2017 SECURITYMETRICS
GUIDE TO
HIPAA COMPLIANCE
WHAT HEALTHCARE ENTITIES AND BUSINESS ASSOCIATES NEED TO KNOW
FOREWORD

Despite advances in security technology and regardless of increased government cyber security initiatives, attackers will not abandon their pursuit of unprotected patient data. Last year, medical and healthcare entities accounted for 36.5% of reported data breaches.

It is clear the healthcare industry is less prepared with HIPAA compliance than patients expect. HIPAA compliance, especially with the Security Rule, has never been more needed especially with cybercrime increasing and patient data increasing in value.

Often, it’s the small, simple, easy-to-correct things that go unnoticed and create vulnerabilities that lead to data compromise. In other cases, healthcare organizations with layers of sophisticated IT defenses are tripped by an employee who opens an errant email or uses a less than complex administrative password.

Our security team put together a few surveys with topics concerning top HIPAA security technologies and processes used for HIPAA compliance, such as network security, firewall configuration, data encryption, and general patient health data protection issues.

We specifically designed this document as a reference guide to help healthcare entities and business associates with the most problematic sections of HIPAA compliance. Rather than reading our guide cover to cover, we recommend using this as a resource for your HIPAA compliance efforts.

I hope the 2016 SecurityMetrics Guide to HIPAA Compliance will help you better understand today’s breach trends and recommended best practices to protect data from compromise through data security and HIPAA compliance.

BRAND BARNEY

SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
</tr>
<tr>
<td>HIPAA COMPLIANCE OVERVIEW</td>
</tr>
<tr>
<td>PERSPECTIVES FROM FORENSIC INVESTIGATORS</td>
</tr>
<tr>
<td>HIPAA SECURITY RULE</td>
</tr>
<tr>
<td>SECURITY RULE INTRODUCTION</td>
</tr>
<tr>
<td>RISK ANALYSIS AND RISK MANAGEMENT PLAN</td>
</tr>
<tr>
<td>PERMANENTLY DESTROYING PHI</td>
</tr>
<tr>
<td>ENCRYPTING PHI</td>
</tr>
<tr>
<td>HIPAA COMPLIANT EMAILS</td>
</tr>
<tr>
<td>MOBILE DEVICE SECURITY</td>
</tr>
<tr>
<td>PHYSICAL ACCESS</td>
</tr>
<tr>
<td>HIPAA COMPLIANT FIREWALLS</td>
</tr>
<tr>
<td>WIRELESS NETWORKS (WI-FI)</td>
</tr>
<tr>
<td>SYSTEM CONFIGURATION STANDARDS</td>
</tr>
<tr>
<td>SECURE USER ACCESS</td>
</tr>
<tr>
<td>SECURING YOUR REMOTE ACCESS</td>
</tr>
<tr>
<td>LOGGING AND LOG MANAGEMENT</td>
</tr>
<tr>
<td>VULNERABILITY SCANNING</td>
</tr>
<tr>
<td>PENETRATION TESTING</td>
</tr>
<tr>
<td>HIPAA BREACH NOTIFICATION RULE</td>
</tr>
<tr>
<td>BREACH NOTIFICATION RULE INTRODUCTION</td>
</tr>
<tr>
<td>HOW TO MANAGE A HEALTHCARE DATA BREACH</td>
</tr>
<tr>
<td>HIPAA PRIVACY RULE</td>
</tr>
<tr>
<td>PRIVACY RULE INTRODUCTION</td>
</tr>
<tr>
<td>MINIMUM NECESSARY</td>
</tr>
<tr>
<td>NOTICE OF PRIVACY PRACTICES</td>
</tr>
<tr>
<td>HIPAA COMPLIANCE BEST PRACTICES</td>
</tr>
<tr>
<td>BUSINESS ASSOCIATE CONCERNS</td>
</tr>
<tr>
<td>HIPAA DOCUMENTATION</td>
</tr>
<tr>
<td>HIPAA TRAINING</td>
</tr>
<tr>
<td>HOW TO PREPARE FOR A HIPAA AUDIT</td>
</tr>
<tr>
<td>AUDIT PREPARATION BEST PRACTICES</td>
</tr>
<tr>
<td>HIPAA BUDGET</td>
</tr>
<tr>
<td>CONCLUSION</td>
</tr>
<tr>
<td>CONTRIBUTORS</td>
</tr>
<tr>
<td>TERMS AND DEFINITIONS</td>
</tr>
<tr>
<td>ABOUT SECURITYMETRICS</td>
</tr>
</tbody>
</table>
INTRODUCTION
EXECUTIVE SUMMARY

Based on the department of Health and Human Services’ (HHS) Health Insurance Portability and Accountability Act (HIPAA), we constructed several surveys to analyze various aspects specific to HIPAA’s Privacy, Security, and Breach Notification Rules.

In 2016, we conducted 3 surveys from over 150 different healthcare professionals (who were responsible for HIPAA compliance), primarily from organizations with fewer than 500 employees. They were asked questions about their perspectives ranging from their overall HIPAA compliance status to specific elements of the Security Rule.

