**Chapter 10**

**Data Security**

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

**Real-World Case 10.1**

In 2014, the Department of Health and Human Services reported on its website a $4.8 million HIPAA settlement with New York and Presbyterian Hospital (NYP) and Columbia University following the 2010 breach of thousands of patients’ e-PHI. A Columbia University physician, who was an attending physician at NYP, tried to deactivate a computer server that he owned on the network that contained NYP patient e-PHI. The e-PHI became accessible to the public on Internet search engines because technical safeguards were lacking. A patient’s loved one found e-PHI about the patient on the Internet and filed a complaint.

In addition to the impermissible disclosure, both entities were noncompliant in other ways: (1) no attempts had been made to assure the server was secure; (2) a thorough risk analysis had never been completed that identified all systems able to access the e-PHI of NYP patients and therefore no plan to address potential threats and hazards existed; (3) no appropriate policies and procedures existed regarding authorizing access to its databases; and (4) they did not follow their own policies on information access management (HHS 2014).

This costly mistake, both monetarily and from a reputation standpoint, highlights the negative outcomes that can happen when both technical and administrative safeguards are not followed. It also emphasizes the importance of inventorying all systems and devices that can access an organization’s e-PHI to address threats and an organization’s vulnerabilities. This is not an easy task given the number of personal and mobile devices that access e-PHI, but it is critical.

US Department of Health and Human Services (HHS). 2014 (May 7). Data Breach Results in $4.8 million HIPAA Settlements. http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

# Real-World Case Discussion Questions

1. A risk analysis should include an inventory of all systems and devices that can access an organization’s ePHI (in this case, the breach occurred via a physician’s personal computer server). How can an organization account for all systems and devices on which PHI may be accessed or otherwise present?

An organization can account for all systems and devices on which PHI may be accessed by using computer software specific only to hospital provided technology. This would work similarly to how an iPad can be locked when away from it’s designated use location.

2. What should the risk analysis include?

 The risk analysis should include a complete review of the system, and its machines. Focusing on any discrepancies in computer access.

3. Should the physician have been the one to deactivate the server? Why or why not? The physician should not have been the one to deactivate the server, as they most likely had no prior knowledge of the workings of the computer server.

**Real-World Case 10.2**

Riverside Health System in Virginia announced in 2014 that the e-PHI of nearly 1,000 patients was breached by a nurse who accessed Social Security numbers and EHRs. The violation was discovered during a random organizational audit. Riverside described its compliance program as robust with ongoing monitoring (McCann 2014). This case raises numerous issues; for example, the fact that humans present one of the greatest threats to data security. When this human threat is internal to the organization, it is heightened by the ability to access information in the course of doing business. The article did not describe what type of access was given to employees; however, a nurse role is likely to result in broad access. The inappropriate access had occurred over a four-year period, which raises the issue of monitoring adequacy. Nonetheless, monitoring was taking place. The nurse was terminated after the breach was discovered. When the perpetrator of the breach was identified, all electronic access for that person should have been terminated immediately as well.

McCann, E. 2014 (January 2). 4-Year Long HIPAA Breach Uncovered. HealthITNews. http://www.healthcareitnews.com/news/four-year-long-hipaa-data-breach-discovered.

# Real-World Case Discussion Questions

1. What red flags does this case raise?

The biggest red flag the case raises is how often hospitals actually check/monitor ePHI privacy and adequacy. If this breach continued for four years then there must not have been reviews of the system. A major breach like this would have been picked up by even a small review.

2. How would you have avoided this breach?

To avoid this breach I would have instituted at least a yearly full review of the system, and a monthly check on high risk areas.

3. Alternatively, given limited human resources that most organizations have to conduct audits, is it realistic to conclude that monitoring truly was robust and this breach still occurred, undetected? PHI is so important that even limited human resources should not have stopped organizations from auditing their system. This breach continued to occur undetected from lack of monitoring guidelines.

# Application Exercises

*Instructions:* Answer the following questions.

1. Search the Internet for news about security breaches in healthcare and other industries in the last three years. Make a summary of each case. Identify the principal threats in each of these cases and what could have been done to minimize the threats.

Maine General experienced a cyber attack, information including dates of birth and emergency contact names, addresses, and telephone numbers for certain patients and employees had been released to an external website. To minimize threats they could have a monthly scan of their PHI system.

Muhlenberg Community Hospital in Kentucky experienced a breach from a keystroke logger, which is a virus that sends of any information you type on the infected computer. The virus may have been in place since 2012. Information entered on infected computers were patient financial data and health information, potentially even more. This hospital could have at least done a yearly system scan, maybe even change their computers.

2. Search the Internet for as many sites as you can that are concerned with health information privacy and security. Make a list of the sites and provide a two- or three-sentence description of each. What are the biggest security concerns expressed on each site? Share and compare the sites during a classroom session with your classmates.

<http://www.healthcareitnews.com/> Is a site concerned with sharing the most up to date information with everyone on breaches that have occurred, are occurring, or may occur.

<http://www.healthcareinfosecurity.com/> This website has information on how to better protect your organization, train employees, and news on previous breaches.

<http://www.himss.org/library/healthcare-privacy-security> Gives you the tools to learn basic cyber security skills.

3. View the security breaches affecting 500 or more individuals posted on the Office for Civil Rights website at <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>. Instruct the students to categorize the breaches by type and location of breached information. Are most large breaches intentional or negligent? What medium presents the greatest risk for a breach? Have the students select three cases and list ways (using HIPAA security rule requirements and news articles about the breaches) that these breaches might have been avoided.

