HIPAA SECURITY AND POLICIES AND PROCEDURES

By: Michele Cuper

THESIS FOR MASTERS DEGREE

INFORMATION ASSURANCE

CAPS 795

DAVENPORT UNIVERSITY

PRESENTED TO:

DR. LONNIE DECKER

JULY 25, 2012
Abstract

With all the Privacy Laws in the Health Care field today anyone that works with confidential information should know how to protect that information. They should understand the company’s policies and procedures and follow them. If the company does not follow certain policies and procedures they could be out of compliance. Companies need to have good ethics and keep confidential information safe and secure. Training is a key resource in being HIPAA Compliant. If your staff doesn’t know or understand HIPAA then they will have a hard time being compliant with HIPAA.

Hypothesis: By training staff on HIPAA security a company can lower their risks and also an employee’s risks of breaching confidential information.
Table of Contents

Abstract .......................................................................................................................... 2

Table of Contents ........................................................................................................... 3-4

Introduction to HIPAA ................................................................................................. 5-6

Literature Review .......................................................................................................... 6-7

Research ......................................................................................................................... 7

  HITECH ACT ........................................................................................................ 7-8
  HIPAA AND NETWORK SECURITY ...................................................................... 8-9

Filing a Complaint ........................................................................................................ 9

Security ........................................................................................................................ 9-11

HIPAA Compliancy ..................................................................................................... 11-13

Case Example ............................................................................................................. 13

Main HIPAA Requirements ....................................................................................... 14

HIPAA Training Reasons ......................................................................................... 14-15

Steps to take to help you become HIPAA Compliant ............................................. 15-17

HIPAA/HITECH ........................................................................................................ 17-20

Training ...................................................................................................................... 20-21

Email Encryption ....................................................................................................... 21

Your Filing System and HIPAA ............................................................................. 21-22

HIPAA Audits ............................................................................................................ 22

HIPAA Violations ....................................................................................................... 22-23

Awareness .................................................................................................................. 23-24

Breaches ..................................................................................................................... 24-25
Research Methodology........................................................................................................25-27

Suggestions for Further Research........................................................................................27

References................................................................................................................................28-31

Appendix A- Acronyms.............................................................................................................32

Appendix B- Tables..................................................................................................................33-35
**Introduction to HIPAA**

A person’s privacy is very important and with all the technology in today’s world a lot of people can gain access to a lot of information easier than in the past.

In 1996 there was an act called the HIPAA (The Health Insurance Portability and Accountability Act) created to protect health information. This will protect the privacy and also security of that based on certain rules that were established by the HHS (Health and Human Services) Department. HIPAA has changed how things work in the health care field. There are now requirements that need to be followed. With all the new technology and companies striving to move to being paperless a lot has changed in the health care field and computers are being used more often to store confidential information. This increases the risk of security (U.S. Department of Health & Human Services, n.d.c).

The Security and Privacy Rule Title 45 Public Welfare Part 164 Subpart C 164.312 Technical Safeguards states the required and addressable parts:

- Required to have a unique identity assigned.
- Required to have an emergency process for accessing information.
- Addressable to have your computer screen logoff after a certain amount of time that no one is using it.
- Addressable to encrypt computer information and decrypt computer information.
- Addressable to have security measures implemented for transmitted electronic computer information making sure it is not modified improperly.
- Addressable to have something in place for encryption when necessary.
(National Archives And Records Administration 1985, 2012).

**Literature Review**

Since the Privacy and Security rule seem go hand in hand this paper will be focusing on both rules and trying prove this hypothesis statement.

**Hypothesis:** By training staff on HIPAA security a company can lower their risks and also an employee’s risks of breaching confidential information.

Do companies believe that nothing will ever happen to them? Is that why they usually don’t like to spend money on security, or do they feel the risk is worth taking? Maybe they just need to be more educated on security and HIPAA compliance. After working in the healthcare field for several years and computer field for over 12 years understanding security and the importance of HIPAA compliance is a must in the healthcare field. Training should be number one in the process of being HIPAA compliant.

When you look around today most people have some sort of portable or mobile device. Most of these devices are a lot like computers or are actually computers. Also, most are able to store a lot of information. Even the very tiny devices can store a lot more information then they use to be able to. This information needs to be protected when dealing with confidential information. There have been a lot of changes that technology brings to the personal and workplace environment. All this new technology can be a nightmare for the IT Department if not managed correctly. How do you manage all the staff and technology correctly? Good policies and procedures and proper training can help manage staff and technology. The focus in this paper will be on training. Training plays an important part of being HIPAA compliant. Policies and procedures cannot be just in place and hope for the best. Also, how many people really read the handbook from front to back? Involve your staff and teach them why it is
important to keep confidential information secure and how to go about doing that on a daily basis.

**Research**

The purpose of this paper is to explain the importance of training and research what it takes for a company to be HIPAA Compliant. Also, explaining what is expected of companies if there is an audit. How does HIPAA training play a big part in HIPAA Compliance and who in the company needs to be trained and why?

**HITECH ACT**

As part of an economic stimulus bill President Obama created the HITECH ACT which stands for The Health Information Technology for Economic and Clinical Act on the 17th of February of 2009. The bill was called The American Recovery and Reinvestment Act of 2009 (ARRA). This bill states that beginning 2011 until 2015 there will be financial incentives for those in the healthcare field that demonstrate meaningful use of Electronic Health Records (EHR) and also grants for those supporting the infrastructure of IT for training centers (TechTarget, n.d.). HITECH gives incentives but it also has added stricter requirements and penalties to HIPAA. More than were stated previously in the HIPAA requirements. With EHR you are able to track disclosure of what data was accessed by whom and when it was accessed. Companies need to be prepared in case of a breach. “If a breach of patient information happens at your practice, the legislation requires you to post information publicly about it if the security breach affects 10 or more patients. If a security breach affects 500 or more patients, practices must notify all of their patients, a local media outlet, and the HHS secretary.” (Bakhtiari, E., 2009).
The media loves attention so you better be prepared. Identity theft has grown with all the digital information and Business Associates also need to be in compliance with HIPAA if dealing with patient data (Bakhtiar, E., 2009).

Figure 1 – Resolutions by Year and Type (U.S. Department of Health & Human Services, n.d.a).

**HIPAA AND NETWORK SECURITY**

Years ago it wasn’t really a big deal if an employee looked at patient data even if they had nothing to do with that patient but now with HIPAA employees’ cannot do that anymore. It has become more of a CIA (Confidentiality, Integrity, and Availability) model. Not everyone is authorized to see patient data and network security plays a big role. Network security consists of keeping the data secure on the network, protecting the network from malicious attacks and tracking and reviewing reports of the network to see the behavior and to determine if someone is
trying to gain access that should not have access. Access should be based on an employee’s role and security must be implemented. Updates must also be applied. If there is an intrusion on the network then civil and criminal charges could result and remember a company can be investigated anytime to see if they meet the regulations required. Documentation must be kept otherwise fines could occur and reports and event logs can help keep track of what is going on with the network (3 Com Corporation, 2005).

**Filing a Complaint**

Anyone can file a complaint but it must be in writing. Make sure to tell which covered entities are being written about and also tell which acts or omissions of the Privacy or Security Rule were believed to have been violated. This could be done on paper or electronically and needs to be done within 180 days of the violation that has been believed to have occurred. There could be an extension to the amount of days depending on the cause. One can obtain a copy of the complaint form that is recommended for anyone to use from the Office for Civil Rights (OCR) Regional office by request and they can also help with any questions on this form (U.S. Department of Health & Human Services, n.d.b).

**Security**

Risk Management needs to be done on a regular basis. This can help reduce the Organization’s risks and audit controls put in place to help to see if there is anything going on in the computer system that shouldn’t be. Are users accessing information that they shouldn’t? Are there vulnerabilities on the system? Organizations must evaluate their security and document any changes. This can be done internally or through an external company or both. As shown in the table below there needs to be administrative and technical safeguards. Risk management, evaluation, and audit controls are all required under HIPAA for compliance. “Risk
management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level” (Supremus Group, n.d.).

Some questions to ask may be. What are the chances of vulnerability? How would this affect the company? As far as audit controls there should be something in place to track what is happening on the system. Be able to track both devices and users and make sure to keep logs for a certain period of time so if there is a legal issue you could present those as evidence if needed. Make sure to document and re-evaluate especially when changes in the company have been made.

**Objective of HIPAA Audit and Evaluation for Compliance**

The objective of HIPAA Audit includes the following activities:
1. Assess if all vulnerabilities have been addressed.
2. Verify that all compliance requirements have been met.

<table>
<thead>
<tr>
<th>Item</th>
<th>HIPAA Citation</th>
<th>HIPAA Security Rule Standard Implementation Specification</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>180.308(a)(1)(i)</td>
<td>Security Management Process</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>180.308(a)(1)(ii)</td>
<td>Risk Management</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>180.308(a)(6)</td>
<td>Evaluation</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>180.312(b)</td>
<td>Audit Controls</td>
<td>Required</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2- Objective of HIPAA Audit and Evaluation for Compliance (Supremus Group, n.d.).

The HIPAA audits started in November 2011 and will end at the end of 2012. Companies really need to make sure they are HIPAA compliant. There have been a lot of breaches reported. Also, make sure that mobile devices are protected. There was a study done by the Ponemon Institute showing that in healthcare mobile devices are being used by 81% of the company and contain patient data and no security is being considered by 49% percent of those companies (Pham, T., 2012).
Jackson & Coker also included in the report below shows the top three users of mobile devices in healthcare. Companies should put a policy in place that requires a password be set on mobile devices so that way no one else can gain access to the information on that device in case it gets lost (Pham, T., 2012).

![Mobile Device Security](image)

**Figure 3- Mobile Device Security (Pham, T., 2012).**

**HIPAA Compliance**

There are companies that provide HIPAA compliant messaging. According to an article in Business Wire on May 29, 2012 the #1 in HIPAA compliant messaging is TigerText. This allows PHI information to be exchanged quickly and securely. This can be used on any mobile device that an employee may own and is easy to implement (Business Wire, 2012).

Some companies use what is called a Business Associate Agreement (BAA) to help them be in compliance. This is when a contract is signed by an outside vendor stating each of their responsibilities in protecting that Company’s data. According to the data below not all
companies sign this agreement. Companies really need to do their research when choosing an
outside source to host their data. This is where a lot of the data breaches occur. Although a lot
of breaches occur with the outside vendor it happens internally also. Training of employees is
very important according to a survey done by PricewaterhouseCoopers (Pham, T., 2012).

If a company is dealing with patient data and needs to be compliant or thinking about
choosing a hosting company they really should make sure they are also HIPAA compliant.
Online Tech’s is a company that meets 100% HIPAA compliance. They have physical security,
network security, and data security that is all HIPAA compliant. All employees are trained on
HIPAA compliance. Online Tech monitors this all day every day and they have alarms that let
them know of anything suspicious. Redundancy is included to be able to access data at all times
and disaster recovery is also provided (Online Tech, 2012b).

Ask the hosting company questions such as have they been audited and are they HIPAA
Compliant? Find out what policies and procedures are in place in case there is a breach. Are the
HIPAA standards for protecting sensitive health information such as using certain encryption
standards met? What about HIPAA requirements and firewalls? Also what servers are being
used for production? Find out if all employees’ have been trained on being HIPAA Compliant. Make sure to have a Business Associates Agreement with them (Online Tech, 2012a).

Companies need to keep patient information files protected. Some may be using electronic key cards to access file rooms or using other companies to help protect electronic file transactions. Who needs to follow the HIPAA guidelines? As stated in an article by Bobbie Sage in HIPAA Law and Regulations any provider or organization that works with healthcare information must follow the HIPAA guidelines but some small self-administrated health organizations are excluded (Sage, B., n.d.).

How does physical and network security play a role in HIPAA? There must be safeguards in place to meet HIPAA compliance such as physical access controls to your workstations and networks, hardware and software installation and removal procedures, protection of data, backups of the system, and detection of an intruder or intruders. Also workstations should log off automatically (Gossels, J., & Noll, L. C., 2004).

Case Example

Employees need to be trained in order to know what information is supposed to be given out. There have been penalties for violations where employees have not released medical records to their patients. If a patient requests a copy of their medical records then the covered entity is supposed to give them a copy. A company has 30 days from the time this copy was requested. There was a $1.3 million penalty given to Cignet Health of Prince George’s County, Md. The company denied patients the ability to view their records which is a violation and also didn’t cooperate with the Office for Civil Rights while being investigated for this. The civil money penalty for this was $3 million (U.S. Department of Health & Human Services, 2011d).
Main HIPAA Requirements

Below is listed what are considered some of the main requirements of HIPAA according to an article from HIPAA EXAMS. This should be followed in order to help protect from receiving violations.

- Procedures need to be set to make sure that information is protected and not being used wrong fully. Only employees authorized should be accessing and using that information.
- All violations need to be recorded even if they are non-intentional.
- Servers and computers are required to have security software installed on them if they are handling patient information.
- Anti-virus must be up to date and hardware and other software should also be up to date.
- There needs to be standards for passwords and all files being transmitted need to have encryption and password protection.
- Need to be ready in case of disaster make sure all patient information is backed up and only individuals that are authorized should have limited access to this information by using a password to login. These backups should be tested regularly.
- Training needs to be done for all employees handling patient information.

(HIPAA Exams, 2012b).

HIPAA Training Reasons

Listed below are reasons to be trained in HIPAA Compliance:

- Employees need to be aware of various provisions.
• Training can be provided to just employees that handle confidential patient information or they can train all employees. It’s better to train all so that all employees are aware.

• Training is usually not very long maybe a couple hours and then employees are given a test to take at the end.

• By being aware you can help avoid violations since most violations are not on purpose they are because of lack of training.

• Secure your patients confidential information with physical and technical safeguards.

• Employees need to be aware of any updates to HIPAA.

There are various training courses available and the pricing of the training courses fluxuates (HIPAA Exams, 2012d).

Steps to take to help you become HIPAA Compliant

Taking the following steps may help you become HIPAA Compliant:

a. Do a risk assessment

Properly assess all devices that may contain possible ePHI whether they are connected to the network or not. Companies don’t always think of medical devices and other machines. Machines such as ultrasound machines need to be assessed along with computers. Any type of device that may contain patient information. Look at the password policy to see if it is strong enough and make sure that others cannot see the computer screen when patient information is on the screen. If investigated by HIPAA make sure to be able to show them that a plan is in place to fix
areas that may need fixing when resources are available that can fix those issues.

b. Work with or communicate with stakeholders

Get the stakeholders together and communicate with them the issues and explain the problems. Ask for their ideas to help solve the problem. If a problem isn’t seen then it may be hard get the approval or money to fix it. Keep all departments of the organization involved since there are people in every department that have information on something and can help. As far as using medical devices that may attach to computers go directly to the source or people using certain equipment since they know best what they do and what problems they face.

c. Create policies that cover what should to be accomplished

Create them to be for the whole organization not just certain departments. Even though every department may be somewhat different it needs to be created toward the organization. Get information from all departments to help in writing those policies. Include exceptions if needed to meet HIPAA compliance. Just because encryption may be used doesn’t always mean you’re compliant. For example, if someone writes down their password and someone else sees it and accesses the system that could cause a privacy breach. If policies are in place make sure they are enforced or otherwise they are no good.

d. Review purchasing of IT and medical equipment
Don’t purchase on emotion because you like something. For example, you prefer Windows XP over Windows 7. If Windows 7 has more security options you may want to consider purchasing that versus Windows XP and make sure your software if updated.

e. Accountability

That doesn’t necessary mean blame someone else. Figure out what the problem is and correct it so that it doesn’t happen again.

(Reber, E., 2012).

**HIPAA/HITECH**

Even though HIPAA has been around since 1996 it wasn’t taken seriously until HITECH was put into place in 2010. HITECH extended the HIPAA that was put into place in 1996 which contained two parts: Title I and Title II.

- **Title I** to protect people in case they lost their job or switched jobs so that they could still have healthcare coverage.

- **Title II** called Administrative Simplification was about data protection. From an IT Departments aspect HIPAA/HITECH is to control who can see what data depending on their job position, tracking data, and monitoring data. Also protecting stored data and data while it is being transferred through encryption. Access controls and processes also need to be set up.

**Under HIPAA Section 164.308 the Administrative Safeguards are:**
164.308(a)(1)(ii)(D) deals with the review of information activity and is required by HIPAA. There needs to be procedures in place to be able to track what people or doing. You could do this with audits and reports.

164.308(a)(3)(ii)(C) deals with terminating a person account when they are no longer with the company no matter what the reason is. This is considered addressable which means that if not done then you must document why.

164.308(a)(4)(ii)(A) if the company is part of a larger company then they must protect the patient’s information. It is required that they have policies and procedures in place so that the larger company doesn’t access information they are not suppose to be accessing.

164.308(a)(4)(ii)(C) is addressable that you have policies and procedures on establishing and modifying access rights.

164.308(a)(5)(ii)(C) you should monitor the amount of times an account has tried to login and report anything abnormal. This is addressable not required.

164.308(a)(5)(ii)(D) this is addressable but you should have password procedures.

164.3089(a)(6)(ii) it is required that any security incidents you find are reported and responded to.

164.308(a)(7)(ii)(B) it is required that a company has a plan for disaster recovery.

**Under HIPAA section 164.312 the Technical Safeguards are:**
164.312(a)(2)(i) it is required that a user have a unique identification.

164.312(b) HIPAA requires that there are controls in place in order to audit changes on the system.

164.312(d) it is required that the company has procedures in place to make sure that the person trying to gain access to the system is actually who they are suppose to be.

**Under HIPAA section 164.528 the Protected Health information accounting disclosures:**

164.528 it’s required that the company gives a person accounting of disclosure that was made by the company for the past six years from the date they requested it.

(NetWrix Corporation., 2012).

When you go to your doctor’s office for treatment or checkup or whatever you are there for they probably give you a clipboard or something with a paper attached called the “HIPAA privacy notice” (United States Department of Labor, n.d.). This tells about the protection of your health information. HIPAA has also helped in ways such as if you have preexisting conditions. If you had a medical condition for years before you applied for health coverage but yet you have not had treatment on it in the last 6 months then they cannot count that against you since they can only look back 6 months into your medical conditions. If pregnant you cannot be denied the coverage. Even if something is within that 6 month period and is excluded you still qualify for the other benefits in that new plan. Although this helps protect employees somewhat it is not required that health care benefits are to be offered by an employer (United States Department of Labor, n.d.). There are rights under the HIPAA Privacy Rule. Those rights state that patients have the right to see and make a copy of their medical records within 30 days from the day
requested unless there is a reason to believe that they may be a danger to their self or others. If there is incorrect information it can get changed within 60 days from the day of letting them know. There are also rights to obtain a written explanation of your health conditions (Peoplechart Corporation, n.d.).

**Training**

Training can be done in a classroom or even online. A May, 2012 article on HIPAA EXAMS states the 4 top teaching methods used for this training.

- Training on policies and procedures. Focusing on certain areas that may be related to those employees responsibilities.
- Use an instructor that has experience and you can do this as already mentioned either in a classroom or online.
- Employees should be trained on the computer since they may use when dealing with patient data. This training should also teach about passwords and other encryption.

How often do we train our staff? Training should be continuous and the company should inform their employees of any updates that have been made. Any new employees need to be trained also so a company should not just be training once a year they need to make sure every new employee coming onboard also is trained. This could be done in several ways such as through memos, the company’s newsletter, more classes or online courses. This will help lower the violations that could cause penalties (HIPAA Exams, 2012c).

HIPAA training can be divided into 67 Policies and 5 categories which all need to be understood in order to be in compliance and avoid the penalties that could be acquired if not understood and in compliance. Not only will it help employees be in compliance but makes
them aware of those penalties. Employees need to take a test at the end of their training and need to pass or they need to take the training again. Most employees prefer the online training so that they can complete when and where it is convenient for them. By training and making employees aware of HIPAA expectations they will better be able to protect patient information and help keep it secure (HIPAA Exams, 2012a).

**Email Encryption**

Having patient information sent by email is a major concern for companies. Email containing patient information needs to be encrypted. There are services that provide email encryption and many companies are using them. A data breach can be very stressful on a patient and maybe even embarrassing. Also, a data breach depending on who obtains the patient’s information and what type of information they gain access to could cause financial problems and even identity theft. It could be more than one patient that is breached if the company is sending several emails a day. If patient information is breached the company could get big fines, lawsuits, and this could also hurt the company’s reputation. In 2008 a survey was done by Healthcare Information and Management Systems Society (HIMSS) and less than half of those responding companies were using email encryption. Training and attending seminars whenever possible is a great way to help keep up to date on the HIPAA laws and being HIPAA compliant (Email Encryption is Vital Under New HIPAA Regulations, 2012).

**Your Filing System and HIPAA**

HIPAA doesn’t only mean that electronic data needs to be secure but also patient charts. Identifying information cannot be on the outside of a file. By assigning patient’s numbers and then placing that number on the outside of the chart to identify that patient would be HIPAA compliant. Having a name, address, or social security number on the outside of a chart is not
HIPAA compliant anymore. Develop another way to identify patients such as the number system mentioned above. Just like with electronic data only authorized employees are allowed to access a patient’s chart. Charts should be locked up so that only those authorized can access them. Just make sure they are under lock and key to be HIPAA compliant (The Smead Manufacturing Company, Inc., 2012).

**HIPAA Audits**

What might the OCR be looking for when auditing in 2012? The OCR wants to improve compliance. They are looking to see if a company is compliant or not. If they believe the company is not compliant they may call for a review. The audits are done by a company called KPMG and they are expected to do 150 audits in the year 2012. They will be focusing on auditing those covered entities in the health care field that electronically transmit information. They will want to talk mainly with leadership and the CIO about their policies in regards to HIPAA compliance. This could be a long process since sometimes the audits can take up to 30 days. A company can prepare for an audit by training their employees. Not training employees could create a liability for the company. The auditors may ask for documentation on the company’s compliance so make sure your policies and procedures meet HIPAA compliance standards since this information is usually required within 10 business days (Corporate Law Report, 2012).

**HIPAA Violations**

What are the penalties for HIPAA violations? Below is a table from an article by the American Medical Association showing the violations and what the minimum and maximum penalties are for those violations?
Table 1- (American Medical Association, n.d.).

If a person knows that they are disclosing personal information and are not supposed to they can also receive fines and spend time in prison. Time in jail could be anywhere from one to ten years depending on the situation (American Medical Association, n.d.).

**Awareness**

Since HITECH the fines for HIPAA violations increased substantially going from a maximum penalty of $250,000 to $1.5 million. Although not all HIPAA violations are intentional both employee and the company can still face penalties if there is a breach. There was a case where an employee sold patient information and the penalties included jail time.
Another case involved employees’ unauthorized access of medical records in which the company then suspended some employees’ and terminated others. The company and employees need to be trained and aware of what the fines may consist of and how to be in compliance to avoid those fines. As already mentioned fines could be over a million dollars. There was also a case where paperwork was left on a subway and that paperwork contained information that was confidential. There were severe penalties for this accident. Since this case that company has put together a training program (NYU Langone Medical Center, 2011).

According to a 2012 article written by Dina Overland, there were 57 unencrypted hard drives stolen that belonged to Blue Cross Blue Shield of Tennessee. This resulted in a fine of $1.5 million for being in violation of HIPAA and that was only part of the settlement. They have spent over 18 million dollars since this incident. A big portion was spent on investigating and notifications. They also spent a lot on encryption and are also looking at changing their policies and making sure employees are being trained. They may have been able to avoid this if they would have had access controls in place and done a security evaluation (Overland, D., 2012).

**Breaches**

The table below shows breaches affecting more than 500 people as of May 17th 2012.