Even though larger healthcare organizations’ responses might show more compliance to HIPAA requirements and/or security best practices, the following statistics remain impactful for healthcare organizations of any size. This is because most (if not all) healthcare organizations share patient data and interact with smaller organizations (e.g., hospitals send patient data to specialist clinics), which might influence their security and HIPAA compliance practices.

PATIENT DATA SECURITY

• 38% of respondents don’t know if they encrypt patient data; 12% don’t encrypt stored patient data

• 50% of respondents don’t know if their organizations use multi-factor authentication

• 7% of organizations’ employees share ID credentials

• 7% of organizations don’t have automatic timeouts/log outs on workstations

FIREWALLS

• 27% of respondents don’t know what firewalls their organization uses

• 12% of respondents don’t know if a security professional or third party manages their network’s firewall(s)

• 41% of respondents don’t know how often their firewall rules are reviewed; 7% never review firewall rules

• 37% of respondents don’t know if they store firewall logs; 15% don’t store firewall logs

• 32% of respondents don’t know if someone is assigned to review logs daily; 24% don’t review firewall logs daily
MOBILE DEVICE SECURITY

- 17% of organizations allow employees to use personal mobile devices to access patient data
- 15% of respondents have employees that use organization-owned mobile devices for non-office related activities (e.g., checking personal email downloading apps)
- 55% of respondents have a mobile device policy
- 26% of respondents don’t use mobile encryption; 10% don’t know if they use mobile encryption

EMAIL SECURITY

- 45% of organizations send emails containing patient data
- 27% of organizations don’t encrypt emails containing patient data; 9% don’t know if emails are encrypted
- 910% of organizations’ employees send patient data to themselves
- 32% of organizations send patient data that is either unencrypted or through normal email services

HIPAA TRAINING

- 60% of respondents train employees yearly; 8% never receive training; 12% don’t know how often they train employees
- 74% of respondents provide HIPAA Privacy Rule related-training; 70% provide HIPAA Security Rule related-training; 70% provide HIPAA Breach Notification Rule related-training
- 51% of respondents don’t test employees on HIPAA-related training
HIPAA COMPLIANCE OVERVIEW

HIPAA is enforced by the Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR). Any covered entity (CE) and business associate (BA) that stores, processes, transmits, maintains, or touches protected health information (PHI) in any way must be HIPAA compliant.

The three HIPAA rules include:

- The Security Rule containing 75 requirements with 254 validation points
- The Privacy Rule containing 72 requirements with 255 validation points
- The Breach Rule containing 10 requirements with 26 validation points

Entities are expected to complete a Risk Analysis, create and complete a Risk Management Plan, conduct regular employee trainings, and implement updated policies and procedures.

The investigation of numerous healthcare compromises has confirmed that the security controls and processes required in HIPAA are essential to protecting patient data. But if organizations are breached and not compliant with HIPAA regulations, they may face financial consequences. In general, fines may cost as much as:

- HHS fines: up to $1.5 million per violation per year
- Implementation of new systems and processes: Depends
- On-going credit monitoring for affected patients: $10 per individual
- Federal Trade Commission: $16,000 per violation
- Class action lawsuits: $1,000 per record
- State attorney generals: $150,000 – $6.8 million
- Patient loss: 40%

Based on the size of breach and noncompliance, these estimates can be higher or lower. With all the financial consequences, healthcare organizations need to take HIPAA compliance seriously, especially by understanding the underlying motivations for the HIPAA rules, current forensic trends.
PERSPECTIVES FROM FORENSIC INVESTIGATORS

Forensic Investigators thoroughly analyze the environment of organizations that suspect data breach. Through a forensic examination of the in-scope computer systems related to the handling of patient health information (PHI), data acquired from the breach site can reveal when and how the breach occurred, contributing vulnerabilities, and aspects of the IT environment out of compliance with HIPAA standards.

INCREASED WINDOW OF COMPROMISE

The window of compromise starts from the date an intruder accesses a business network and ends when the breach is contained by security remediation. On average, it took 844 days from the time an organization was vulnerable for an attacker to compromise the system.

Nearly every organization will experience system attacks from a variety of sources. Due to inherent security weakness in systems or technology, some organizations have systems, environments, software, or website weaknesses that can be exploited by attackers from the day their environment is set up. In other cases, an organization becomes vulnerable because they fail to apply a security patch or make system modifications without properly updating related security protocols.

Based on data collected by SecurityMetrics Forensic Investigators from 2016 breaches, the average organization was vulnerable for 1,021 days.

Once compromised, attackers were able to capture sensitive data for an average of 163 days in 2015. This may be attributed to aggregation methods employed by data thieves. Attackers have been known to save patient data from malware scraping (or other tools), without using or selling the data for months to years.

Using this aggregation method prevents organizations from identifying malicious account activity too early, which would expose the data breach much sooner and greatly limit the amount of patient data that attackers could acquire.
HIPAA SECURITY RULE
SECURITY RULE INTRODUCTION

Healthcare organizations are often less zealous in applying the Security Rule, as opposed to the Privacy or Breach Notification Rules. This is why PHI is mostly leaked or stolen from healthcare organizations that have not properly implemented the Security Rule. The HHS's OCR Breach Portal shows that over 1000 breaches since 2009 occurred because of electronic device misuse or loss (e.g., laptops, desktop computers, network servers, etc.).