Most large breaches are negligent on the organizations side but intentional on the thieves side. People raid PHI so they can sell identities, which is so very confusing. Why sell an identity when you can apply for legal residence? Buying an identity is just a person asking to be deported.

4. Inventory the security policies of a healthcare organization in your area. Use the following table to help organize your inventory. Share your inventory during a class session or in a class presentation with your classmates. Compare and contrast how these policies meet HIPAA security provisions.

|  |  |  |
| --- | --- | --- |
| **Policy name and** **date of policy** | **Summary of policy** | **Complies with which HIPAA sections** |
|  |  |  |
|  |  |  |

**Review Quiz**

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

1. Data security includes protecting data availability, privacy, and \_\_\_\_\_\_\_\_.

 a. Suitability

 b. Integrity

 c. Flexibility

 d. Quality

2. Within the context of data security, protecting data privacy means defending or safeguarding \_\_\_\_\_\_\_\_\_.

 a. Access to information

 b. Data availability

 c. Health record quality

 d. System implementation

3. The greatest threat category to electronic health information is which of the following?

 a. Natural disasters

 b. Power surges

 c. Hardware malfunctions

 d. Humans

4. The first and most fundamental strategy for minimizing security threats is which of the following?

 a. Establish access controls

 b. Implement an employee security awareness program

 c. Establish a secure organization

 d. Conduct a risk analysis

5. Administrative safeguards include policies and procedures that address which of the following regarding computer resources?

 a. Management

 b. Maintenance

 c. Modification

 d. Manipulation

6. The individual responsible for ensuring that everyone follows the organization’s data security policies and procedures is which of the following?

 a. Chief executive officer

 b. Chief information officer

 c. Chief privacy officer

 d. Chief security officer

7. An employee accesses PHI on a computer system that does not relate to her job functions. What security mechanism should have been implemented to minimize this security breach?

 a. Access controls

 b. Audit controls

 c. Contingency controls

 d. Security incident controls

8. A visitor to the hospital looks at the screen of the admitting clerk’s computer workstation when she leaves her desk to copy some admitting documents. What security mechanism would best have minimized this security breach?

 a. Access controls

 b. Audit controls

 c. Automatic logoff controls

 d. Device and media controls

9. A laboratory employee forgot his user ID badge at home and uses another lab employee’s badge to access the computer system. What controls should have been in place to minimize this security breach?

 a. Access controls

 b. Security incident procedures

 c. Security management process

 d. Workforce security awareness training

10. A dietary department donated its old microcomputer to a school. Some old patient data were still on the microcomputer. What controls would have minimized this security breach?

 a. Access controls

 b. Device and media controls

 c. Facility access controls

 d. Workstation controls

11. HIPAA requires that policies and procedures be maintained for a minimum of \_\_\_\_\_\_\_.

a. Seven years

b. Six years from date of creation

c. Six years from date of creation or date when last in effect, whichever is later

d. Seven years from date when last in effect

12. A visitor walks through the computer department and picks up a CD from an employee’s desk. What security controls should have been implemented to prevent this security breach?

 a. Device and media controls

 b. Facility access controls

 c. Workstation use controls

 d. Workstation security controls

13. Threats to data security are most likely to come from which of the following?

 a. Employees

 b. Natural disasters

 c. Compromised firewalls

 d. Hackers outside an organization

14. These are automatic checks that help preserve data confidentiality and integrity.

 a. Access controls

 b. Audit controls

 c. Application controls

 d. Incident controls

15. An employee in the physical therapy department arrives early every morning to snoop through the EHR for potential information about neighbors and friends. What security mechanism should have been implemented that could minimize this security breach?

 a. Audit controls

 b. Facility access controls

 c. Facility access controls

 d. Workstation security

16. An employee observes an outside individual putting some computer disks in her purse. The employee does not report this security breach. What security measures should have been in place to minimize this threat?

 a. Access controls

 b. Audit controls

 c. Authentication controls

 d. Security incident procedures

17. Locks on computer room doors illustrate a type of \_\_\_\_\_\_\_\_\_.

 a. Access control

 b. Workstation control

 c. Physical control

 d. Security breach

18. An admission coordinator consistently enters the wrong patient gender while entering data in the MPI. What security measures should be in place to minimize this security breach?

 a. Access controls

 b. Audit trail

 c. Edit checks

 d. Password controls

19. Which of the following statements is true regarding HIPAA security?

a. All institutions must implement the same security measures.

b. HIPAA allows flexibility in the way an institution implements the security standards.

c. All institutions must implement all HIPAA implementation specifications.

d. A security risk assessment must be performed every year.

20. For HIPAA implementation specifications that are addressable, the covered entity \_\_\_\_\_\_\_\_\_.

a. Implements the specification

b. May choose not to implement the specification if it is too costly to execute

c. Must conduct a risk assessment to determine if the specification is appropriate to its environment

d. Does not have to implement the specification if it is a small hospital

21. A user recently opened a file that they thought would help them with their job but it copied files to unsecure ares of the computer. What thpe of malware was activated?

a. Rootkit

b. Computer virus

c. Computer work

d. Trojan horse

22. Training that educates employees on the confidential nature of PHI is known as which of the following?

a. Awareness

b. Risk

c. Incident

d. Safeguard

23. “Something you have” is demonstrated by:

a. CAPTCHA

b. Retinal scan

c. Password

d. Token

24. Policies are which type of safeguards?

a. Technical

b. Application

c. Administrative

d. Network

25. A hospital is looking to use something to act as a buffer between two networks. What should be recommended?

a. Application control

b. Cryptography

c. Firewall

d. Digital certificate