<table>
<thead>
<tr>
<th># of Breaches</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Theft</td>
</tr>
<tr>
<td>29</td>
<td>Unauthorized Access/ Disclosure</td>
</tr>
<tr>
<td>18</td>
<td>Loss</td>
</tr>
<tr>
<td>5</td>
<td>Hacking/IT Incident</td>
</tr>
<tr>
<td>3</td>
<td>Unauthorized Access/ Disclosure and Hacking IT Incident</td>
</tr>
<tr>
<td>2</td>
<td>Improper Disposal</td>
</tr>
</tbody>
</table>

Source: *Health Information Privacy/Security Alert Analysis of HHS Office for Civil Rights*
Table 2- (Melamedia LLC., 2012).

According to CMS the total number of transaction standards complaints received up to February 29, 2012 was a total of 812 with 800 cases being now resolved and 12 cases still outstanding (Melamedia LLC., 2012).

Research Methodology

If Cignet Health of Prince George’s County, Md employees’ had been properly trained then they would have known that they were expected to release the patients their medical records. This would have saved them from receiving the penalties that they did. Providing proper HIPAA compliance training such as making sure all employees’ are trained properly and trained on the materials that they should be according to their job position can help prevent a lot of breaches that have occurred or will occur in the future (U.S. Department of Health & Human Services, 2011d).

A case study written about a hospital in Pennsylvania that was audited found out that people were not using the secure email system that was implemented by their IT Department because it was too complicated and then needed to make changes to become compliant. They changed to a vendor called Proofpoint that had what they needed to be in compliance with HIPAA. If training had been done their risk of having potential violations may have been much lower or nonexistent since the employee’s might have taken sending unencrypted email more serious (Proofpoint, Inc., 2006).

If the hypothesis in this paper had been used then they may have already been HIPAA compliant instead of finding out later at audit time. Hypothesis: By training staff on HIPAA security a company can lower their risks and also an employee’s risks of breaching confidential
information. If the IT Department had proper compliance training they might have fixed this issue with email before an audit even occurred. Having proper training can save a company from possible breaches of information. By training employees’ not only on email compliance but also on password protection and keeping a patients data confidential companies can be in better compliance and could save them from getting a bad reputation in the community. This could also be viewed as being unethical depending on some breaches. Being compliant and ethical could mean a lot when it comes to a customer’s point of view. If media is involved a company doesn’t want to be seen as unethical or noncompliant that could really hurt a company.

Training could be #1 in keeping up with HIPAA compliance. If employees’ know why they shouldn’t share passwords and why it is so important to keep certain information protected and confidential they may be more apt to be in compliance since with training they would know how important it is and that it is required or there could be penalties to pay. (Proofpoint, Inc., 2006).

**Hypothesis:** By training staff on HIPAA security a company can lower their risks and also an employee’s risks of breaching confidential information.

After reviewing the research others have done this hypothesis on training may be a key in helping companies. All employees’ of a company that need to comply with HIPAA need to be trained for HIPAA compliance. Training plays a big role in a Company’s success to be HIPAA compliant and helps with risk management. An employee needs to know how to handle certain situations and know what to do and say when it comes to confidential information. If they don’t know that they need to release medical records when asked by the patient to the patient and they don’t do it within a certain amount of time then they could be out of compliance. If an employee accesses certain information that they shouldn’t be since that was alright in the past or before
HIPAA was in existence and don’t realize they could get in trouble for that then they may be out of compliance and receive penalties.

Employees need to be responsible when it comes to mobile devices also whether it is a mobile phone, laptop, or tablet of some sort since if it is lost or stolen and there is confidential information on it then that could result in a breach. They needed to be trained to password protect those devices and be very careful what information is on those devices and of their whereabouts.

By having policies and procedures and training employees on those policies and procedures you can substantially lower a Company’s risk of being out of compliance since I don’t believe most people intentionally do things to hurt others they are just unaware of what they are really doing since they have never been taught or told what they need to do to be in compliance with HIPAA and how important it really is. They need to be updated on changes with HIPAA compliance also. You shouldn’t just train them once then never again companies need to reoccurring trainings.

