**Anita Hakala-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?

***Risk Management encompasses the identification, evaluation, and control of risks that are nherent in unexpected and inappropriate events. Must take steps to prevent, detect, and mitigate both internal and external incidents.***

2. What should the risk analysis include?

***Risk analysis should:***

***Identify security threats***

***Identify vulnerability (weakness in operations)***

***Determination of how likely it is that any given threat may occur and estimate its impact***

***Identify how e-PHI is created, managed, stored and transmitted within and outside the***

***organization***

***Make a likelihood determination- an estimate of the probability of the threats occurring***

***Impact analysis-what the impact of the threats on information may be***

3. Should the physician have been the one to deactivate the server? Why or why not?

***No. IT experts have thorough knowledge of how information is managed and should be the only personnel to do the deactivation***

**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?

***Robust monitoring over a four-year period should have better alert, notifications or warnings of unusual use or suspicious activity relating to a covered account. Although, in my job, I have access to all that information on a routine basis and even share the information with business partners and can see how it may be very difficult to find this in a shorter period of time. Maybe healthcare should be more like the banking industry, who mandates that employees with a lot of access take two weeks of vacation together at least once a year, and take that time to review changes that may occur or not occur during that employees’ absence.***

2. How would you have avoided this breach?

***More frequent audit and making sure the user needs access to that specific information***

***before providing access.***

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?

***Yes, that is a definite possibility, if it was Monitoring only. Again they maybe should look at access.***

# 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.

**1. Anthem**

**80 Million Records Compromised**

The largest healthcare breach to date affected [Anthem](https://www.bitsighttech.com/blog/anthem-continuously-monitoring-information-security), the second largest health insurer in the U.S. In late January 2015, the medical insurance provider began notifying 80 million individuals that their personal information was compromised in a December 2014 cyber attack.

They [noted that the hackers may have accessed](https://www.anthemfacts.com/) “names, dates of birth, social security numbers, healthcare ID numbers, home addresses, email addresses, and employment information, including income data” and did not believe medical or credit card information was released. After the breach, Anthem [set up a website](https://www.anthemfacts.com/) where affected customers could learn about their credit monitoring services and identity theft repair.

Anthem has been [notoriously secretive about their cybersecurity](http://www.csoonline.com/article/2893668/data-breach/anthem-accused-of-avoiding-further-embarrassment-by-refusing-audit.html), leading some to suggest that the company’s lack of transparency was an attempt to avoid further embarrassment. Several months after their breach was brought to light, they refused a request for an audit, noting that performing an audit would require them to disable their anti-virus software, which could cause outages within their IT system. This was especially troubling as Anthem insured many government employees and thus had a business relationship established**. Very difficult to tell in this case what may have caused the breach**

**2. Premera**

**11 Million Records Compromised**

In March of 2015, Premera—a large medical insurance company—revealed that a hacker had accessed their network, compromising the data of 11 million individuals. The company didn’t expound on how the hacker accessed the information, but it [did disclose that they might have accessed](http://money.cnn.com/2015/03/17/technology/security/premera-hack/) “social security numbers, birthdays, emails, physical addresses, bank account information, clinical information and detailed insurance claims” to both past and present customers, dating back to 2002. A [Premera web page](https://www.premera.com/wa/visitor/about-the-cyberattack/?WT.z_ref=krebsonsecurity.com/tag/fireeye/&WT.z_redirect=www.premera.com/cyberattack/" \t "_blank) set up to release information about the breach stated that the company learned of the breach in January of 2015, but that the original breach had actually taken place nine months earlier, in May of 2014. **Very difficult to tell in this case what may have caused the breach**

**3. TRICARE (Via Science Applications International Corporation)**

**4.9 Million Records Compromised**

This 2011 breach was unique for many reasons. [According to Reuters](http://www.reuters.com/article/us-data-breach-texas-idUSTRE78S5JG20110929), an employee for one of TRICARE’s vendors— Science Application International Corporation (now Leidos Holdings Inc.)—was transporting backup tapes that included electronic healthcare data for TRICARE’s patients when the employee’s vehicle was broken into and robbed. Those tapes were among the items that the robber stole, but investigators didn’t believe the thief was after the tapes—or even knew what they were. In 2014, [federal judges closed out all but two lawsuits](http://www.bizjournals.com/washington/blog/fedbiz_daily/2014/05/computer-tape-theft-exposing-personal-info-of-5.html) that formed after the breach, citing that “the mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.” **An employee carrying tapes in their car??? Why and where to and why were they left in a car??? Seems like a simple fix is instituting a policy on how and when back-up tapes get to their destination. Data transmission may actually be safer.**

