacy.