MPCA HIPAA Compliance/meaningful Use Requirements and Security Risk Assessment Series

Webinar 2

HIPAA/HITECH Requirements for FQHCs and the New Omnibus Rule (Part 2)

February 20, 2014

Presented by:  
Jay Trinckes, CISO  
CISSP, CISM, CRISC
Table of Contents

Table of Contents ........................................................................ 2
About MPCA ................................................................................ 5
About OSIS .................................................................................. 5
  Services............................................................................................. 5
Presenter Bio............................................................................... 6
Background ................................................................................... 7
Webinar 2 ..................................................................................... 8
Objectives ............................................................................................. 8
Recap of Part 1: ........................................................................... 9
  Overview............................................................................................. 9
Privacy Basics.................................................................................. 11
  Direct Identifiers.............................................................................. 11
Minimum Necessary ........................................................................ 12
Administrative Requirements ............................................................ 12
Enforcement Rule ............................................................................. 12
Personal Liability ............................................................................... 13
Privacy vs. Security Rule .................................................................... 14
Required vs. Addressable .................................................................... 14
Omnibus Rule.................................................................................... 14
  Enforcement Rule ............................................................................. 14
  Breach Notification Rule ................................................................. 15
Meaningful Use .................................................................................. 15
Importance of Security ........................................................................ 16
State of Healthcare Security.............................................................. 16
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Identity Theft</td>
<td>18</td>
</tr>
<tr>
<td>Health Insurance Dossiers</td>
<td>19</td>
</tr>
<tr>
<td>Breach Notifications</td>
<td>20</td>
</tr>
<tr>
<td>Presumption of Breach – LoProCo</td>
<td>21</td>
</tr>
<tr>
<td>Compromised Risk Assessment</td>
<td>21</td>
</tr>
<tr>
<td><strong>Administrative Safeguards</strong></td>
<td>22</td>
</tr>
<tr>
<td>Security Management</td>
<td>22</td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>26</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>26</td>
</tr>
<tr>
<td>First Layer of Defense</td>
<td>26</td>
</tr>
<tr>
<td><strong>Physical Safeguards</strong></td>
<td>27</td>
</tr>
<tr>
<td>Facility Access Controls</td>
<td>27</td>
</tr>
<tr>
<td>Workstation Use</td>
<td>28</td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td>29</td>
</tr>
<tr>
<td>Remote Use and Mobile Device</td>
<td>30</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>30</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>31</td>
</tr>
<tr>
<td>Trust and Loyalty</td>
<td>31</td>
</tr>
<tr>
<td>Laws of Security</td>
<td>32</td>
</tr>
<tr>
<td><strong>Technical Safeguards</strong></td>
<td>33</td>
</tr>
<tr>
<td>Evaluation</td>
<td>33</td>
</tr>
<tr>
<td>Vulnerability/Penetration Testing</td>
<td>33</td>
</tr>
<tr>
<td>Access Control</td>
<td>34</td>
</tr>
<tr>
<td>Unique Use Identification</td>
<td>36</td>
</tr>
<tr>
<td>Emergency Access Procedure</td>
<td>40</td>
</tr>
<tr>
<td>Automatic Logoff</td>
<td>40</td>
</tr>
<tr>
<td>Encryption and Decryption</td>
<td>40</td>
</tr>
<tr>
<td>Not All Encryption IS the Same</td>
<td>40</td>
</tr>
</tbody>
</table>
About MPCA

Michigan Primary Care Association (MPCA)
Has been the voice for Health Centers and other community-based providers in Michigan since 1980. It is a leader in building a healthy society in which all residents have convenient and affordable access to quality health care.
MPCA’s mission is to promote, support, and develop comprehensive, accessible, and affordable quality community-based primary care services to everyone in Michigan

www.MPCA.net
517-381-8000

About OSIS

Ohio Shared Information Services, Inc. (OSIS)
We are a 501(c)3 non-profit organization that partners with Federally Qualified Health Centers (FQHCs) to provide IT and security related services to improve the quality of care delivered to the underserved population.
Our security division has professionals on staff dedicated to providing information security services to transform healthcare.
OSIS started in December 2000 when three (3) Federally Qualified Health Centers came together to share their medical IT initiatives. They received a grant from the Health Resources and Services Administration (HRSA) to launch OSIS. OSIS has since grown to become one of the few full-service Health Center Controlled Networks in the country. OSIS has a staff of sixty-eight (68) highly experienced professionals dedicated to serving FQHCs, Community Behavioral Health Organizations, and other healthcare centers. OSIS is headquartered in Cincinnati, OH, but has employees located in eleven (11) different states and counting. OSIS currently has a satellite office in Salt Lake City and will be opening up another office in the greater Chicago metropolitan area.

Services
Some of the services that OSIS provides to its partner clients are the following:

Implementation support; Training; Upgrades; Hosting; Custom Development; Security/Risk Analysis; Patient Portal; Meaningful Use Assistance; PCMH Assistance; Reporting – UDS –I2I; Governance Development; IT Support; Helpdesk; IMO – Care Sentry

www.OSISSecurity.com
513-677-5600 x1223
Presenter Bio

Jay Trinckes is Chief Information Security Officer at OSIS, a 501c(3) non-profit organization that assists Federally Qualified Health Centers (FQHC) with IT and security related services to improve the quality of care delivered to the underserved population. Mr. Trinckes is the author of “The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules”, (CRC Press, 2012) and “The Executive MBA in Information Security”, (CRC Press, 2010). Recently, Mr. Trinckes has presented on the topic of HIPAA and other related Information Security topics across the country through RAC Monitor, NWRPCA-CHAMPS Conference, NACHC-FOM-IT Conference, and locally through HRSA regional group. Mr. Trinckes is scheduled to present on HIPAA at the Practice Management Institute’s National Conference held in Chicago, IL this May. Mr. Trinckes holds a Bachelor’s Degree in Business Administration/MIS along with several certifications such as the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), National Security Agency (NSA) INFOSEC Assessment Methodology (IAM), and INFOSEC Evaluation Methodology (IEM). Mr. Trinckes brings a wealth of knowledge in information security through his hands-on experience performing risk assessments, vulnerability/penetration tests, developing information security management programs, and from his experiences as a former law enforcement officer.
Background

Health Centers are faced with ever increasing regulations as changes in HIPAA/HITECH took place from the finalization of the Omnibus Rule along with increasing security requirements related to electronic health records through Meaningful Use incentives. Why should health centers be concerned? Health Information has become a ‘hot’ commodity in the underground markets and is about ten (10) times more valuable than financial information such as credit cards. Why is healthcare information so valuable? Individuals can sell insurance information and resell to people that don’t have insurance, they can gain access to prescription drugs, and of course, steal identities to open up fraudulent accounts. Medical identity theft is the fastest-growing crime and has grown over 20% since 2012 costing the US close to $31 billion a year. In addition, it costs an individual over $20,000 to resolve a case of medical identity theft.

Of course, civil monetary penalties and class action lawsuits are always a concern to consider if your health center falls victim to a security breach. Data security breaches cost the U.S. healthcare industry $6.5 billion annually. On average, it costs a healthcare organization $233 per individual record breached with a full cost of a breach to a company on average of $5.4 million. Considering federal civil monetary penalties for a privacy/security violation can cost $50,000 per violation with an aggregate limit of $1.5 million per year and OCR has collected over $50 million to date from enforcement activities, it is definitely more cost effective for a health center to be HIPAA compliant.

As more incentives are paid out for health centers to convert over to electronic health records, more requirements will be placed on securing this electronic information. Electronic health records offer 45% reduction in documentation time, a net savings of $142 billion over 15 years for outpatient and $371 billion for inpatient along with patient safety with better tracking of adverse drug events. As of April 2013, CMS has paid out an estimated $14.6 billion and will increase as more and more providers switch over. Currently, under Stage 1 and Stage 2, health centers attesting to meaningful use are required to perform a security risk analysis as described under the Security Rules. This includes performing a technical and nontechnical evaluation as well. Individuals attesting to meaningful use are claiming federal funds and should be aware that any false, incomplete, or misleading information provided could subject them personally to civil and criminal penalties. It is imperative that you complete your risk assessment today and comply with the HIPAA/HITECH Privacy and Security Rules. At the end of the day, it is about protecting your organization’s information, revenue, and reputation.
As a continuation to Webinar 1, this seminar will present the importance of information security for federally qualified health centers by demonstrating the State of Security in the healthcare industry. With the recent news of major breaches, it is important that patient information maintained by your organization is kept in a secure and private manner. Is your organization able to survive if you fall victim to a breach? What type of damages can your organization face? What can your patients expect if they fall victim to identity crimes as a result of a breach? Questions like these will be answered and discussed during this seminar.

This webinar was designed to be a continuation of Webinar #1 which was an overview of the HIPAA/HITECH Privacy and Security Rules along with the changes to these rules as part of the finalizations of the New Omnibus Rule.

Objectives

Attendees will learn:

• Importance of Security and the State of Security for the healthcare industry.
• Breaches and why do they matter.
• Review of addressable versus required standards.
• Elements of Administrative Safeguards.
• Importance of a good Risk Management Program.
• What items should be reviewed under information system activities.
• The role of the Security Official.
• Importance of Security Awareness.
• Importance of a defined Security Incident Response Plan.
• Importance of a Business Continuity/Disaster Recovery Plan.
• Elements of Physical Safeguards.
• Importance of Workstations, Media, and Device Controls
• How to prevent Social Engineering.
• Ten Laws of Security.
• Elements of Technical Safeguards.
• Difference between a Vulnerability and a Penetration Test.
• Properly dealing with Business Associates and vendor due diligence activities.
Recap of Part 1:

Overview

Like many other industries, the healthcare industry has faced its share of challenges. From regulations to fraud, from data breaches to substantial inflation in costs, the healthcare industry is not immune to these different factors. At one time, every state in the union established different rules and regulations regarding the healthcare providers in their state. Since insurance companies and healthcare providers were isolated regionally, regulations were not uniform and often times, state laws contradicted with federal regulations.

With the increase use of technology, it became apparent to the United States’ Congress that there could be potential fraud or compromise of sensitive information leading the way to the establishment of security and privacy standards. In 1996, Congress enacted The Health Insurance Portability and Accountability Act (HIPAA) in response to these concerns. The Department of Health and Human Services (HHS) was assigned the responsibility and oversight for the implementation and enforcement of these regulations.

In the years that followed, the Privacy Rule, the Electronic Transactions and Code Sets Rule, the National Identifier Requirements, and the Security Rule were published and finalized as a result of the Administrative Simplification provisions of HIPAA. The following figure shows the components that make up the HIPAA Act:

---

*There are only two types of companies: Those that have been hacked, and those that will be.* – Former FBI Director Robert Mueller (Fox News 2012)
In 2009, as part of the American Recovery and Reinvestment Act (ARRA), the Health Information Technology for Economic and Clinical Health Act (The HITECH Act) revised HIPAA and amended the enforcement regulations as related to civil monetary penalties. This new rule-making gave HHS more control over enforcement and compliance of the HIPAA regulations with stiffer penalties. It also paved the way for the Attorney Generals of each state to take enforcement actions for violations of these regulations.

Monetary penalties are not the only ways in which Congress forces mandatory compliance with the HIPAA/HITECH regulations. The Centers for Medicare & Medicaid Services (CMS) has developed an Electronic Health Records (EHR) Incentive Program. This incentive program provides a monetary incentive to comply with the HIPAA/HITECH regulations, but will also create payment adjustments in Medicare reimbursements for eligible entities that do not successfully demonstrate “meaningful use” by the year 2015.

Over half of the HIPAA security requirements are covered under the Administrative Safeguards. As a reminder, the Security Rule defines administrative safeguards as, “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the health center’s workforce in relation to the protection of that information.” Some of these safeguards are required, while others are addressable. Compliance with the Security Rule will depend on several factors as defined in 45 § 164.306(b)(2) to include: the size of the health center; complexity of the health center; capabilities of the health center; the health center’s technical resources to include hardware and software security capabilities; costs of controls; and the risk assessment based upon probably and criticality of potential risks to electronic protected health information.

One of the first layers of defense for any organization is the physical layer. This primarily includes the controls around the physical access to the facility or structures that may store protected health information. These safeguards also involve the controls surrounding procedures and maintenance of documents or hardware that contain protected health information. The HIPAA Security Rule separates physical safeguards into two (2) primary areas: facility access controls and device/media controls. Both of these areas have several sub-sections of controls that are either required or addressable under the HIPAA Security Rule standards.

As technology advances in the healthcare industry it is becoming imperative to increase the level of security in this technology. Health centers are expected and required to implement an adequate level of security for safeguarding their electronic protected health information. As part of the requirements under the HIPAA Security Rule, health centers must implement security measures to comply with these standards. The objective of these safeguards is to mitigate the risk of electronic protected health information being used or disclosed in an unauthorized manner. These technical safeguards include the following measures: access control, audit controls, integrity, person or entity authentication, and transmission security.
Privacy Basics

In the most basic terms, a health center (and business associate) may not use or disclose protected health information except as permitted or required by the HIPAA Privacy Rule. A health center and business associate must develop policies and procedures to reasonably limit to, the *minimum necessary*, its disclosures and requests for protected health information for payment and healthcare operations. A health center and business associate should apply the least amount of privileges to their individual employees based upon the roles of their employees. These restrictions should be applied through policies and procedures to restrict access to protected health information as need-to-know or to perform their job functions. There are several different examples to demonstrate how the minimum necessary standards can be applied, but there may be an easier example of what not to do. It would be a violation of the minimum necessary standard if a hospital employee is allowed routine, unimpeded access to patients’ medical records if that employee does not need this access to do his or her job.

Direct Identifiers

**Direct Identifiers** of the individual or of relatives, employers, or household members of the individual are defined under 45 CFR § 164.514(e)(2) and include the following eighteen (18) items:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three (3) digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   b. The initial three (3) digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to ‘000’.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over eighty-nine (89) and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age ninety (90) or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code.

**Minimum Necessary**

Workforce members will use and disclose the least amount of information necessary to perform tasks within their job function; and OSIS will provide the least amount of privileges to its workforce members based upon their roles within the organization. *Minimum necessary requirements do NOT apply to disclosures to or requests by a healthcare provider for treatment; uses or disclosures made to the individual; uses or disclosures made pursuant to an authorization; disclosures made to the Secretary; uses or disclosures that are required by law; and uses or disclosures that are required for compliance with the Privacy Rule.*

**Administrative Requirements**

Administrative Requirements include, but may not be limited, to the following:

- **Privacy Personnel Designations**— health centers are required to designate a Privacy Official;
- **Privacy Training**— health centers and business associates are required to provide specific privacy/security training;
- **Administrative Safeguards**— health centers and business associates are required to implement administrative, physical, and technical safeguards;
- **Complaint Handling**— health centers and business associates are required to implement complaint handling procedures;
- **Workforce Member Sanctions**— Workforce Member Sanctions – sanction policies are required to be developed and implemented regarding workforce members that fail to comply with HIPAA Privacy and Security Rule requirements;
- **Mitigation**— health centers and business associates are required to mitigate
- **Retaliation**— health centers and business associates are required to refrain from intimidating or retaliating against complaints of non-compliance;
- **Waiver of Rights**— health centers are not permitted to waive any of the Privacy Rights as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- **Privacy Policies**— Privacy Policies and Procedures along with documentation health centers and business associates are to develop and implement appropriate Privacy Policies and Procedures and retain this documentation for at least six (6) years.

**Enforcement Rule**

The Department of Health and Human Services (HHS) strengthened HIPAA enforcement as a response to the Health Information Technology for Economic and Clinical Health (HITECH) Act that was enacted as part of the American Recovery and Reinvestment Act of 2009. New, stricter civil money penalties were enacted for violations of the HIPAA Act occurring after February 18, 2009. The revisions included four (4)
categories of violations along with four (4) different, incrementing tiers of monetary
amounts. The modifications capped each violation at $50,000 per violation with an
aggregate limit for identical violations set at $1.5 million per calendar year. As a note of
reference, an organization could get assessed penalties for different kinds of violations
so they could face total fines in excess of $1.5 million. The new requirements also
provided an affirmative defense, waiver, and Notice of Proposed Determination. Finally,
the new HITECH Act provided for the enforcement of HIPAA Privacy or Security Rule
violations by states’ attorney generals.

Recently, the Director of the Office for Civil Rights (OCR), Leon Rodriguez,
emphasized a new era of “monetary enforcement” rather than the long-standing approach
of “hand-holding” to assist health centers (and business associates) in compliance efforts.
In an interview conducted by Report on Patient Privacy, Mr. Rodriguez discussed OCR’s
plans to refocus on “high-impact cases”. He emphasized “health centers (CEs) and
business associates (BAs), in the future, will face sanctions on all lapses discovered
during an investigation regardless of whether they are directly related to the incident that
sparked OCR’s attention in the first place.” (Report on Patient Privacy 2012)

Mr. Rodriguez also warned that OCR will be going after a health center along with
their business associate for sanctions resulting from a breach or violation when they are
jointly responsible. Systemic issues underlying an incident will be a big consideration
when determining an assessed monetary amount. Cases involving corrective action-only
to fix issues five (5) years ago will now have a greater amount of resources focused on
the high-impact side where investigating of these cases will be done more quickly and will
also have more fulsome enforcement. Once the Omnibus Rule is implemented, OCR will
also be focusing attention on business associates. “There are going to be cases where
culpability is shared equally between the CE and BA and in other cases where it might be
more heavily found on one side or the other,” Mr. Rodriguez indicated. (Report on Patient
Privacy 2012)

Personal Liability

Individuals can be personally liable for handling health information. There are steep
penalties for a person who knowingly uses or causes to be used, obtained, or disclosed
individually identifiable health information to another person. Penalties increase if the act
is done under false pretense or with the intent to sell, transfer, or use for commercial
advantage, personal gain, or malicious harm.

<table>
<thead>
<tr>
<th>US Code Title 42 Chapter 7 – 1320d-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrongful disclosure of individually identifiable health information</td>
</tr>
<tr>
<td>• Offense: A person who knowingly and in violation of this part</td>
</tr>
<tr>
<td>• Uses or causes to be used a unique health identifier;</td>
</tr>
<tr>
<td>• Obtains individually identifiable health information relating to an individual; or</td>
</tr>
<tr>
<td>• Discloses individually identifiable health information to another person</td>
</tr>
<tr>
<td>• Fined not more than $50,000, imprisoned not more than 1 year, or both;</td>
</tr>
<tr>
<td>• If committed under false pretenses, be fined not more than $100,000, imprisoned</td>
</tr>
<tr>
<td>not more than 5 years, or both; and</td>
</tr>
<tr>
<td>• If committed with intent to sell, transfer, or use individually identifiable health</td>
</tr>
<tr>
<td>information for commercial advantage, personal gain, or malicious harm, be fined</td>
</tr>
<tr>
<td>not more than $250,000, imprisoned not more than 10 years, or both.</td>
</tr>
</tbody>
</table>
Not only is there huge financial losses due to the lack of security, but entire companies along with people’s careers have been ruined. In February of 2010, an article was published citing the Chief Executive Officer, Aaron Barr, of HBGary Federal, regarding the names of the individuals in a hacktivist group known as ‘Anonymous’. An all-out hacking campaign was conducted on HBGary Federal’s servers to find out what Barr knew about the group. It took a weekend to gain access to the company’s e-mails that were then publicly released. Unfortunately, the names of the individuals were off-base and the repercussions of the hack devastated the security company along with forcing Barr’s resignation.

After a hack was discovered in July of 2011, and made public in August, the Dutch certificate authority, DigiNotar, a subsidiary of VASCO, filed for bankruptcy protection. Approximately five hundred thirty-one (531) fake certificates were issued as a result of the breach. Digital certificates are used as the authentication backbone of secure transactions over the Internet. If one of these certificates is compromised, any transmission thought to be secured using the certificate would ultimately be able to be intercepted and deciphered. Other companies such as CloudNine and Blue Frog were also forced to be shut down due to online attacks. (Kingsley-Hughes 2011)

Gary S. Miliefsky, Founder and Chief Technology Officer of NetClarity, a leading provider of patented network access control products, made some rather disturbing predictions for 2012 related to cybercrime and cyberwar. One of the top predictions is that smaller and medium sized (SMB) organizations will be the top target for cybercriminals in 2012. Mr. Miliefsky advises that the effects on these businesses will be huge and as a result, cause a lot of them to go out of business. (PRWEB 2012)

Privacy vs. Security Rule

Let’s take a second to clarify that there is a difference between the Privacy Rule and the Security Rule under HIPAA/HITECH. The Privacy Rule requires the implementation of appropriate and reasonable safeguards to secure Protected Health Information (in whatever form it is in, for example paper or digital form) while the Security Rule is intended to secure protected health information that is in electronic form only. Both rules deal with administrative, physical, and technical controls; however, the Security Rule goes into more detail and is more comprehensive when dealing with the confidentiality, integrity, and availability of this information while allowing only authorized access to the information. The Security Rule is a subset of the Privacy Rule.

Required vs. Addressable

If you are familiar with the regulations, you will note that some are required and others are addressable. Being addressable doesn’t mean being optional. The regulations are supposed to be ‘flexible’ and if an organization doesn’t want to implement a control for any reason, they better have some mitigating controls in place and be able to justify why they still meet or address the requirements accordingly.

Omnibus Rule

The Omnibus Rule went into effect March 26, 2013 with 180 days to comply. The deadline for this compliance passed on September 23, 2013 and all health centers (along with business associates) fall under these new requirements. The Omnibus Rule, in my opinion, didn’t necessarily change the obligations of healthcare providers that drastically since they all were supposed to be compliant with the standards under the HIPAA/HITECH Privacy and Security Rules. The Omnibus Rule did modify some Privacy, Security, Enforcement and Breach Notification Rules. It made business associates (and subcontractors of business associates) directly liable for compliance. Some of the other major changes were that it provided individuals the right to electronic copies of their health
information and right for individuals to restrict disclosure of information about services they paid for ‘out of pocket’. It increased tier civil monetary penalties and detailed what ‘willful neglect’ for noncompliance means to a health center. Under the breach notification, it removed the ‘harm’ threshold and presumes a security incident is a reportable breach unless it can be demonstrated that there was a low probability of a compromise of the information. It defined genetic information as protected health information and there were some guidance issued in the de-identification process of protected health information. If you haven’t yet had the chance to see a couple good videos that HHS has put out regarding some of the changes with the Omnibus Rule, here are the links of interest: 
https://www.youtube.com/watch?v=3-wV23_E4eQ  
https://www.youtube.com/watch?v=mX-QL9PoePU

Breach Notification Rule

Increased breach notification requirements came about as part of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) enacted under the American Recovery and Reinvestment Act (ARRA) on February 17, 2009. These breach notification provisions apply to HIPAA health centers and business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. In short, if a health center discovers a breach of unsecured protected health information, they are required to promptly notify the affected individuals and the Secretary of Health and Human Services. If a business associate of a health center discovers that they had a breach, they must notify the health center of the breach. In some cases, the media must also be notified of such a breach and for any breach involving more than five hundred (500) individuals, the Secretary of Health and Human Services is required to post a list of health centers on the Health and Human Services’ web site. As of January 15, 2014, there were eight hundred four (804) organizations reporting data breaches of more than five hundred (500) records since September 2009. A list of these organizations can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Meaningful Use

To achieve health and efficiency goals, the Centers for Medicare and Medicaid Services (CMS) has implemented an Electronic Health Records (EHR) Incentive Program. This incentive program provides a monetary incentive to comply with the HIPAA/HITECH regulations, but will also create payment adjustments in Medicare reimbursements for eligible entities that do not successfully demonstrate “meaningful use” by the year 2015.

As of July 2013, there appears to have been over $9.5 billion paid out to over 250,000 physicians and hospitals. There are three (3) main components of ‘Meaningful Use’. These include the use of certified EHR technology in a meaningful manner, for electronic health information exchanges, and for clinical quality submissions. Over the next five (5) years, meaningful use will be implemented in three (3) stages. Stage 1 required the providers to meet 15 core objectives. I like to point out Core 15 objective that deals with a security risk analysis required to be conducted or reviewed under 45 CFR
164.308(a)(1). Furthermore, security updates were required to be implemented. Stage 2 still requires eligible professionals to ensure adequate privacy and security protection for personal health information (same as Core 15 above). It adds another requirement to address encryption/security of data stored within the EHR software. Stage 2 also addresses using secure electronic messaging to communicate with patients on relevant health information.

Here is a good info-graphic that describes the cost benefits to implement an electronic health record over traditional paper records. Some of the big items here are the 45% reduction in documentation time with electronic health records, a net savings of $142 billion over 15 years for outpatient and $371 billion for inpatient services, and for safety purposes to better track adverse drug events. It is all about time, environment, financial, and health benefits that technology can provide.

**Importance of Security**

“The state of technology security overall is so weak that intelligence officials see hacking as one of the largest threats to western powers”. (Menn 2011)

**State of Healthcare Security**

Let’s take a second to think about this quote….”security is so weak… HACKING is considered one of the largest THREATS to western powers.” It is assumed that you have all read the news or heard stories on cyber activities, hacking, breaches, identity theft, etc. These are just some of the outcomes as a result of lax security procedures.

According to technology research firm, Gartner, law enforcement officials arrest less than one percent (1%) of the cybercriminals. Although most law enforcement agencies concentrate their efforts on nation-backed cyber-attacks, a new wave of ‘hacktivism’ (the combination of computer hacking with political activism) has sprung up blurring the lines between protesters, criminals, and spies. Law enforcement does not have the resources or expertise to handle this problem since the best cyber-experts usually work for higher paying private security companies.

Why is Security Important? In January 2012, former FBI Director Robert Mueller testified before the Senate Select Committee on Intelligence explaining that cyber-threats would surpass terrorism as the nation’s top concern. Think about this for a moment, ‘cyber-threats surpassing terrorism’. At the RSA Conference in San Francisco held on March 1, 2012, speaking to a crowd of 20,000 cyber-security professionals, Mr. Mueller stated, “We are losing data, we are losing money, we are losing ideas and we are losing innovation. Together we must find a way to stop the bleeding.” (Fox News 2012) A study performed by Norton, an anti-virus software development company, determined that there are one hundred forty-one (141) victims of cybercrime per minute in the United States. The study suggests that over the last year, the total bill for cybercrime topped $139 billion in the United States with over $388 billion being assessed globally. In healthcare, medical identity theft crimes is close to $31 billion a year. Annually, the
Ponemon Institute conducts a study on the impact (or costs) a company faces if they were breached. For 2012, it was calculated that the cost to an organization was $188 per individual record breached. In healthcare (and pharmaceutical companies), it was more. The average cost of a data breach is $233 per individual record in healthcare. How many patients do you see throughout the day? How many medical records do you have? In the case of electronic records, how many unique records do you have in your database? Now, take that number and multiply it by $233. Could your organization sustain such a loss? A full cost of a breach for a company averages $5.4 million. This includes costs such as legal/regulatory (that includes fines, civil monetary penalties, lawsuits); financial (involving business distraction, remediation costs, communication, insurance costs, changing vendors); operational (to include recruiting new hires or possible reorganization); clinical (includes diagnostic delays, processing fraud, research disruptions); and reputational costs (includes the loss of future patients, business partners, staff losses.)

“I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.”

(source: http://nedv.net/health/hippocratic_oath.html
Medical Identity Theft

We discussed ‘hacking’ and as a lot of people believe, this activity occurs from outside sources. This isn’t always the case when it comes to healthcare information. Hacking activity is increasingly being carried out by knowledgeable insiders bent on identity theft or access to prescription drugs. Identity theft is the fastest-growing crime. Theft of medical identities is a big problem. There is an estimated 313,000 Americans that will have their medical identities stolen this year. According to the Ponemon Institute, there has been about 1.84 million identities stolen over the past few years. [Source: http://www.timesdispatch.com/news/national-world/medical-identity-theft-a-growing-risk/article_cb6794aa-5ed8-5073-b900-96f8970db6b9.html?mode=jqm#! ]

Providers may not recognize the seriousness of medical identity theft. First, it is fairly easy to carry out. This may be due to victims tending to be older, these crimes are hard to investigate, and most of these crimes are occurring by family members. Why? Family members know personal information about their victims. What process does your practice have in place to verify or validate the identity of your patients? Do you check identification appropriately? In a recent news report, medical identity theft has risen over 20% since 2012. The risk and high cost of medical identity theft are not resonating with the public. There is definitely a need for greater education and awareness. As we move into the requirements under Obama Care and Health Insurance Exchanges, what type of safeguards or controls will we put in place to make sure that the information collected is secure?

In the Second Annual Survey on Medical Identity Theft, published March 2011, the Ponemon Institute found that nearly 1.5 million Americans are victims of medical identity theft. The extrapolated cost per victim was up by about five hundred dollars ($500) from the previous year to astounding twenty thousand six hundred sixty-three dollars ($20,663) to resolve a case of medical identity theft. The national impact of medical identity theft crimes is close to $31 billion a year. (Ponemon Institute LLC 2011)

Some of the key factors identified in this study were as follows:
Many people are unaware of the seriousness of medical identity theft crimes and the affects that it can have on them such as negatively affecting credit scores. Primary consequences to these types of crimes are the financial harm that it could cause to the victim or the loss of health coverage.

Committing medical identity theft is fairly easy such as utilizing a name to obtaining healthcare services, treatment, pharmaceuticals, equipment, benefits.

Medical identity theft victims tend to be older.

Victims have a hard time determining when the crime may have occurred.

Since most victims share their medical information with family, these family members become the most likely individuals to steal identity.

Larry Ponemon, Chairman and Founder of the Ponemon Institute stated, “Our study shows that the risk and high cost of medical identity theft are not resonating with the public, revealing a serious need for greater education and awareness.” He further opinionates that, “… these results put an even greater onus on healthcare organizations to make the security of sensitive personal health information a priority in order to protect patient privacy.” (Millard 2011) Some experts are claiming that cyber espionage and privacy violations are going to be some of the biggest security threats in 2012. (b 2012)

To help organizations and consumers to prevent or protect themselves from identity theft, the Federal Trade Commission’s (FTC’s) Bureau of Consumer Protection has established a campaign, “AvoID Theft: Deter. Detect. Defend.” Through this effort, a repository of ID theft information has been developed including the FTC’s Consumer Education Tool Kit to assist individuals. The Tool Kit includes a how-to guide, video, brochure, CD-Rom, and an in-depth guide to identity theft. This kit along with other information can be obtained by going to the FTC’s website at: http://business.ftc.gov/documents/taking-lead-prevent-identity-theft

Health Insurance Dossiers

Why is healthcare information so valuable? Individuals can sell insurance information and resell to people that don’t have insurance. They can gain access to prescription drugs. They can steal identities to open up fraudulent accounts.

Dell SecureWorks Reports Hackers Selling Health Insurance Dossiers For Over $1,000 Each

These packages of data are referred to in the underground as “fullz, compiled specifically for the purpose of identity theft and fraud

Dark Reading
July 15, 2013
URL: http://www.darkreading.com/privacy/dell-secureworks-reports-hackers-selling/240158267
Hacker Pricing for Stolen Credentials:

"Kitz"--- these particular Kitz contained verified health insurance, SSN, bank account info/logins (account & routing numbers, account type), driver's license, full name, address, phone, etc. and counterfeit physical documents and hardware related to the identity data in the package (eg: credit cards, driver's license, insurance cards, etc.)--- ranging between $1200 - $1300 per Kit. Add $100 - $500 for rush orders and other miscellaneous fees like wire transfer, escrow, etc.

"Fullz"--- If these records also include health insurance credentials for a US victim, then they were negotiated for about $500 each, based on what was included: full names, addresses, phone numbers, email addresses (with passwords), dates of birth, SSN or EIN, one or more of: bank account information (account & routing numbers, account type), online banking credentials (varying degrees of completeness), or credit card information (including full track2 data and any associated PINs).

This is a recent article from Dell SecureWorks uncovering the underground market for health information. As you can see, hackers are selling ‘kitz’ that include all sorts of personal information along with fraudulent papers for $1,200 to $1,300. They will provide a discount for ‘fullz’ that is all the same personal information, but without the fraudulent papers for around $500.

Health Insurance Credentials that include names, date(s) of birth, contract number, type of plan, etc. are going for $20 each. If these insurance plans have associated dental, vision, or chiropractic coverage, they can go for an additional $20. Now, take a look at the underground market value for US credit cards, even with the CVV code at $1 to $2.

This indicates that health insurance information is about 20 times more valuable than financial information in the criminal underground. Data security breaches cost the US healthcare industry $6.5 Billion (with a B) annually. Small companies don’t have the resources to prevent or mitigate against some of these breaches. They are focused on time/productivity activities rather than security. Healthcare is focused on treating patients, and rightfully so, but as you have seen, part of this treatment is to also protect privacy and maintain the security of the information they collect. Companies tend to seriously underestimate potential damage of cyber threats and reveal a great data breach perception gap.

**Breach Notifications**

A breach is defined as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E [the Privacy of Individually Identifiable Health information] that compromises the security or privacy of the protected health information. Compromises the security or privacy was formally defined as poses a significant risk of financial, reputational, or other harm to the individual.

Increased breach notification requirements came about as part of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) enacted under the American Recovery and Reinvestment Act (ARRA) on February 17, 2009. These breach notification provisions apply to HIPAA health centers and business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. In short, if a health center discovers a breach of unsecured protected health information, they are required to promptly notify the affected individuals and the Secretary of Health and Human Services. If a business associate of a health center discovers that they had a breach, they must notify the health center of the breach. In some cases, the media must also
be notified of such a breach and for any breach involving more than five hundred (500) individuals, the Secretary of Health and Human Services is required to post a list of health centers on the Health and Human Services’ web site. A list of these organizations can be found at: [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachttool.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachttool.html)

**Presumption of Breach – LoProCo**

Under the changes in the Omnibus Rule, an acquisition, access, use, or disclosure of protected health information, not permitted under Subpart E [the Privacy of Individually Identifiable Health Information], is presumed to be a breach unless it can be demonstrated that there is a low probability that the protected health information has been compromised based on a risk assessment being performed.

**Compromised Risk Assessment**

Additional guidance is forthcoming from OCR on this; however, the risk assessment that needs to be performed to determine a compromise includes the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identifications;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.
Security Management

Under 45 CFR § 164.308(a)(1), a health center must “implement policies and procedures to prevent, detect, contain, and correct security violations.” One of the first policies and procedures to be implemented involves conducting a risk assessment. A health center should develop and disseminate risk assessment policies and procedures so that all workforce members have an idea of this process. These risk assessment policies and procedures should be reviewed and updated as necessary. In addition, workforce members that are affected or responsible for risk assessment activities should be trained accordingly.

At a minimum, the risk assessment policy should address the following: the purpose of the policy; the scope of the policy; high level overview of the different roles and responsibilities of the workforce members; the commitment that management has towards the importance of a risk assessment; coordination between different department or units within the health center; how workforce members are trained in risk assessment procedures; and how the health center will come into compliance with the risk assessment policies and procedures. The health center’s risk assessment policy should also define the frequency that the risk assessment is reviewed and updated.
In conducting the risk assessment, the health center should make sure to identify the types and uses of the information it creates, maintains, processes, stores, or transmits. This information should be classified based on its sensitivity levels. All information housing electronic protected health information should be identified. This inventory should be complete with all hardware including removable media, remote access, and mobile devices. Inventory should account for software including any types of reports, spreadsheets, databases, etc. that may contain electronic protected health information. This inventory should also include all business functions of the health center along with verification of control over information systems. Inventory should be kept updated, current, and reviewed on a periodic basis to make sure that all information systems containing electronic protected health information is appropriately accounted for. Configurations for these information systems should also be documented including any connections to other systems within the internal network and external network.

Risk Analysis

The health center is required to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the health center.” An entire section of this book was devoted to discuss the process of conducting a risk analysis. For the sake of simplification, a risk analysis must identify potential security risks. These risks can come from many different areas. The risk analysis must also determine the probability of an event will occur and the magnitude of damage or loss of information that may occur from such an event if it were to occur. A security categorization should be determined for each information system along with the rationale behind such a ranking to be included in the health center’s security plan. These security categorization decisions should be reviewed and approved by an official or delegated representative of the health center.

Risk Management

A health center is required to “implement security measures [that are] sufficient to reduce risks [to] vulnerabilities to a reasonable and appropriate level.” A covered should have policies and procedures in place for security as part of their risk management process. To conduct proper risk management, the health center should identify the security measures or safeguards that are already in place to secure protected electronic health information. These safeguards should ensure the confidentiality, integrity, and availability of electronic protected health information. These safeguards should also protect against any reasonably anticipated threat or hazard to the unauthorized use or disclosure of electronic protected health information or not permitted under the HIPAA Privacy Rule.

Sanction Policy

A health center is required to “apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the health center.” A health center must have an existing sanction policy and procedure to meet this requirement. If a health center doesn’t have an existing sanction policy, the health center should modify their policy to include language relating to violations of the security policies and procedures. In addition, the health center is required to have workforce members sign a statement of adherence to security policies and procedures as a prerequisite for
employment. Compliance to this requirement could come in the form of signing a statement as part of the employee’s initial hire and when they receive the health center’s employee handbook or as part of a signed confidentiality statement.

**Information System Activity Review**

A health center must have procedures in place to “regularly review records of information system activities.” These information system activities may include audit logs, access reports, and security incident tracking reports. First, the health center should identify what types of auditing and activity reviewing functions the current information system is capable of providing. The health center should determine the types of logs or reports the information systems can generate. Second, the health center should determine whether or not these functions are adequately used and monitor appropriate activity to promote continual awareness of the information systems. Finally, there should be policies in place to establish the reviews that will be conducted on the information system activities and procedures to describe specifics of the reviews.

**Assigned Security Responsibility**

A Security Official will be designated. The Security Official is “responsible for the development and implementation of the [security] policies and procedures required by [the Security Rule].” The health center should clearly identify and document the responsibilities of the Security Official. The Security Official should also have the appropriate authority to carry out their responsibilities within the health center. This means that a senior-level executive or manager should be assigned the Security Official role. Depending on the size, complexity, and technical capabilities of the health center, the roles and responsibilities of the Security official should be developed appropriately. The Security Official should be provided a complete job description that accurately reflects their security duties and responsibilities. In some instances, the Security Official may also be designated as the Privacy Official.

**Malware Protection**

An enterprise level anti-virus solution should be installed on all workstations and servers. There should be adequate procedures in place for “guarding against” malicious software. This solution should also detect and report on types of malware, viruses, spyware, Trojans, back doors, suspicious programs, open ports, etc. There are several different credible software vendors that produce good anti-virus solutions. Each one of these solutions come with their own pros and cons along with different pricing structures. A discussion will not take place on all the different brands of anti-virus here, safe it to say, that any solution chosen should come from a reputable source and the health center should conduct their own due diligence in choosing the right solution to meet their needs. The anti-virus solution should be controlled from a central console that can provide a report of all the systems that have been updated with new virus definitions and report on any possible viruses that were detected.

**Log-in Monitoring**

To verify that appropriate access is being maintained, the health center should have adequate procedures in place to monitor any log-in attempts. These procedures should
also report any discrepancies between those accesses that are permitted and those that should be denied. The following are some recommendations for logging parameters:

- Account Logon – Success and Failure auditing
- Account Management – Success and Failure auditing
- Directory Service Access – Failure auditing
- Logon Events – Success and Failure auditing
- Object Access – Success and Failure auditing
- Policy Change – Success and Failure auditing
- Privilege Use – Success and Failure auditing
- Process Tracking – Failure auditing
- System Events – Success and Failure auditing

A health center should implement a system log (or syslog) server that can collect all the audit logs from different sources such as internal servers and routers. This syslog server will allow the aggregation of information and should be able to produce reports to show suspicious activity or behavior. The syslog should allow writing of logs from the different sources, but allow read-only access to the user to prevent any unauthorized manipulation of the log events. These logs should be reviewed on at least a weekly basis or when unusual activity is suspected. There should be a specific individual, or group of individuals, assigned the responsibility of reviewing these logs. These logs should be kept for six (6) years to maintain consistency with other requirements of the HIPAA Security Rule.

Password Management

A health center should have procedures in place for “creating, changing, and safeguarding passwords”. Since passwords are one of the most common ways to validate access to an information system, it goes without saying that these passwords need to be protected. As a way to protect against individuals from performing particular actions as another individual, policies should state that workforce members, under no circumstances, should share their passwords with others. In addition, the workforce member should commit their password to memory and not write their passwords down in a notebook. From experiences, this author has found passwords written on sticky notes taped to the underside of keyboards, taped to monitors, or written in a rolodex under ‘P’ for passwords. An emphasis should be made through security awareness training that a common sense approach should be used to maintain the security over workforce members' passwords.

As a note of reference, usernames are the first half of the username/password combination utilized in most information systems. The health center should consider making usernames unique just like the passwords to make it more difficult for brute force password type attacks. Since it is common practice to use a part of the workforce member’s name, it is pretty easy to figure out the username. In a brute force attack, once the username is known, the attacker can run through a list of passwords to see if a common password was used. If a lockout parameter was not set, it is just a matter of time before an account is compromised.
Security Incident Procedures

Security incidents are those situations where it is believed that protected health information has been used or disclosed in an unauthorized fashion. A security incident can also be the actual unauthorized access, use, or disclosure of such information or the modification or destruction of this information. Any interference with system operations of an information system can also be considered a security incident. Several different examples of security incidents will be provided in the following section and an entire chapter was devoted in this book on how to appropriately handle these types of security violations.

Contingency Plan

A health center needs to be able to sustain or resume business during or after an emergency. To this end, health centers must implement adequate policies and procedures, as needed, to respond to emergency or other situations that could cause damage to systems that contain electronic protected health information. Some of the emergency situations that should be considered are fire, vandalism, system failures, and natural disasters. Preventative measures or steps that the health center can take immediately for each scenario should be outlined throughout the contingency plan. Costs of these preventive measures should also be considered.

Emergency Access Procedure

A health center should identify all workforce members that may need access to electronic protected health information in the event of an emergency. A health center is required to have policies and procedures in place to provide appropriate access to these workforce members in emergency situations. In addition, a health center should have a policy in place that designates a responsible workforce member to make a decision about activating emergency procedures and the appropriate time these should be activated. These emergency procedures should contain methods of supporting continued operations in situations that affect normal operations. It should be determined whether or not the information systems can allow for the automatic failover to emergency configurations or will a workforce member have to manually configure these failover procedures.

First Layer of Defense

A way to think about security is in layers of defense. One of the first layers of security defense is Physical Security. A health center should have policies and procedures in place that adequately limit the physical access to electronic information systems and protected health information. This includes the facilities that these systems are located in such as data centers, workstation locations, IT workforce member areas, medical records areas, and other areas. It also includes physical control over devices and media that may contain protected health information. As mentioned, for security to be successful, there must be a total commitment to a culture of security and adherence to sound principles. These principles include obtaining proper identification, authorization, and the need to know certain information. A disturbing statistic to share is that sixty percent (60%) of all theft is committed by internal staff. There should be steps implemented to discourage or lower this stat. Remember, the goal of physical and
environmental protection is to secure protected health information along with the security of the facility and workforce members working within the facility.

There, of course, is a fine balance between limiting unauthorized access and access that must be allowed to conduct business. Policies and procedures should reflect this balance keeping in mind the minimum necessary rule. These policies and procedures should identify workforce members, by title or job function, that are authorized to have physical access to the facilities that house the electronic information systems. In addition, business associates, contractors, sub-contractors, or any other individuals that may require access to the health center’s facilities should be addressed in the policies and procedures. Policies and procedures should also address maintaining proper access levels in the event of repairs, upgrades, or modifications are made to the facility or controls in place to secure the facility. A current list of workforce members having authorized access to the facility and specific access to certain areas containing protected health information needs to be developed and maintained. This list should be reviewed to ensure the appropriate access levels to the facility are being kept.

## Physical Safeguards

### Security Standards

<table>
<thead>
<tr>
<th>Physical Safeguards</th>
<th>Facility Access Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.310(a)(1)</td>
<td>Facility Access Controls</td>
</tr>
<tr>
<td>164.310(a)(2)</td>
<td></td>
</tr>
<tr>
<td>164.310(a)(2)(i)</td>
<td>A Contingency Operations</td>
</tr>
<tr>
<td>164.310(a)(2)(ii)</td>
<td>A Facility Security Plan</td>
</tr>
<tr>
<td>164.310(a)(2)(iii)</td>
<td>A Access Control and Validation Procedures</td>
</tr>
<tr>
<td>164.310(a)(2)(iv)</td>
<td>A Maintenance Records</td>
</tr>
<tr>
<td>164.310(b)</td>
<td>R Workstation Use</td>
</tr>
<tr>
<td>164.310(c)</td>
<td>R Workstation Security</td>
</tr>
<tr>
<td>164.310(d)(1)</td>
<td>Device and Media Controls</td>
</tr>
<tr>
<td>164.310(d)(2)</td>
<td></td>
</tr>
<tr>
<td>164.310(d)(2)(i)</td>
<td>R Disposal</td>
</tr>
<tr>
<td>164.310(d)(2)(ii)</td>
<td>R Media Re-use</td>
</tr>
<tr>
<td>164.310(d)(2)(iii)</td>
<td>A Accountability</td>
</tr>
<tr>
<td>164.310(d)(2)(iv)</td>
<td>A Data Backup and Storage</td>
</tr>
</tbody>
</table>

## Facility Access Controls

A health center should have policies and procedures in place that adequately limit the physical access to electronic information systems and protected health information. This includes the facilities that these systems are located in such as data centers, workstation locations, IT workforce member areas, medical records areas, and other areas. There, of course, is a fine balance between limiting unauthorized access and access that must be allowed to conduct business. Policies and procedures should reflect this balance keeping in mind the minimum necessary rule. These policies and procedures should identify workforce members, by title or job function, that are authorized to have physical
access to the facilities that house the electronic information systems. In addition, business associates, contractors, sub-contractors, or any other individuals that may require access to the health center's facilities should be addressed in the policies and procedures. Policies and procedures should also address maintaining proper access levels in the event of repairs, upgrades, or modifications are made to the facility or controls in place to secure the facility. A current list of workforce members having authorized access to the facility and specific access to certain areas containing protected health information needs to be developed and maintained. This list should be reviewed to ensure the appropriate access levels to the facility are being kept.

Remember, the goal of physical and environmental protection is to secure protected health information along with the security of the facility and workforce members working within the facility.

**Workstation Use**

A health center is required to have policies and procedures regarding the proper functions that are to be performed on a workstation. These policies and procedures need to be developed and implemented to identify the manner in which these functions are to be performed on a workstation. In addition, the policies and procedures need to identify the physical attributes of specific workstations or class of workstation that is authorized to access electronic protected health information. This means that the policies and procedures should describe which workstations have access to electronic protected health information and which ones are restricted from this access.

An asset inventory list should be maintained specifying the types of electronic devices and locations of these devices throughout the health center to include, but not limited to, workstations, laptops, Personal Data Assistants (PDAs), tablets, smart phones, printers, etc. The inventory should contain the classification of these devices, their capabilities, and the common functions utilized by these devices. A workforce member, or a group of workforce members, should be assigned responsibility to conduct this inventory and keep it current. Since each device has their own unique security concerns, the health center should ensure that their policies and procedures address these issues. For example, mobile devices like tablets have a lot of storage and computing powers. Since they are smaller and more portable than a workstation, they could have a tendency of getting lost or stolen if they are taken out of the facility. There should be some procedures in place to ensure that these devices won’t contain electronic protected health information or if they do, they are fully encrypted with password protection. Just as this example demonstrates, the health center needs to identify certain risks that each of these devices may have and train their workforce members on possible breaches of these devices.

A health center should consider providing users with the minimum necessary privileges on their workstations needed to perform their job functions. This means that users should not be administrator level or power users on their local workstations. Users should be restricted from installing any programs on their systems that is not approved by IT management. In addition, IT Staff members should have technical controls in place to monitor for any software or programs that are legitimately or illegitimately installed on the workstations.

Since the Internet can be a dangerous place to traverse and many people have become victims of hacking or other malicious type attacks from Internet activity, a health center should consider restricting or filtering Internet access. A web filtering solution
should be considered to protect the health center from workforce members going to liable web sites such as the following categories of sites:

- Pornography;
- Anonymizer or proxy avoidance;
- Hacking;
- On-line Chat;
- Web Mail;
- Social Media; and
- Remote or On-line Storage.

This web filtering solution should be able to log users by a unique identifier so that workforce members will be accountable for their actions.

The health center should have security controls in place to secure electronic protected health information that is being stored, being processed, or being transmitted. Policies and procedures should be able to correlate these attributes with the information systems controls. When dealing with remote access capabilities, for instance, policies and procedures should document the authorized access to these information systems. For each method of remote access, procedures should be established to restrict usage of these methods. There should also be monitoring in place for unauthorized remote access and prior authorization should be met before the connection is made. Finally, remote connections should have these and other security requirements enforced prior to gaining access to the information systems.

**Device and Media Controls**

A health center needs to have policies and procedures to identify the types of hardware and other electronic media that must be tracked. The receipt and removal of hardware and electronic media in and out of a facility along with the movements of these items within a facility should be addressed in these policies and procedures. Hardware and electronic media includes:

- Hard drives;
- Magnetic tapes or disks;
- Optical disks;
- Digital memory cards;
- Removable thumb drives; or
- Any other items that may contain electronic protected health information.

The media protection policy should cover at least the following components: the purpose, scope, responsibilities, management commitment, coordination among different departments, and compliance. These policies should be formally documented, disseminated, and reviewed and updated on a periodic basis (i.e. annually or upon any major changes that affect media protection). These policies should define the health center’s overall objectives and include all areas where media protection is required. Remember, the goal of media protection is to maintain the security over electronic protected health information that removable media stores.

A health center should have a current inventory of system components that identifies the information system boundaries and contain the necessary information to keep proper accountability of the systems. The inventory list needs to have enough details to efficiently and accurately, track and report on system components. The inventory list
should also be available for review and audited by a designated workforce member that is responsible for attesting to its accuracy.

The health center should have security measures in place to protect and control digital and non-digital media transported outside of secure areas. This transportation should be accounted for and tracked. Responsibility for transporting such media should be restricted to authorized workforce members or designated individuals such as a trusted third party courier service. Remember that media containing electronic protected health information needs to be secured until it is destroyed by an approved sanitation method such as wiping or physical destruction. If a wiping solution is implemented, this solution should be Department of Defense grade sanitation. As a note, this sanitation process may take some time depending on the size of the media being wiped. There is other degaussing equipment that may be considered to wipe media, but in certain cases, this may be cost prohibitive. A determination on how or what solution is implemented in handling the disposal of media should be conducted based on the resources the health center has available. This will be discussed further in the next section.

Remote Use and Mobile Device

Recently, the Office of the National Coordinator for Health Information Technology’s (ONC’s) Office of the Chief Privacy Officer (OCPO) launched a Privacy and Security Mobile Device Project in collaboration with the Office for Civil Rights (OCR). The goal of this project is to provide better security for mobile devices that contain protected health information. Some examples of these mobile devices are tablets and smartphones. Although the Department of Health and Human Services (HHS) published Security Guidance related to Remote Use December 28, 2006, it appears that health centers have not taken this area of security seriously.

“There have been a number of security incidents related to the use of laptops, other portable and/or mobile devices and external hardware that store, contain or are used to access Electronic Protected Health Information (E PHI) under the responsibility of a HIPAA health center. All health centers are required to be in compliance with the HIPAA Security Rule, which includes, among its requirements, reviewing and modifying, where necessary, security policies and procedures on a regular basis. This is particularly relevant for organizations that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the health center.” (The Department of Health and Human Services 2006)

The guidance separates risks and possible mitigating strategies into three (3) areas of concern over electronic protected health information: accessing, storing, and transmitting.

Social Engineering

Tip #1: Learn to Identify Social Engineering Attacks
Tip #2: Security Awareness Should be Personal and Interactive
Tip #3: Understand the Value of the Information They Possess
Tip #4: Updates are Essential
Tip #5: Develop Scripts
Tip #6: Have and Learn from Social Engineering Assessments
Personnel Security

OSIS cares about its employees. Personnel security is taken very seriously. The company needs to protect its employees and care for their well-being. Employees should stay vigilant at all times and be aware of their surroundings. If something appears to be suspicious, it shouldn’t be dismissed, but rather, a higher sense of importance should be placed on the details of the situation.

Employees should attempt to travel in groups and not alone, as much as possible. They should attempt to travel in lighted areas at night and should attempt to take different routes to and from work so as not to form a routine or pattern. Employees that travel out of town should take special precautions in areas that they are not familiar. Employees should stay at reputable hotels and take special care when transporting sensitive information, files, or equipment.

Trust and Loyalty


Above all else, companies should appreciate their employees’ hard work. All too often, employees will become disgruntled if they are not shown appreciation or respect they feel they deserve. If this occurs, it could definitely increase the company’s chances of becoming a victim of information theft or some other sort of computer-related crime. Your company doesn’t want to become another statistic. Appreciation can be shown in small ways and won’t cost the company much, but the return on investment will be seen in many areas. It will be seen as an increase in productivity and may lower the risks associated with insider criminal activities.

Two important elements that go along with appreciation are trust and loyalty. As part of retention, companies need to realize that one of the most important assets they have in their company is people. You must trust in your employees and make them feel appreciated for the work that they do.

Most individuals are motivated by at least one major factor: being happy. Sometimes it won’t matter how much money you make; if you aren’t happy with what you are doing, you won’t stay around to do it.

As an executive, it is important to listen to your employees since they are usually on the front line in the day-to-day operations of your business. Many times we forget that we may have in-house experts, and instead go out and hire consultants at huge per-hour rates. This may be necessary due to independent audit regulations or the lack of expertise the company may have in a particular area. It may also be more cost effective in the long run to hire a consultant over hiring an employee. I would caution you to make sure that these consultants have your best interest in mind.

As a consultant, I want to preserve my reputation and provide the best possible and professional services that I can to my clients. Unfortunately, there are a lot of individuals who call themselves ‘consultants’, but have no professional experience, education, training, certification, or other items to back up their claim. It is important to get references on these individuals and do your due diligence in conducting background checks. We will talk more of some specific steps you could follow in selecting service providers and to conduct a review of these providers in Section 5.11 Service Providers/Service Level Agreements/Vendor Reviews.
For right now, I would like you to think about trust and loyalty since your security posture can depend heavily on these two items.

“When we are debating an issue, loyalty means giving me your honest opinion, whether you think I’ll like it or not. Disagreement, at this stage, stimulates me. But, once a decision has been made, the debate ends. From that point on, loyalty means executing the decision as if it were your own.” -- Colin Powell

**Laws of Security**

“Your security is only as strong as your weakest control.” – John J. Trinckes Jr.

One of the best articles I found on the basic laws of security is paraphrased here from the *10 Immutable Laws of Security*, written by the Microsoft Security Response Center.

**Law #1**: If a malicious individual persuades a user to run his/her program on their computer, it is no longer their computer.

**Law #2**: If a malicious individual can alter the operating system of a user's computer, it is no longer their computer.

**Law #3**: If a malicious individual has physical access to a user’s computer, it is no longer their computer.

**Law #4**: If a user allows a malicious individual to upload programs to their website, it isn't their website anymore.

**Law #5**: Strong security is always undermined by weak passwords.

**Law #6**: Treat your system administrators well and make sure they can be trusted, since a computer is only as secure as the administrator makes it.

**Law #7**: The decryption key determines how securely your data is encrypted. (If you use a weak encryption algorithm or don't secure the keys, encryption is worthless.)

**Law #8**: Keep your virus scanners up to date since an old .dat file is just slightly better than having no virus scanner installed at all.

**Law #9**: It is very difficult to be anonymous in the real world and on the web. (Your behaviors will determine the level of privacy you will have.)

**Law #10**: “Security is a process… Not a product.” (– phrase coined by Bruce Schneier.)

These laws should be taken to heart since they are fundamental in understanding the principals of good Information Security management.
Technical Safeguards

<table>
<thead>
<tr>
<th>Security Standards</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Safeguards</strong></td>
<td>Access Control</td>
</tr>
<tr>
<td>164.312(a)(1)</td>
<td>R Unique User Identification</td>
</tr>
<tr>
<td>164.312(a)(2)(i)</td>
<td>R Emergency Access Procedure</td>
</tr>
<tr>
<td>164.312(a)(2)(ii)</td>
<td>A Automatic Logoff</td>
</tr>
<tr>
<td>164.312(a)(2)(iv)</td>
<td>A Encryption and Decryption</td>
</tr>
<tr>
<td>164.312(b)</td>
<td>R Audit Controls</td>
</tr>
<tr>
<td><strong>164.312c(1)</strong></td>
<td>Integrity</td>
</tr>
<tr>
<td>164.312c(2)</td>
<td>A Mechanism to Authenticate Electronic Protected Health Information</td>
</tr>
<tr>
<td>164.312(d)</td>
<td>R Person or Entity Authentication</td>
</tr>
<tr>
<td><strong>164.312e(1)</strong></td>
<td>Transmission Security</td>
</tr>
<tr>
<td>164.312e(2)(i)</td>
<td>A Integrity Controls</td>
</tr>
<tr>
<td>164.312e(2)(ii)</td>
<td>A Encryption</td>
</tr>
</tbody>
</table>

**Evaluation**

One of the most important requirements of the HIPAA Security Rule is reflected in 45 CFR § 164.308(a)(8) that states a health center is required to “perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule [the HIPAA Security Rule] and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements [of the HIPAA Security Rule].” This should also be part of the Meaningful Use requirement mentioned earlier.