**4. Community Health Systems**

**4.5 Million Records Compromised**

In August 2014, Community Health Systems—which owns and operates over 200 hospitals across the U.S.—reported a massive cyberattack that compromised the records of over 4.5 million patients. According to [InformationWeek](http://www.informationweek.com/healthcare/security-and-privacy/what-healthcare-can-learn-from-chs-data-breach/a/d-id/1317696), the information, which included “patient names, addresses, birthdates, telephone numbers, and social security numbers,” was gathered as a result of an exploited SSL vulnerability, Heartbleed. Interestingly, cybersecurity analysts have [speculated that this breach and the Anthem breach were linked](http://www.forbes.com/sites/danmunro/2015/02/10/are-the-data-breaches-at-anthem-and-chs-linked/#77ab38702161). **I don’t think there is any way to prevent cyber attacks in some cases. There are a lot of people in the world that thrive on their computer abilities to compromise information. It seems that a risk assessment in all of these case may be helpful in analysing if and where there may be a breakdown in their organizational framework.**

**5. Banner Health**

**3.7 Million Records Compromised**

[A data breach affecting up to 3.7 million individuals at Banner Health](http://www.infosecurity-magazine.com/news/37-million-people-hit-in-massive/) was disclosed in early August 2016. The data compromised included patient and physician names, addresses, social security numbers, clinical information, and health insurance information. It is believed that payment data used at vending machines and other food and beverage outlets was compromised as well. It is still unclear how attackers gained unauthorized access to Banner Health's servers and computer systems. **Inclusion of their vendors in the business contracts. This is interesting, I wonder if organizations include such vendors and why are they linked to the secure hospital servers and not another type of server.**

**6. Mass General Hospital**

**4,300 Records Compromised**

In late May 2016, [Mass General Hospital (MGH) announced](https://threatpost.com/massachusetts-general-hospital-confirms-third-party-breach/119000/) that 4,300 dental patient records were stolen. According to MGH, these records were not stored on their systems, but instead stolen from the network of a third-party vendor—Patterson Dental Supply Inc. (PDSI)—that assists the hospital in managing dental patients at several practices. The records stolen from PDSI included names, dates of birth, social security numbers, dental provider information, medical record numbers, and dental appointment information of MGH patients. **A risk analysis on vendors should also be included in the organizations analysis of themselves.**

**7. Prosthetic & Orthotic Care Inc.**

**Unknown Number Of Records Compromised**

Prosthetic & Orthotic Care Inc. (P&O Care) recently announced a data breach that resulted in the exposure of critical patient information. The records exposed included personally identifiable information (PII) and [personal health information (PHI)](http://www.healio.com/orthotics-prosthetics/industry-news/news/online/%7Beb153c63-279d-46d1-98b4-2866abadfcf4%7D/prosthetic-and-orthotic-care-inc-issues-notification-of-data-breach), such as names, contact information, patient identification numbers, diagnostic codes, appointment dates, billing amounts, social security numbers, birth dates, insurance providers, and photos of procedures. It has been reported that records were dumped in plain text on Pastebin.

The P&O Care breach occurred after a hacker exploited a zero-day flaw—or [an issue unknown to the vendor](http://www.pctools.com/security-news/zero-day-vulnerability/)—within software the company had recently purchased. **A risk analysis on vendors should also be included in the organizations analysis of themselves.**

**Steps Healthcare Organizations Should Take To Mitigate Cyber Risk**

Healthcare organizations typically outsource a great deal of their technology. But with cyber risks constantly evolving, the vendor selection process has become extremely important. With confidential patient records at risk, healthcare companies cannot simply outsource services or make purchases based on the lowest bidder—cybersecurity also needs to be an important deciding factor.

There are a few steps you can take to mitigate the cyber risk your healthcare organization faces from third parties:

1. **Know the security performance of the vendors you work with already.** Many healthcare providers tend to rely on software provided by third parties and, as a result, are often playing catch-up when vulnerabilities emerge in software they have already purchased and implemented. This can leave your healthcare organization in a bad place when it comes to potential security breaches.
2. **Make sure you’ve done your due diligence during the selection stage of your products or services.** Knowing how well your prospective vendors handle security is imperative for the selection process. These vendor security assessments can help organizations evaluate potential partners and identify third party risk before they become problematic.
3. Once you've chosen a vendor to work with:
   * **Monitor their security performance in real time** to be alerted of any security incidents that may affect your organization.
   * **Ensure that any third-party software you're running is up-to-date**, and stay on top of all emerging vulnerabilities.
   * **Make sure your third parties and your internal security teams patch vulnerabilities quickly** to reduce the chance of infection and data loss. No matter what safeguards you put in place, vulnerabilities *will* affect your network or the services you’re running—it’s inevitable.

**What To Keep In Mind**

**There’s nothing fundamentally different about how breaches happen in the healthcare sector.** A cybersecurity incident takes place for one of three reasons:

1. Because of someone on the outside—like a phishing scam where someone is sent an embedded piece of malicious code in an email.
2. Through a trusted insider—who chooses to exploit their privilege of data or intellectual property.
3. Through an attack to your supply chain—when someone can manipulate the hardware or software your company uses to gain access to an infrastructure or network.

But just because these attacks aren’t unique to healthcare providers doesn’t mean they don’t hold unique consequences. In a recent [USA Today article](http://www.usatoday.com/story/money/2015/04/14/hacking-health-data-privacy/25597337/), Ann Patterson, the senior vice president and program director for the Medical Identity Fraud Alliance, spoke about how these types of breaches could be far worse than credit card breaches: "You really can't change your birth date. So when that kind of [personally identifiable] information is out there, the type of fraud that is perpetrated in the healthcare sense involves your well being, your life."

Retrieved from the internet <https://www.bitsighttech.com/blog/security-breaches-healthcare>

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.

I think that Privacy and security are the two biggest areas that all of these websites have information about. Some offer the how and why of making complaints, educational resources, and laws and rules pertaining to PHI.

|  |  |
| --- | --- |
| Site | Comment |
| <https://www.healthit.gov/providers-professionals/ehr-privacy-security>  Integrating Privacy & Security Into Your Medical Practice  Security Risk Assessment  Privacy & Security and Meaningful Use  Mobile Devices Privacy and Security |  |
| [www.ahima.org/topics/psc](http://www.ahima.org/topics/psc)  Privacy  Security  HITECH Omnibus Rule |  |
| healthinformatics.uic.edu  Privacy  Confidentiality  Security |  |
| <https://www.hhs.gov/hipaa/>  HIPAA for Individuals  HIPAA for Professionals  How to File a complaint |  |
| [www.health-law.com/practices-Health-Information-Privacy-Security.html](http://www.health-law.com/practices-Health-Information-Privacy-Security.html)  Health Information Privacy  Health Information Security |  |
| <https://www.ncbi.nlm.nih.gov>  retrieval of article pertaining to health information and security |  |

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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Vascular Surgical Associates | GA | Healthcare Provider | 36496 | 11/10/2016 | Hacking/IT Incident | Network Server |

**Network Safeguards: The use of firewalls, cryptographic technologies, encryption, digital signatures, digital certificates, web security protocols and intrusion detection systems are all ways that should/could be implemented to secure the network server.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lister Healthcare | AL | Healthcare Provider | 1349 | 11/09/2016 | Theft | Laptop |

**Security awareness and training, workstation use, workstation security, access controls for laptop information, actually the technical safeguard that are required should include all laptops too.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Anthem, Inc. | IN | Health Plan | 3525 | 10/26/2016 | Unauthorized Access/Disclosure | Email |

**Security awareness and training, information access management, access controls, integrity, transmission security.**

**Hacking/IT incident and theft are the top two types of breaches according to** <https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php>

