**Chapter 9**

**Data Privacy and Confidentiality**

*Laurie A. Rinehart-Thompson, JD, RHIA, CHP, FAHIMA*

**Real-World Case 9.1**

HIPAA privacy breaches are of great concern and they occur too frequently. In April 2015, Cornell Prescription Pharmacy (CPP) reached a settlement with OCR to pay $125,000 and implement a corrective action plan following the disposal of PHI pertaining to 1,610 patients in an unlocked container on the premises. The information had not been shredded. No policies and procedures had been implemented, and no training had been conducted (HHS 2015).

This case highlights the fact that simple nontechnical measures (for example, shredding or burning PHI) can avoid a breach. Further, the role of an effective privacy officer (in this case, to implement policies and procedures and provide workforce training) would have been to raise awareness among staff that likely would have prevented this incident from occurring.

The fact that CPP is a small pharmacy with a single location demonstrates that breaches and penalties resulting from breaches do not occur in large organizations only. Covered entities and business associates of all types and sizes can commit breaches and be penalized for them.

US Department of Health and Human Services. 2015. HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cornell/cornell-press-release.html.

# Real-World Case Discussion Questions

1. What steps could a privacy officer have taken to prevent this breach? A privacy officer could have ensured all parties involved were trained in the importance of safeguarding PHI when using it in day to day operations as well as the proper disposal of PHI. The privacy officer could also hold employees accountable once they are trained.

2. How would you have responded to it had it not been prevented at your organization? I would have determined to what level each person was trained and hold them accountable for what they have been trained on. If I found that there were any shortcomings with their training, I would ensure they have the training needed to avoid the breach from happening again.

3. Should small healthcare organizations be charged fines for non-compliance with HIPAA? Justify your response. I believe small healthcare organizations should be fined if they are found to be non-compliant with HIPAA. The fine assessed should be based on the degree of severity of the breach and not based on the size of the organization. Small organizations should not be exempt from fines as any breach, no matter how large or small is still a breach.

**Real-World Case 9.2**

Ronnie Bogle, a resident of San Jose, California, is a medical identity theft victim. He discovered this when he was rejected for a credit card application. He learned that he had multiple pages of unpaid medical treatments, emergency room visits, and hospital stays from around the country, none of which were his. Still battling hospitals over unpaid bills more than five years after he discovered that he was a victim of this crime, it is noted that the intertwining of the perpetrator’s and victim’s medical information makes it much more difficult to undo than simple financial identity theft cases. Further, because medical identity theft involves a person’s health profile, it cannot be quickly shut down as a credit card number can. In 2014, damages related to medical identity totaled $20 billion and affected 2.3 million Americans (Nguyen et al. 2014).

Nguyen, V., D. Paredes, and S. Pham. 2015 (March 30). 2.3 Million Americans Victims of Medical Identity theft. NBC Bay Area Investigative Unit. http://www.nbcbayarea.com/investigations/23-Million-Americans-Victims-of-Medical-Identity-298070211.html.

# Real-World Case Discussion Questions

1. What could Ronnie Bogle, or any of us, do to prevent becoming a victim of medical identity theft? Be in as much control of our PHI as possible under the law and only allow the release of this information to those that need to know.

2. Why should healthcare organizations be interested in financial identity theft? Because it may end up costing the healthcare organization a significant amount of money and employee time to investigate the cases of identity theft.

3. What impact might medical identity theft have on the patient’s care? If the fake health information intertwines with the real care the patient is receiving there is a chance that the patient may be treated for something they do not have and put the patient in harms way.

# Application Exercises

*Instructions:* Answer the following questions.

1. Who would you include on a steering committee that is responsible for ongoing HIPAA privacy compliance, particularly in light of the ARRA privacy provisions? Who should lead this committee?

2. What type of ongoing educational activities would you provide for your organization’s workforce to facilitate compliance with the HIPAA Privacy Rule and the ARRA privacy provisions? How would you implement these activities?

3. What criteria would you use to determine whether an incident is a security breach that workforce members should report per the ARRA requirements? What types of notification to individuals would you recommend? Would the method of notification vary based on the nature of the breach?

4. What process would you use to update policies and procedures? How frequently would you update them? How would you ensure that they continue to be valid and compliant with HIPAA, including ARRA provisions?

**Review Quiz**

*Instructions:* For each item, complete the statement correctly or choose the most appropriate answer.

1. Which of the following is true of the Health Insurance Portability and Accountability Act (HIPAA)?

 a. Provides a federal floor for healthcare privacy

 b. Duplicates state laws

 c. Does not need to be followed if it is not feasible to do so

 d. Duplicates Joint Commission standards

2. Under the HIPAA Privacy Rule, which of the following is a covered entity category?

 a. Business associate

 b. Healthcare clearinghouse

 c. Physician office

 d. Document disposal company

3. Under the HIPAA Privacy Rule, an impermissible use or disclosure should be presumed to be a breach unless the covered entity or business associate demonstrates that the probability the PHI has been compromised is \_\_\_\_\_\_\_\_\_\_\_.

 a. High

 b. Moderate

 c. Low

 d. Non-existent

4. Under usual circumstances, a covered entity must act on a patient’s request to review or copy his or her health information within what time frame?

 a. 10 days

 b. 20 days

 c. 30 days

 d. 60 days

5. The HIPAA Privacy Rule requires that covered entities limit use, access, and disclosure of PHI to the least amount necessary to accomplish the intended purpose. What concept is this?

 a. Minimum necessary

 b. Notice of privacy practice

 c. Authorization

 d. Consent

6. Which of the following should be included in a covered entity’s notice of privacy practices?

 a. Description with one example of disclosures made for treatment purposes

b. Description of one other purposes for which a covered entity is permitted or required to disclose PHI without consent or authorization

 c. Statement of the healthcare organization’s rights

 d. Patient’s signature and e-mail address

7. Which of the following is true of the notice of privacy practices?

 a. It must be made available at the corporate headquarters

 b. It must be posted in a prominent place

 c. Its content cannot be changed

 d. It cannot be posted on the website

8. Which of the following statements is true?

 a. An authorization must contain an expiration date or event

 b. A consent for use and disclosure of information must be obtained from every patient.

 c. An authorization must be obtained for uses and disclosures for treatment, payment, and operations.

 d. A notice of privacy practices must give tenexamples of a use or disclosure for healthcare operations.

9. In which of the following instances must patient authorization be obtained prior to disclosure?

 a. To an insurance company for payment

 b. To the patient’s attorney

 c. To public health authorities as required by law

 d. To another provider for treatment

10. Which of the following is true about a facility’s patient directory?

 a. A written authorization from the patient is required before any information about the patient is placed in a facility directory.

 b. Only the patient’s name may be placed in a facility directory.

 c. The covered entity must inform the individual of the information to

 be included in the facility directory.

 d. Because this is considered a normal hospital operation, an individual may not prohibit his or her inclusion in the directory.

11. Which of the following statements about a business associate agreement is true?

 a. It allows the business associate to use or disclose PHI for any purpose.

b. It allows the business associate to maintain PHI indefinitely after termination of the contract.

 c. It allows the business associate to use or disclose PHI in limited ways.

 d. It requires the business associate to make available records relating to PHI use and disclosure to the HHS.

12. How many days does a covered entity have to respond to an individual’s request for access to his or her PHI when the PHI is stored off-site?

 a. 10 days beyond the original requirement

 b. 30 days

 c. 60 days

 d. 90 days

13. Which of the following statements is true of the notice of privacy practices?

 a. It gives the covered entity permission to use information for treatment purposes.

 b. It must be provided to every individual at the first time of contact or service with the covered entity.

 c. It must be provided to the individual by the covered entity within 10 days after receipt of treatment or service.

 d. It serves the same purpose as the authorization.

14. Which of the following statements about a facility directory of patients is true?

 a. Disclosures from the directory need not be included in an accounting

 of disclosures.

 b. Individuals must provide a written authorization before information can be placed in the directory.

 c. The directory must contain only the patient’s name and birth date.

 d. The directory may contain diagnostic information as long as it is kept confidential.

15. In which of the following situations can PHI be disclosed without authorization, as long as there was an opportunity for the individual to agree or object?

 a. Disclosures for public health purposes

 b. Disclosures to health oversight agencies

 c. Disclosures regarding decedents

 d. Facility directory disclosures

16. Who of the following would be considered a member of a hospital’s workforce?

a. A clerk working in the hospital’s registration office

b. A lawn care service for the hospital grounds

c. An employee of a company that picks up laundry from the hospital every day

d. An employee of one of the hospital’s business associates who is on the hospital premises occasionally

17. When would PHI loses its status?

a. If health information is not identified by the person’s name

b. After an individual has been deceased more than 50 years

c. When it is being used for research

d. When it is is in the hands of a business associate

18. A covered entity may deny an individual’s amendment request for which of the following reasons?

a. If the PHI in question is not part of the designated record set

b. If the PHI in question was created by the covered entity and therefore cannot be amended

c. If the PHI in question cannot be amended in an electronic health record

d. If the PHI in question was created over a year ago

19. Which of the following is a public interest and benefit exception to the authorization requirement?

a. Treatment, payment and operations

b. Facility directory

c. Notification of relatives and friends

d. Judicial and administrative proceedings

20. The breach notification requirement applies to:

a. All PHI

b. Unsecured PHI only

c. Electronic PHI only

d. PHI on paper only

21. A subpoena should be accompanied by which of the following?

a. Patient authorization

b. Patient consent

c. Court order

d. Interrogatory

 22. In court, hearsay is generally \_\_\_\_\_\_\_\_\_\_\_\_.

a. Non-admissible

b. A key component of the decision making process

c. Admissible

d. e-discovery

23. The American Recovery and Reinvestment Act expanded the definition of business associates to include which of the following?

a. Consultants

b. Billing companies

c. Patient safety organizations

d. Transcription companies

24. Critique this statement: According to HIPAA, workforce members include students.

a. This is a true statement

b. This is a false statement as students are not employees in the organization

c. This is a false statement as workforce includes employees only

d. This is a false statements as the workforce includes employees and physicians only

25. The designated record set includes which of the following?

a. Strategic plan

b. Policies and procedures

c. Audits

d. Billing records