The only way to prove that solutions implemented as part of policies and procedures is meeting the requirements of the HIPAA Security Rule standards is to perform testing on these measures. It is recommended that an annual technical and nontechnical evaluation is performed on the health center. This should be performed by an experienced and reputable third party provider to maintain independence. Although there may be a lot of highly skilled resources on staff, the unfortunate part to an evaluation is that they may not have enough separation of duties or be independent enough to provide value to the review. Normalcy or the possibility of being short sighted in conducting these types of evaluations points to the support of getting an outside party to conduct such reviews. Furthermore, internal staff may not have the appropriate experience or training necessary to conduct a thorough technical and nontechnical evaluation.

**Vulnerability/Penetration Testing**

To conduct the appropriate technical evaluation, you need to consider a vulnerability/penetration test. What is the difference between a vulnerability test and a penetration test? I use an analogy of a burglar checking a neighborhood for a house to break into. A vulnerability test is synonymous with the burglar checking doors and
windows to make sure they are locked. A penetration test actually starts when the burglar finds an open door or window and gains entry into the house. (It could also start when the burglar decides to break a window and enter the house.) Be aware that not all service providers that perform these types of services are qualified to conduct such services. You should make sure to utilize qualified and experienced assessors to perform these services. The difference between a good and a great evaluation is the quality of the analysis, the ability to interpret the findings into business ‘talk’, and the rationale for justifying expenditures to mitigate risks.

**Access Control**

This standard requires a health center to implement adequate technical policies and procedures for electronic information systems that maintain electronic protected health information in such a way as to allow access only to those workforce members that have been granted access rights under the Information Access Management policies and procedures. This includes restricting certain software programs and allowing only authorized workforce members to utilize these programs that have access to electronic protected health information.

The access control policy should cover at least the following components: the purpose, scope, responsibilities, management commitment, coordination among different departments, and compliance. These policies should be formally documented, disseminated, and reviewed and updated on a periodic basis (i.e. annually or upon any major changes that affect access control). These policies should define the health center’s overall objectives and include all areas where access control is required. Remember, the goal of access control is to allow only authorized workforce members (or other individuals) access and restrict those workforce members (or other individuals) that should not have access to use/disclose electronic protected health information and the devices that store/process this information.

To maintain an acceptable level of access control the health center should implement safeguards, not only for the information systems such as workstations and laptops, but also for the network as a whole. This would include placing firewalls between internal networks and external networks, the use of port security or network access control to limit unauthorized devices from connecting to the network, and deploying encryption capabilities.

The health center should determine what type of access control would work best in their environment. For instance, would identity-based, role-based, or attribute-base policies work best in the health center’s environment? Identity-Based Access Control (IBAC) utilizes the user’s identity to grant access to specific objects or data. For example, each workforce member may have access to their own private working directory, but not have access to each other’s directory based upon their own unique login credentials. In Role-Based Access Control (RBAC), the access is determined by the information system rather than the individual owner. For example, a workforce member is assigned a ‘nurses’ role. This means that this workforce member would have access to any information that the system recognizes as being authorized for that role. Based on the role and the role authorization, transactions can be performed such as editing a patient’s electronic medical record based upon the transactions that are allowed under the workforce member’s role. In Attribute-Based Access Control (ABAC), access is granted to a workforce member based on their attributes rather than their rights. For example, let’s
say that information about a patient may only be seen by workforce members that are over eighteen (18) years of age. In this case, any workforce member that can prove the claim of being over eighteen (18) will be granted access to this specific information.

The health center should be able to document the roles of each user for each application, information system, server, or other device that may hold electronic protected health information. In addition, the health center should determine the access capabilities of their systems such as creating, viewing, modifying, or deleting the information. Access enforcement mechanisms should be used such as access control lists, matrices, encryption, and other controls that will be discussed below. Not only does the health center want to control access at the physical level, but they need to control access at the network and application levels. In case of emergency situations, these automatic controls should have an override that can be issued and audited in accordance with the health center’s business continuity and disaster recovery policies and procedures.

The documentation of roles is important to determine if there are separations of duties to prevent against fraud or collusive acts. For example, a workforce member conducting a transaction should not be the same individual that reviews or audits the report of those transactions. Some other duties that should be considered to be separated between different workforce members are operational functions and informational support functions. Related to information support functions, duties should be separated for system administrative functions and security testing functions. The same individual writing software code should not be the same individual testing the code. In addition, workforce members that administer access control functions should not be the same workforce members that audit or review these functions. Finally, it is recommended that system administrator accounts are set up for different roles and accounts should be assigned at the least privilege with only the amount of privileges necessary to perform the assigned function.

Wireless networks have become mainstream and are now being widely deployed throughout healthcare providers’ networks. There are, however, some special consideration and configurations that should be implemented when utilizing this technology. For instance, wireless network devices deployed on a network should have all of their default configurations modified. This includes not broadcasting the Server Set Identifier (SSID), changing the SSID to a unique identifier, not utilizing Wired Equivalent Privacy (WEP), placing a firewall between a wireless access point and the local area network, utilizing strong Virtual Privet Network (VPN) encryption technology, copying wireless audit logs to a secure log server, and routinely searching for rogue wireless access points that may not belong to the health center. A workforce member, or other individual, that may be authorized to use the wireless technology should accept a liability disclaimer that releases the health center from any damage and identifies the appropriate use of this technology.

All devices connected to the network should require authentication prior to gaining any access to the resources on these devices. For example, there shouldn’t be any directories that are accessible or shared out to everyone on the network. In addition, File Transfer Protocol (FTP) that is generally used to transfer files from one system to another should be limited. Due to the insecure nature of FTP, it is recommended not to be used; instead, SSH File Transfer Protocol (SFTP) or FTP over Secure Socket Layer (SSL)/Transport Layer Security (TLS) - (or FTPS) - should be considered. If FTP is being
utilized on the local area network (LAN), then it needs to require authentication. Anonymous FTP servers are strongly discouraged.

All network devices or services should be kept up to date to mitigate known vulnerabilities. These devices should not be deployed in production environments with any default configurations still set. For instance, network devices such as routers or switches need to have their account usernames and passwords change for their administrative consoles or configuration sessions. In cases of software packages or web server interfaces, the administrative accesses should not be left as default. It has been my experience that vendors, even those in the security arena, may install their information systems on the network without changing their settings. I have, on several occasions, compromised the entire network by targeting these vendor systems and leveraging their access levels on the network to gain total control of the network. Any devices connecting to the network becomes the health center’s responsibility and should be tested to verify that the proper security controls are implemented on these systems.

Firewalls are an essential piece of network equipment that can be utilized to comply with the access standards. Firewalls should provide ‘state-ful inspection’, or dynamic packet filtering, that only allows established connects to enter the network. Firewalls can be a bit difficult to configure and it is recommended to employ the resources of an outside expert if these resources are not available in house. Firewalls normally work from a standpoint of Access Control Lists (or ACLs). ACLs only allow those networks or devices that are implicitly identified in their rules access to other resources or devices on the network. All other networks or devices have an explicit ‘deny all’. Firewall rules should be designed to allow access specifically from one source to one destination over specific protocols or ports. These firewall rules should be reviewed on a regular basis and any entries into the ACL should be justified and documented.

Unique Use Identification

Each and every workforce member should have a unique user identifier when logging onto the workstation, network, or software program that has access to electronic protected health information. In many cases, this unique user identifier is known as the username or the user ID. This unique identifier should be utilized to track the user’s activity within the information system and users should be restricted from sharing this information with anyone else. To authenticate the user, a password is generally used with the unique user identifier.

The health center should have a formal access control policy in place that should help guide the development of procedures related to the implementation of access control authorization and restrictions. Access control procedures should include the management of information system accounts. Management of accounts includes:

- Account Establishment;
- Account Activation;
- Account Modification;
- Account Termination; and
- Eventual Account Removal.

In addition, the access control procedures should include the process for initial access, process for increasing or restricting access, and a process for providing access to different applications or other systems that the user may need. Once the access control
procedures have been developed, they will need to be effectively implemented, communicated to all workforce members, and compliance with these policies and procedures need to be enforced. A designated workforce member, such as the Security Official, should be responsible for managing the procedures for access control.

One of the ways that access control policies and procedures can be communicated to the workforce members is through training specific to access control and management of access control. All new workforce members should be instructed on these policies/procedures and others related to securing electronic protected health information. All workforce members should have refresher training and advised of any updates to the access control policies and procedures.

Information system accounts, as per policy and procedures, should be managed in a certain way. System accounts should be identified by account type. For example, there may be individual accounts or group accounts set up for an information system. There may also be system or application level accounts for a particular information system or application. Finally, there may be guest, anonymous, or temporary accounts that may need to be treated with special care such as additional monitoring for these accounts or disabled entirely from the information system.

One of the easiest ways to manage system accounts is by setting up group memberships. These groups may correspond to the roles of the individual workforce members within the health center. Conditions will need to be established on group memberships for the appropriate access levels required on the information system and appropriate requests for approval to these groups need to be established. For instance, the health center may have an accounting group established in a specific information system or application. One of the conditions placed on this group is that only workforce members working in the accounting department will be authorized to be a member of this group. The manager of the accounting department should send a request to the IT department to establish an account in this group for one of their workforce members. Once the account is set up within the group, the individual will inherit all of the rights or restrictions placed on this group. Depending on the information system and its function, the accounting group, for example, may or may not have privileges to access this information system or other information systems that do not run accounting functions. If the workforce member leaves or transfers positions, procedures should be implemented to modify or terminate the workforce member’s access. A review or audit of system accounts needs to be conducted on a periodic basis to ensure compliance with access control policies and procedures.
There has been a lot of emphasis placed on the protection of passwords with little thought about the unique user identifiers or usernames. Since the username is half of the username/password authentication scheme widely deployed in most information systems, the username should be protected just as the password. Most organizations set up accounts using a person’s name or a portion of the name. For example, an account may be the first initial and last name of the person to which that account belongs. This may be easy to manage, but it is also easy for a malicious person to figure out. A possible solution could be the assignment of a number that may be a little more difficult to identify as part of this security schema for username/password authentication. Furthermore, this unique identifier can be different for different types of applications or when accessing different types of data. Remember, unique identifiers are used to track all system activities involving electronic protected health information back to a specific user. This audit trail is necessary to ensure compliance with policies and procedures.

Since most information systems are deployed with a privileged user account, ‘super user’ account, or ‘root’ account, it is imperative that this account is not left with any default settings. For instance, the administrator account in a Windows operating system is generally named ‘administrator’. If possible, this account should be renamed or disabled.
after another account is created to take its place. In addition, for auditing purposes, accounts should not be reused and every new user should receive a unique user account.

Passwords are normally required with a unique user identification to authenticate a user. There are several ways that passwords are compromised. Most of these have to deal with the lack of control that a user places over the security of their passwords. One example of this is by using simple passwords. A password like ‘123456’ or ‘11111111’ is not appropriate and provides just a little more protection than if the password was just ‘blank’ in the first place. Common passwords such as ‘Password1’ and ‘qwerty’ should also not be used. Most password hacking programs utilize a dictionary list that can automatically insert passwords into the password field. It is recommended that passwords do not contain any type of words that may be found in a dictionary, common misspellings of these words, these words spelled backwards, or slang terms. Passwords should also not be the same as the unique user identifier or a hybrid combination of the name of the health center such as ‘[health center name]1234’.

Since passwords are used for all types of resources on the Internet and other applications, it is recommended not to use the same password across different sites. For instance, email passwords should be different than banking passwords that are different than passwords for social media sites. If the passwords were all the same for these accounts than if one of these resources were compromised, all the applications could be compromised as well.

The following are some recommendations that could be followed to keep passwords secure:

1. Don’t tell anyone your password.
2. If passwords need to be written down to remember them, make sure they are secured. Replace a password list with a ‘tip list’ to assist in remembering passwords.
3. Change passwords on a routine or periodic basis.
4. When entering passwords, cover the keyboard and make sure no one is around that is watching.
5. Make passwords at least eight (8) characters long with a mix of uppercase, lowercase, numbers, and symbols.
6. Use strong passwords that can be remembered, but can’t be guessed. For instance, use a phrase from a song and replace symbols with similar characters or words like ‘to’ with a number ‘2’.
7. Use the keyboard as a palette to make shapes. For instance, to make a ‘V’ shape, use ‘$rfvGY7’. Slide your fingers up or down the keyboard to create different combinations.
8. Avoid entering passwords into unknown systems or public use systems like Internet cafes. These systems could have software installed that could be used to capture the credentials entered.
9. Avoid entering passwords over unsecured Wi-Fi connections. Make sure that any site requiring passwords has a secure connection (i.e. through HTTPS).
10. If a site provides a password strength analyzer to determine how strong a password entered is, make sure to follow its advice and make the password as strong as possible. (Siciliano 2011)
Emergency Access Procedure

A health center should identify all workforce members that may need access to electronic protected health information in the event of an emergency. A health center is required to have policies and procedures in place to provide appropriate access to these workforce members in emergency situations. In addition, a health center should have a policy in place that designates a responsible workforce member to make a decision about activating emergency procedures and the appropriate time these should be activated. These emergency procedures should contain methods of supporting continued operations in situations that affect normal operations. It should be determined whether or not the information systems can allow for the automatic failover to emergency configurations or will a workforce member have to manually configure these failover procedures.

Automatic Logoff

Health centers should implement an automatic logoff of information systems after a period of workforce member inactivity. This automatic logoff capability is generally seen within a Windows network through a group policy that can enforce a password protected screen saver after a certain period of inactivity. This inactivity period is generally recommended to be ten (10) minutes, but could be adjusted for a group of workforce members that may require a little more time. This could also be adjusted in cases where certain processes are running on information systems, but may not be picked up as activity and if the session was terminated, the process may not complete as desired. The automatic logoff feature should be activated on all workstations with access to electronic protected health information.

Encryption and Decryption

A health center needs to identify or address all electronic protected health information that requires encryption so that it is restricted from access by individuals or other software programs that may not be granted access rights to this information. This encryption standard is addressable under the Security Rules; however, it doesn’t mean that it is optional. The encryption should be reasonable and appropriately implemented to prevent unauthorized access to electronic protected health information. The health center may decide to encrypt electronic protected health information in transit and while being stored depending on the risk of exposure of the information in these two states.

Not All Encryption IS the Same

Breach Notification ‘Safe Harbor’ Exception

Purpose

This white paper gives an overview of the Breach Notification ‘Safe Harbor’ Exception provided for in the HITECH Act as it relates to rendering unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Overview
An acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rules is presumed to be a breach unless a health center (or business associate) demonstrates that there is a low probability that the protected health information has been compromised based on the risk analysis performed.

Unsecured protected health information is defined as protected health information that is not secured through the use of a technology or methodology specified by the Secretary (of the Department of Health and Human Services) in guidance and provides that the guidance specify the technologies or methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.\(^1\)

The ‘Safe Harbor’ exception applies when a health center (or business associate) that implements the specified technologies and methodologies with respect to protected health information are not required to provide notification in the event of a breach of such information. The guidance specifies encryption and destruction as the two methods for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals, thus making it secured and exempt from the breach notification obligations.\(^2\)

Electronic protected health information is considered encrypted as specified under the HIPAA Security Rule by using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process (or key) that might enable decryption has not been breached.\(^3\)


As a special note of reference, NIST SP 800-52 was withdrawn on March 13, 2013 and is now considered an archived publication. For this reason, this paper refers to the FIPS 140-2 standards.

**FIPS 140-2**

Some FIPS compliant symmetric keys are:
- Advanced Encryption Standard (AES)
- Triple-DES Encryption Algorithm (TDEA)
- Escrowed Encryption Standard (EES)

Some FIPS compliant asymmetric keys are:
- Digital Signature Standard (DSS)
- Digital Signature Algorithm (DSA)
- Ron Rivest, Adi Shamir, and Leonard Adlemann Algorithm (RSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

**SSL and TLS**
The most common cryptographic protocols used in securing communication over the Internet are Sockets Layer (SSL) and Transport Layer Security (TLS). These protocols utilize asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

There are different versions of SSL and TLS. Some of the older versions (SSL v2, SSL v3, and TLS v1) may not be secure. These versions may be susceptible to a Browser Exploit Against SSL/TLS (BEAST) attack. In addition, although SSL v3 is the most secure of the SSL protocol versions, it is not approved for use in the protection of Federal information (and possibly protected health information) because it can partly rely on cryptographic algorithms that are not FIPS-Approved (or compliant).

Recommendations

A health center (or business associate) is required to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. Encryption and decryption could be one of these technical security measures implemented and encryption/decryption is considered an addressable standards under the HIPAA Security Rule. A health center (or business associate) must address the implementation of a mechanism to encrypt and decrypt electronic protected health information. Although the use of non-FIPS compliant encryption meets the standard of the Security Rule, if a breach were to occur of the information that did not abide by the guidelines, it will not fall under the ‘safe harbor’ exception. Based on the new Omnibus Rule, the presumption of a breach occurring could generate the breach notification requirements. Although a low probability of a compromise could be demonstrated through the required compromise risk assessment, it is recommended to utilize FIPS-compliant encryption algorithms for data at rest and in motion.

For these reasons, it is recommended that all secure network connections utilizing SSL or TLS, enforce the use of TLS v1.1 or TLS 1.2 encryption utilizing strong ciphers with at least 128 bit key ciphers.

IIS Crypto is a free tool from Nartac Software that gives administrators the ability to enable or disable protocols, ciphers, hashes, and key exchange algorithms on Windows Server 2003, 2008, and 2012. This tool is based on instructions from Microsoft on how to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll.

External testing of all publicly available network devices should include testing of SSL/TLS and recommendations should be made on strengthening the configurations if any weak ciphers are discovered.

In cases where systems need the use of a weaker protocol, a formal documented exception should be made and other mitigating controls should be implemented to ensure the security levels of protected health information are reasonable and appropriate accordingly.

Source/Resources

1 13402(h) of the HITECH Act
2 74 FR 42741-43
3 Definition of encryption – 45 CFR 164.304
Audit Controls

A health center is required to implement audit control mechanisms that are reasonably implemented to record and examine activity in information systems that contain or use electronic protected health information. Most current information systems have built-in audit control capabilities and the health center should identify what type of logging is currently in place. Audit controls need to be adequately implemented to allow the health center to adhere to its policies and procedures regarding compliance with the implementation specifications for Information System Activity Review.

The audit and accountability policy should cover at least the following components: the purpose, scope, responsibilities, management commitment, coordination among different departments, and compliance. These policies should be formally documented, disseminated, and reviewed and updated on a periodic basis (i.e. annually or upon any major changes that affect auditing). These policies should define the health center’s overall objectives and include all areas where access control is required. Remember, the goal of auditing is to record and examine activity in information systems that affect electronic protected health information. This includes any hardware, software, or procedural controls in place to track such activity as modifying electronic protected health information within information systems.

Based on the health center’s risk assessment and other business needs, they should be able to define a list of events that need to be audited. These events should cover a cross section of audit-related information supported by input from departments across the entire health center. There should be documented rationale behind the list of events chosen to adequately support an investigation after a breach or incident occurs. The audit records generated from logging should, at a minimum, detail the type of event, the date and time of an event, the possible identity of the subject of the event, and the information that may have been affected by the event. There also needs to be a workforce member or designated group that is responsible for the overall audit process and reporting. Time frames for audits should be defined within the audit policies and procedures.

Auditing or logging could take up a lot of hard drive space on an information system. Depending on the types of events that are recorded, storing this information could become exceedingly difficult or expensive. It may not be feasible or necessary to record every possible event so it is important to decide what reporting is essential to the health center’s needs. Storage of audit logs should be carefully monitored so that important reporting information is not overwritten in the event that capacity is exceeded. Since these logs could be extremely large, it is important that a solution is implemented to filter or aggregate the data into an easily readable format so that unusual activity can be identified and findings reported to the designated workforce member such as the Security Official. These thresholds also need to be analyzed so that false-positives are kept to a minimum and resources are not wasted in tracking down non-events. Consideration may
be made to store audit logs on a completely separate server with all the necessary controls implemented to ensure the integrity of the logs stored within.

The auditing or logging process should be flexible. It should monitor for the creation, review, modification, or deletion of electronic protected health information. Based on analysis, reporting, or other audit reviews, auditing should adjust for changes in risk levels of the health center obtained by credible sources such as law enforcement or other intelligence agencies. The auditing process should also include reporting that approaches almost near real-time review or notification capabilities to allow for the immediate reaction to any suspicious activities identified. This suspicious activity, for example, could include any unauthorized or inappropriate access to electronic protected health information.

The auditing process should be reviewed on a continuous basis and at least annually along with updating the system capabilities as necessary. This audit process should have metrics designed to assess the effectiveness of the process and to assist in the determination of improvements. One of the methods that I have seen performed to ensure the effectiveness of the audit process is by testing. When security testing is performed, such as a penetration test, an evaluation on the auditing process can be conducted. Does the monitoring or logging implemented pick up the scanning activity? If access is gained on the system through an exploitable vulnerability, did the audit events log such activity? Did the appropriate workforce members receive notification that any suspicious activity was occurring during the security testing? These are some of the questions that should be answered and items reviewed during these types of exercises. If the auditing process doesn’t provide the expected results, it should be updated appropriately.

Some recommendations regarding the configurations of firewalls have already been touched upon, but along with the access controls that these firewalls provide, they should also provide logging capabilities. Firewalls should be audited for failed and successful connections. Each time a device connects or attempts to connect to another device through the rules provided for in the access control list (ACL), the firewall should be logging this activity. These firewall logs should be reviewed on a daily basis by someone with the experience to identify suspicious activity. In addition, these firewall logs should be stored, for consistency of six (6) years, in accordance with the policies and procedures.

**Integrity**

Integrity deals with the alteration or modification of data. A health center must implement policies and procedures to secure electronic protected health information from unauthorized alteration, modification, or destruction. Information systems and software programs should have the capabilities of maintaining the integrity of electronic protected health information through the use of integrity verification solutions that can identify information that has been modified through human error, omission, or malicious tampering.

The system and security information integrity policy should cover at least the following components: the purpose, scope, responsibilities, management commitment, coordination among different departments, and compliance. These policies should be formally documented, disseminated, and reviewed and updated on a periodic basis (i.e. annually or upon any major changes that affect integrity). These policies should define the health center’s overall objectives and include all areas where access control is
required. Remember, the goal of integrity is to restrict any unauthorized modification to electronic protected health information.