**Suggestions for Further Research**

- This might involve checking several organizations and asking what their policies and procedures are and how they would handle a breach.
- Finding out how often companies update their policies and procedures.
- Researching what training modules are available for companies depending on their needs and to what extent are companies training their employees.
References


http://go.galegroup.com.proxy.davenport.edu/ps/i.do?id=GALE%7CA291241993&v=2.1&u=loom_davenportc&it=r&p=ITOF&sw=w


http://www.hipaaviolations.com/email-encryption-is-vital-under-new-hipaa-regulations/


National Archives And Records Administration 1985. (2012). Electronic Code of Federal Regulations. Retrieved June 24, 2012, from http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr;sid=7b1884158c0552f6f5c0922d26d0be5b;rgn=div5;view=text;node=45%3A1.0.1.3.79;idno=45;cc=ecfr#45:1.0.1.3.79.3.27.6


http://www.onlinetech.com/resources/e-tips/hipaa-compliance/five-questions-to-ask-your-hipaa-hosting-provider


http://www.peoplechart.com/HIPAA.aspx


http://www.beckershospitalreview.com/healthcare-information-technology/5-steps-to-achieving-hipaa-compliance.html


http://personalinsure.about.com/od/health/a/aa041806a.htm


Appendix A- Acronyms

HIPAA The Health Insurance Portability and Accountability Act
HHS Health and Human Services
HITECH ACT The Health Information Technology for Economic and Clinical Act
ARRA American Recovery and Reinvestment Act of 2009
EHR Electronic Health Records
CIA Confidentiality, Integrity, and Availability
CIO Chief Information Officer
CMS Centers for Medicare & Medicaid Services
OCR Office for Civil Rights
BAA Business Associate Agreement
HIMSS Healthcare Information and Management Systems Society
Appendix B-Tables & Figures

Figure 1 – Resolutions by Year and Type (U.S. Department of Health & Human Services, n.d.a).

Objective of HIPAA Audit and Evaluation for Compliance

The objective of HIPAA Audit includes the following activities:
1. Assess if all vulnerabilities have been addressed.
2. Verify that all compliance requirements have been met.

<table>
<thead>
<tr>
<th>Item</th>
<th>HIPAA Citation</th>
<th>HIPAA Security Rule Standard Implementation Specification</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ADMINISTRATIVE SAFEGUARDS</td>
<td></td>
</tr>
<tr>
<td>164.308(a)(1)(i)</td>
<td>Security Management Process</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>164.308(a)(1)(ii)(B)</td>
<td>Risk Management</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>164.308(a)(8)</td>
<td>Evaluation</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TECHNICAL SAFEGUARDS</td>
<td></td>
</tr>
<tr>
<td>164.312(b)</td>
<td>Audit Controls</td>
<td></td>
<td>Required</td>
</tr>
</tbody>
</table>

Figure 2- Objective of HIPAA Audit and Evaluation for Compliance (Supremus Group, (n.d.).)
Mobile Device Security
Who’s Using Them?

![Chart showing mobile device security usage]

- **41%** Emergency physicians
- **33%** Cardiologists
- **31%** Urologists & Nephrologists

81% use mobile devices

49% take no security precautions

Data from Jackson & Coker and Ponemon Institute

Figure 3- Mobile Device Security (Pham, T., 2012).

Business Associate Agreement
Who’s Signed Them?

Only 1/3 of healthcare organizations have signed one.

Data from InformationWeek.com

Figure 4- Business Associate Agreement (Pham, T., 2012).
<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

Table 1- (American Medical Association, n.d.).

<table>
<thead>
<tr>
<th># of Breaches</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Theft</td>
</tr>
<tr>
<td>29</td>
<td>Unauthorized Access/ Disclosure</td>
</tr>
<tr>
<td>18</td>
<td>Loss</td>
</tr>
<tr>
<td>5</td>
<td>Hacking/IT Incident</td>
</tr>
<tr>
<td>3</td>
<td>Unauthorized Access/ Disclosure and Hacking IT/ Incident</td>
</tr>
<tr>
<td>2</td>
<td>Improper Disposal</td>
</tr>
</tbody>
</table>

Source: Health Information Privacy/Security Alert Analysis of HHS Office for Civil Rights

Table 2- (Melamedia LLC., 2012).