**With a huge increase of hacking/IT incident over the past year. I am curious how come they did not breakdown the hacking/IT incident into two separate categories; maybe it is difficult to know which is which. It makes me wonder if the IT employees that are being hired have the appropriate amount of education and experience necessary in the ever-changing technology of the world.**

| **2010** | **2011** | **2012** | **2013** | **2014** | **2015** |
| --- | --- | --- | --- | --- | --- |
| Note: Each count above is the total number of individuals affected by a breach of the specific information source and the breach type. Individual reports of a breach may involve one or more information sources, i.e. laptop, e-mail, etc, and one or more breach types, i.e. theft, loss, etc. In those cases, there may be double-counting of the number of affected individuals or reported breaches in a specific year. | | | | | | |
| Source: U.S. Department of Health and Human Services (HHS) Office for Civil Rights. Breaches Affecting 500 or More Individuals. February 1, 2016. | | | | | | |
| Type of Information Breach | | | | | | |
| **Hacking/IT incident** | 568,358 | 297,269 | 900,684 | 236,897 | 1,786,630 | 111,812,172Of this total, 78M individuals (70%) were affected by a singular hacking/IT incident, and 5 of the 51 hacking/IT incidents affected 97% of all individuals |
| **Improper disposal** | 34,587 | 63,948 | 21,329 | 526,538 | 93,612 | 82,421 |
| **Loss** | 924,909 | 6,019,578 | 95,815 | 142,411 | 243,376 | 47,214 |
| **Theft** | 3,691,460 | 4,720,129 | 927,909 | 5,397,989 | 7,058,678 | 740,598 |
| **Unauthorized access/disclosure** | 130,106 | 118,444 | 338,767 | 383,759 | 3,019,284 | 572,919 |
| **Other breach** | 158,593 | 13,981 | 503,900 | 254,305 | 413,878 | -- |