A health center should have policies and procedures in place that details how workforce members (and other users) are authorized to access electronic protected health information. These procedures should include a list of all users that have access to electronic protected health information and details the rationale behind the access granted such as the roles or responsibilities that require a certain workforce member authority to access the information based on their job requirements. Their job roles or requirements should detail the ability to alter or destroy certain electronic protected health information.

A health center needs to train their workforce members on how to use electronic protected health information. Workforce members need to be aware that there are audit trails available that establishes monitoring of access to electronic protected health information. Workforce members also need to be aware that sanctions can and will be disseminated based on violation of the health center’s access policies and procedures. Any additional training should be considered to mitigate human errors when dealing with the integrity of the data.

Through a risk assessment or analysis, the health center should have identified situations where unauthorized modifications could be made to electronic protected health information such as from disgruntled workforce members, hackers, third party providers, or possibly business competitors. The health center should determine what they can do to secure electronic protected health information in these systems and mitigate the risk of unauthorized access to an acceptable level. Examples of some mitigation controls could be access controls to information systems that store electronic protected health information and encryption while this electronic protected health information is in transit.

The risk assessment should also document the integrity requirements for the electronic protected health information. These requirements should be supported by management or any other designated workforce member responsible for security related functions. These integrity requirements should also be disseminated to the workforce members utilizing the information systems through written policies or procedures. It is important that audit controls take into account methods to adequately address the integrity of electronic protected health information. There may be a situation where current integrity controls are not enough and additional solutions such as a quality control process may need to be implemented to ensure the data is accurate.

As it relates to integrity, the health center should determine what types of periodic backups will be conducted. These backups could be conducted on user-level information, system-level information, or both. System and security documentation should also be considered as critical data that require periodic backups. Backups should be treated as confidential and integrity controls need to be implemented to secure this information especially at off-site storage locations and during transit outside of controlled areas. Backups should be restricted and only authorized workforce members or designated individuals should be allowed access to them. If backups are done through digital methods, the information should be protected across both the internal and external network connections.
Authentication

A health center must implement an authentication mechanism to electronic protected health information that will validate the person or entity accessing this information is the authorized person or entity verified to have access to this information. The risk assessment will assist in determining the proper authentication method implemented within the health center. Authentication can be conducted by utilizing one (1) or more of the following three (3) factors:

1. an authorized individual is required to present something that only they would know prior to gaining access;  
2. an authorized individual is required to present something that they would only have prior to gaining access; or  
3. the authorized individual is presenting something unique to only that individual prior to gaining accesses.

A health center may consider using a multi-factor authentication process that involves utilizing two (2) of the three (3) factors. Some examples of these authentication factors are passwords or Personal Identification Numbers (PINs). These are something that only an authorized individual should know and no one else could obtain or guess. Smart cards, tokens, or even a key are other examples of something that an authorized individual may possess. Unique items that authorized individuals may use for authentication could be biometrics (i.e. fingerprints), voice recognition, facial patterns, or iris patterns. These are items that, in theory, no other individual would possess or could not be duplicated.

A health center needs to have formal established documented authentication policy and procedures that are clearly communication throughout the organization and to all workforce members. These authentication procedures need to be maintained and updated for all information systems, software applications, network devices, and auditing or monitoring tools utilized within the health center. Workforce members need to be trained in the proper authentication methods and there should be trained staff maintaining these systems. Remember that the goal of authentication is to verify and validate that the workforce member is whom they claim to be. As part of the security testing, the authentication method utilized by the health center needs to be tested to validate that the solution is working as expected.

A health center should determine the reasonable and appropriate level (or type) of authentication that should be utilized to grant access to information systems containing electronic protected health information. As discussed, there are several different types of authentication methods that a health center could consider using. The main factor in deciding which is best is ultimately determined by the culture of the health center. If security is considered a high priority then the most stringent authentication methods will probably be deployed such as multi-factor authentication using tokens or biometrics along with username/password combinations. On the other hand, if security is lax, the culture of the health center may dictate only username/password combinations to authenticate to the information system rather than the added second layer of authentication. There will always be a battle between functionality and security, but in the end, work still has to get done and reasonable security controls still need to be implemented.

In addition to authenticating individuals or users of the information systems, the information systems themselves need to be hardened. All information systems or devices on a network should require some form of authentication. Networking devices such as
routers, switches, firewalls, intrusion detection systems, intrusion prevention systems, etc. need to have unique passwords set and configured in such a manner that only authorized individuals can access them.

Maintenance accounts, such as the ‘SA’ account on SQL databases, need to be secured so that only authorized administrators can access these databases. As a note of reference, the authentication process implemented should not compromise the authentication information itself. For instance, if passwords are utilized for authentication, the password file that stores this information should be encrypted.

**Transmission Security**

A health center needs to implement adequate technical security measures to guard against unauthorized access to electronic protected health information being transmitted over an electronic communications network. This is especially important if electronic protected health information is being transmitted across a public accessible network like the Internet. This data needs to be encrypted. In an internal network, controls implemented in the network devices such as switches, routers, and firewalls may provide the necessary levels of security to guard against unauthorized access to electronic protected health information being transmitted on the local area network (LAN).

A health center should have formal policies and procedures in place to detail the methods that will be used to secure electronic protected health information while in transit. Procedures should identify any methods that will be used to implement the transmission security policy. These methods may include hardware or software to secure the transmission of electronic protected health information. Trained workforce members should be monitoring this transmission to ensure that the information is secure. The procedures should also formally document the requirements for transmitting this type of information that is approved by management or a designated official. Through the health center’s risk assessment, scenarios that put this information at risk should be identified. Through security testing, electronic protected health information in transit should be verified secured from unauthorized access. Any deficiencies discovered through this review should be corrected accordingly.

To further limit unauthorized access, it is recommended that all ports or protocols not being utilized for business purposes should be disabled on the information systems. Protocols such as the Simple Network Management Protocol (SNMP), Finger, Trivial File Transfer Protocol (TFTP), or other unnecessary protocols should be restricted on the network.

**Business Associates**

At times, health centers require certain functions, activities, and services be performed from other companies that are NOT a member of a health center’s workforce that may involve the use or disclosure of individually identifiable health information. Some of these functions, activities, and services may include, but not limited to, claims processing, data analysis, utilization review, billing legal services, accounting/financial services, consulting, administrative services, accreditation, or other types of services (such as managed IT services). Companies that provide these types of functions, activities, and services to health centers are known as “business associates” as defined in 45 CFR § 160.103. In addition, a health center may provide these types of services and be a
business associate to other health centers. If services of a company do NOT involve the use or disclosure of protected health information or if access to such information is incidental then the organization or person providing these services are NOT considered a business associate. Some examples of a business associate that would have access to protected health information may include consultants, CPAs, lawyers, medical transcriptionists, benefit administrators, claim processors, etc. As of July 2010, there is an estimated 1.5 million organizations that are considered business associates of health centers. As a point of reference, the new ‘Omnibus Rule’ requires these business associates (and subcontractors of business associates) to be HIPAA/HITECH compliant along with any subcontractors or other associates of these business associates that may have access to electronic protected health information will also need to comply with the HIPAA/HITECH regulations.

The Omnibus Rule also added the following specific organizations to the list of business associations:

- Patient Safety Organizations
- Health Information Organizations
- E-Prescribing Gateways
- Other data transmission services that require routine access to PHI
- Persons that offer personal health records to one or more individuals on behalf of a health center

To meet some of the requirements, under 45 CFR 164.308(b)(1), a health center must obtain “satisfactory assurance” from a business associate that they will appropriately safeguard electronic protected health information. This assurance is met through a business associate agreement. Although there is no specific requirement to perform additional review of a vendor above and beyond getting a business associate agreement signed, due to recent breaches reported by third party providers, it is recommend that additional due diligence activities by developed to review the business associate security practices. We will also find that business associates will be audited by OCR.

One of the major change as a result of the finalization of the Omnibus Rule is the direct liability that business associates now have in protecting and securing electronic protected health information. Business associates are required to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information just as a health center is required to do. In addition, the Omnibus Rule re-defined a business associate as any organization that creates, receives, maintains, or transmits protected health information on behalf of a health center. Furthermore, any agent or subcontractor of a business associate is also considered a business associate and therefore, directly liable for the security of protected health information. These agents, or subcontractors, must enter into a business associate agreement with the business associate and comply with the HIPAA Security Rules along with any applicable Privacy Rules.

### Business Associate Contracts

For a health center to utilize another company for “business associate” type services, the health center must have a contract or other agreement in place with the business associate. This is to ensure the protection and safeguard of the health centers' individually identifiable health information. The health center must obtain satisfactory
assurance that the business associates will use the protected health information only for its intended use, will safeguard the information from inappropriate use, and will assist the health center in complying with the HIPAA/HITECH Privacy and Security Rule. A written contract complies with the satisfactory assurance requirements of the HIPAA/HITECH Privacy Rule; however, it may lack the necessary assurance for the new ‘Omnibus Rule’ related to due diligence under the HIPAA/HITECH Security Rule that will be discussed later.

Per 45 CFR § 164.504(e), the business associate contract must contain, at a minimum, the following elements:

• "Describe the permitted and required uses of protected health information by the business associate;
• Provide that the business [associate] will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
• Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract."

In addition, "where a health center knows of a material breach or violation by the business associate of the contract or agreement, the health center is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a health center is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR)."

As required by 45 CFR § 164.308(b)(1), a health center should obtain “satisfactory assurance” that their business associates will “appropriately safeguard the electronic protected health information created, received, maintained, or transmitted on the health center’s behalf.” The Organizational Requirements under 45 CFR § 164.314 govern the elements related to the components required in the contracts of business associates while The Security Standards: General Rules under 45 CFR § 164.306 define the appropriate safeguards surrounding the security of the electronic protected health information required to be met by the business associate of the health center.

Although ‘satisfactory assurance’ is met through a ‘written contract or other arrangement’, it is recommended that the same level of due diligence met by the health center to secure electronic protected health information is being met by the business associate. One way in which this assurance can be satisfied would be to obtain a review or evaluation from an independent third party providing an opinion or detailing the level of security in place by the business associate. This review should be periodically performed on all business associates to ensure compliance and to evaluate the effectiveness of the security controls implemented by the business associates.

Summary

In summary, health centers should assume that an audit will happen; it is the question of ‘when’, not ‘if’. Health centers should be prepared for an audit. If internal resources are not available, they should seek assistance from professional and experienced third party service providers to assist. Staff members responsible for compliance need to take ownership of the process and health centers, themselves, need to have a
security/compliance mind-set. The information security management program begins from the risk assessment. Risk assessments should be on-going. With the changes implemented by the Omnibus Rule, it is important for health centers to update policies, procedures, revise business associate agreements, and modify Notice of Privacy Practices accordingly. It cannot be stressed enough how valuable training, educating, and making staff members aware of security/compliance related matters along with defining the health center’s expectations appropriately for their staff. Consistently evaluate and adjust efforts to make sure they meet objectives. Finally, document everything the health center does when it comes to information security and compliance efforts.

Services

• HIPAA Compliance Program
  • HIPAA/HITECH Information Systems Security Risk Assessment
    • Administrative Safeguards
    • Physical Safeguards
    • Technical Safeguards
      • Internal/External Vulnerability/Penetration Test
    • Organizational Requirements
    • Policies, Procedures, & Documentation Requirements
  • Policies/Procedures
  • Security Awareness Training
• Mitigation Management
• Vendor Due Diligence
• Security Incident Response Handling
• Business Continuity/Disaster Recovery Planning
• Subject Matter Expertise