1. 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 – As amended by HITECH, authorizes HHS to: (1) adopt standards for transactions and code sets that are used to exchange health data; (2) adopt standard identifiers for health plans, health care providers, employers, and individuals for use on standard transactions; and (3) adopt standards to protect the security and privacy of personally identifiable health information (45 CFR Parts 160, 162, and 164 2013)

ARRA – American Recovery and Reinvestment Act: The purposes of this act include the following: (1) To preserve and create jobs and promote economic recovery. (2) To assist those most impacted by the recession. (3) To provide investments needed to increase economic efficiency by spurring technological advances in science and health. (4) To invest in transportation, environmental protection, and other infrastructure that will provide long-term economic benefits. (5) To stabilize state and local government budgets, in order to minimize and avoid reductions in essential services and counterproductive state and local tax increased.

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 (45 CFR 164.402 2013)

BA – Business Associate: 1. 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 indentifiable health information. 2. 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, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services (45 CFR 160.103 2013)

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 (Public Law 90-174 1967)

Confidentiality – 1. 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, 2. As amended by HITECH, the practice that data or information is not made available or disclosed to unauthorized persons or processes (45 CFR 164.304 2013)

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

Consent – 1. A patient’s acknowledgement that he or she understands a proposed intervention, including that intervention’s risks, benefits, and alternatives, 2. The document signed by the patient that indicates agreement that protected health information (PHI) can be disclosed.

Covered entity – As amended by HITECH, (1) a health plan, (2) a health care clearinghouse, (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter (45 CFR 160.103 2013)

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 an individual; it is commonly used in research.

HHS – Department of Health and Human Services: The cabinet-level federal agency, and principal agency for protecting the health of all Americans and providing essential human services, especially for those who are at least able to help themselves.

DRS – Designated record set: As amended by HITECH: (1) A group of records maintained by or for a covered entity that is (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals (2) For purposes of this paragraph, the term means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity (45 CFR 164.501 2013)

E-discovery – Refers to Amendments to Federal Rules of Civil Procedure and Uniform Rules Relating to Discovery of Electronically Stored Information; wherein audit trails, the source code of the program, metadata, and any other electronic information that is not typically considered the legal health record is subject to motion for 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 (Public Law 97-462 1983)

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 Act: Legislation created to promote the adoption and meaningful use of health information technology in the United States. Subtitle D of the Act provides for additional privacy and security requirements that will develop and support electronic health information, facilitate information exchange, and strengthen monetary penalties. Signed into law on February 17, 2009, as part of ARRA (Public Law 111-5 2009)

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, and guarantees renewability of insurance to all employees regardless of size; requires covered entities (most healthcare providers and organizations) to transmit healthcare claims in a specific format and to develop, implement, and comply with the standards of the Privacy Rule and the Security Rule; and mandates that covered entities apply for and utilize national identifiers in HIPAA transactions (Public Law 104-191 1996)

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 – A type of healthcare fraud that includes both financial fraud and identity theft, it involves either (a) the inappropriate or unauthorized misrepresentation of one’s identity (for example, the use of one’s name and Social Security number) to obtain medical services or goods, or (b) 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. 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 patient’s behalf.

Preemption – In law, the principle that a statute at one level supersedes or is applied over the same or similar statute at a lower level (for example, the federal HIPAA privacy provisions trump the same or similar state law except when state law is more stringent)

PHI – Protected Health Information: As amended by HITECH, individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USC 1232g; (ii) in records described at 20 USC 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years (45 CFR 160.103 2013)

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: (1) alerts, notifications, or warnings from a consumer reporting agency; (2) suspicious documents; (3) suspicious personally identifying information such as a suspicious address; (4) unusual use of, or suspicious activity relating to, a covered account; (5) Notices from customers, victims of identity theft, law enforcement authorities, or other businesses 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: The Privacy Rule provides a number of exceptions for PHI that is 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, claims management, claims collection, review of the medical necessity of care, and utilization review; the Privacy Rule provides a broad list of activities 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 individual permits the recipient of the PHI to further exchange the PHI for compensation.

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. If a breach has been discovered, all affected persons must be notified without unreasonable delay but no more than 60 days. Affected persons must be notified using first class mail or a faster method if it is deemed there is an imminent misuse. For large-scale breaches, all persons are to be notified and the local media outlets are to be notified as well.

   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>

4. Visit the State of Maine website.

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

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

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

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/)

7. Do you think there are problems with any of the HIPAA  Privacy rule's exceptions to the authorization requirement? I personally do not believe there are any problems with the exceptions to authorization put in place.

Do the exceptions minimize patient privacy? I do believe the exceptions minimize privacy, however I feel the reasons for the exceptions trump a person’s privacy.

Are there too many exceptions? No

Are there other exceptions that you would include if you were asked to become involved in revising the law? No, I feel there are the correct amount of exceptions in place.