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** |
| Applications and Data Criticality Analysis Policy  2014 | The purpose is to assess the relative criticality of specific applications and data in support of other contingency planning activities. The applications and data identified as “critical” will be the focus of contingency plans and will be prioritized first for recovery in a disaster. | Somewhat of a  risk analysis |
| Assigned Security Responsibility Policy  2014 | Responsibilities of the IT Security Officer include (but are not limited to):   * Develop policies, procedures and plans required to adequately protect the confidentiality, integrity and availability of systems and data * Ensure all computer-related policies, procedures, and plans required by regulations and law are developed, implemented, and maintained * Monitor changes in legislation that may affect the organization and its security position * Monitor changes and advances in technology that may affect the organization and its security position * Perform technical and non-technical evaluations or audits on security systems and processes in order to find and correct weaknesses and guard against potential threats * Act as an internal consultant and external spokesperson for r the organization elated to security * Ensure that a system for reporting and responding to security incidents is in place and functioning * Deliver, or coordinate, on an ongoing basis, security awareness training to all members of the workforce * The purpose of this policy is to identify the security official who is responsible for the development and implementation of the policies and procedures required to maintain the confidentiality, integrity and availability the organization information systems and support compliance with all applicable laws and regulations including the HIPAA Security Rule. | Assigned Security Responsibility |
| Person or Entity Authentication  2014 | the organization will evaluate the adequacy of authentication mechanisms as part of the Risk Analysis and may make changes to this policy or the Password Management policy. The purpose is to implement procedures to verify that the person or entity seeking access to the organization systems containing confidential or privileged information is the one claimed. | Person or Entity authentication |
| Backup Prior to Significant Changes  2014 | The purpose is to protect the availability of critical data, including ePHI by creating a retrievable, exact copy of critical data, before significant changes that could put the data at risk, including equipment and software upgrades and equipment moves. | Contingency Plan |
| Business Associate Contracts Policy  2014 | The purpose is to obtain from business associate whose work may involve access to electronic protected health information (ePHI) satisfactory assurances that they will appropriately safeguard the Confidentiality, Integrity and Availability of the information and comply with the HIPAA and other applicable laws. | Organizational Business or associate contract |
| Computer Audit Controls  2014 | The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use confidential information, including ePHI. | Audit Controls |
| Computer Security Incident Policy  No date | The purpose is to establish the policy and procedures to address security incidents.  CMHC will create policies, procedures, tools and workforce education to support timely, effective response to security incidents including violations of security policy, and any events that threaten the confidentiality, integrity or availability of the organization systems and information.  The policies and procedures will support timely effective response to security incidents, the prompt mitigation of the effect of those security incidents, the ability to track and trend security incidents and the ability to use data about security incidents to make improvements to organizational security. | Security Incident Procedures |
| Data Integrity  2014 | The purpose is to implement policies and procedures to protect information, especially critical information, from improper alteration or destruction. | Integrity |
| Disaster Recovery  2014 | The purpose is to establish and implement as needed procedures to restore any loss of data or access to data. | Contingency Plan |
| Emergency Mode Operation  2014 | The purpose is to ensure that when the organization is operating in emergency mode (such as in a power outage or other emergency or disaster) security processes to protect confidential information including ePHI are maintained. | Contingency Plan |
| Encryption – Decryption of Media & Stored Data Policy  2014 | The purpose is set policy regarding the use of encryption technology to protect the confidentiality of the organization data that is confidential or privileged including ePHI and other PII. | Transmission Security |
| Facility Access Controls  2014 | The purpose is to provide needed safeguards to protect the confidentiality of the organizations information by implementing policies and procedures to limit physical access to the organization’s computer systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. | Facility Access Controls |
| HIPAA Security Compliance Evaluation Policy  2014 | The purpose is to perform a technical and non-technical evaluation of the organizations compliance with the HIPAA security regulations and any additional security standards or regulations that the organization is obligated to meet. | Evaluation |
|  |  |  |
| Information Security Program Policy  2014 | The purpose of the organization’s Information Security Program is to provide reasonable and appropriate safeguards to ensure the   * Confidentiality * Integrity * Availability   of the organization data and systems by protecting the data and systems from unauthorized access, modification, destruction, or disclosure | Security Management Process |
| Information System Activity Review  2014 | The purpose is to identify and report security incidents by regularly reviewing (auditing) records of information system activity, such as audit logs, access reports, and security incident tracking reports.  Audits may be conducted to:   * Ensure confidentiality, integrity, and availability of confidential information * Investigate possible security incidents and ensure conformance to the organization security policies * Monitor user or system activity where appropriate | Audit Controls |
| Log-In Monitoring Policy  2014 | The purpose is to implement procedures for monitoring log-in attempts and reporting discrepancies. | Audit |
| Protection from Malicious Software  2014 | deploy effective protection against malicious software on all technology platforms that present significant vulnerabilities and for which there are threats.  the organization will deploy updates to all software used to provide protection.  the organization conducts security training | Security Training |
| Password Management  2014 | The purpose is to implement procedures for creating, changing and safeguarding passwords and train users on the procedures. | Access Control |
| IT Policies and Procedures Standards  2014 | to ensure compliance with the standards, implementation specifications and other requirements of state and federal regulations, including the HIPAA Security regulations. | Security Management Process |
| Risk Analysis Policy  2014 | the organization will conduct an accurate and thorough assessment of the vulnerabilities and risks to the confidentiality, integrity, and availability of critical systems and confidential information (including ePHI) held by the organization  The approach taken to Risk Analysis (also known as a risk assessment or security assessment) is to be guided by best practices such as those in the NIST standards or HIPAA Security guidance (see the reference section of this policy). | Strategic for minimizing security threats |
| Security Awareness and Training  2014 | The purpose is to implement a security awareness and training program for all members of the organization’s workforce, including management. Without a knowledgeable workforce compliance with good security practices is not possible. | Security Awareness and Training |
| Security Reminders  2014 | The purpose is to implement periodic security reminders to all members of the workforce. | Security Awareness and Training |
| Transmission Security Policy (Encryption)  2014 | The purpose is to implement technical security measures to guard against unauthorized access to and alteration of information, especially confidential information such as ePHI, that is transmitted over an electronic communications network. | Transmission Security |
| Workforce Security Policy (Access Controls)  2014 | The purpose of this policy is to implement policies and procedures to ensure that all members of the workforce have appropriate access to information systems, to limit access to only what is necessary and properly authorized, and to prevent those workforce members who should not have access and have not been authorized from obtaining access. | Access Controls |
| Workstation Security and Use Policy (Including handhelds)  2014 | the organization will develop standards and procedures regarding workstation use in order to best protect the confidentiality, integrity and availability of the organization’s information and information systems. | Workstation Use |
| Security Management Process Policy  2014 | The purpose of the Security Management Process is   * To implement policies and procedures to ensure the confidentiality, integrity and availability of the organization information systems with efforts and resources prioritized toward those deemed critical and those which contain or transmit confidential information * To prevent, detect, contain, and correct security violations | Security Management Process |

**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 areas of the computer. What type 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