According to the HHS, a major goal of the Security Rule is to protect the privacy of individuals' health information, while allowing organizations to adopt new technologies to improve the quality and efficiency of patient care.

For example, some HIPAA Security Rule requirements try to make it more difficult for attackers to install malware and other harmful viruses onto systems, such as:

- § 164.308(a)(5)(ii)(A) Install periodic security updates.
- § 164.308(a)(5)(ii)(B) Procedures for guarding against, detecting, and reporting malicious software (anti-virus).
- § 164.308(a)(5)(ii)(C) Enable logging and log alerting on critical systems.
- § 164.308(a)(5)(ii)(D) Password management procedures for creating, changing, and safeguarding passwords.
- § 164.308(a)(5)(i) Implement a security awareness and training program for all workforce members (including management).

The Security Rule was designed to accommodate healthcare organizations of all sizes and technical usage. The path to HIPAA compliance is different for every organization, and each organization must implement security controls that will effectively minimize their unique set of risks.
RISK ANALYSIS AND RISK MANAGEMENT PLAN

CONDUCTING A RISK ANALYSIS

The HHS states, "conducting a Risk Analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a Risk Analysis is foundational." A Risk Analysis is a way to assess your organization’s potential vulnerabilities, threats, and risks to PHI.

THE PURPOSE OF THE RISK ANALYSIS IS TO HELP HEALTHCARE ORGANIZATIONS DOCUMENT POTENTIAL SECURITY VULNERABILITIES, THREATS, AND RISKS.

Besides helping you know where your vulnerabilities, threats, and risks are in your environment, a Risk Analysis will also protect you in the event of a data breach or random audit by the HHS. Organizations that have not conducted a thorough and accurate Risk Analysis can expect to be hit with severe financial penalties.

The HHS has stated on multiple occasions they will make examples of healthcare organizations that put PHI at risk. Given the importance associated with the Risk Analysis, you may want to consider working with a HIPAA security expert.

Though the HHS does not specify an exact Risk Analysis procedure, they do require certain elements be present in a Risk Analysis, specifically:

- Scope analysis
- Data collection
- Vulnerabilities/threat identification
- Assessment of current security measures
- Likelihood of threat occurrence
- Potential impact of threat
- Risk level
- Periodic review/update as needed
WHERE IS YOUR PHI?

Detailed PHI flow diagrams are vital for your Risk Analysis because they show how people, technology, and process that create as well as store, process, or transmit PHI, revealing where you need to focus security efforts and training.

Create a diagram that shows how PHI enters your network, the systems it touches as it flows through your network, and any point it may leave your network. For example, patients fill out forms at hospitals, which pass patient records to doctors’ offices, which then transfer medical records to pharmacies. Patients add sensitive information to third party patient portals online, which then email a dentist receptionist, who then prints and stores it in a giant file cabinet.

PHI ENTRY

Identify everywhere PHI is created and enters your entity. By doing so, you know exactly where to start with your security practices.

Consider the following questions about where your electronic PHI is created and enters your environment:

- **Email:** How many computers do you have, and who can log on to each computer? What email services are in use?
- **Texts:** How many mobile devices do you own, and who uses them?
- **EHR entries:** How many staff members do you have entering in data? Who are they? From where do they enter the data?
- **New patient data:** How much are patients required to fill out, and where? Front desk? In the examination room?
- **Business associate communications:** How do business associates communicate with you?
- **Databases:** How do you communicate with patients? What records and data do you enter into your database?

YOU NEED TO DOCUMENT WHERE PHI IS CREATED AND HOW IT ENTERS YOUR ENVIRONMENT, WHAT HAPPENS ONCE PHI ENTERS, AND HOW PHI EXITS.
PHI STORAGE
You need to know exactly what happens to PHI after it enters your environment. Is it automatically stored in your EHR/EMR system? Is it copied and transferred directly to a specific department (e.g., accounting, marketing)?

Additionally, you must document all hardware, software, devices, systems, and data storage locations that can access PHI. PHI is commonly stored in the following places:

- EHR/EMR systems
- Mobile devices
- Email
- Servers
- Workstations
- Wireless (networked) medical devices
- Laptops
- Computers
- Calendar software
- Operating systems
- Applications
- Encryption software
- Physical locations/storage (e.g., filing cabinets)
- Shred bin containers
- Non-approved storage locations

PHI TRANSMISSION
When PHI leaves your organization, it is your job to ensure it is transmitted or destroyed in the most secure way possible. Here are some things to consider when PHI leaves your environment:

- Business associates: Are you sending through encrypted transmission? Are they? Is data sent to them kept at a minimum?
- Email: How does your organization send patient data?
- Flash drives: What policies are in place?
- Trash bins on computers: How often are these cleared out?
- Physical storage and transportation: How do you transport PHI from one location to another?
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

HOW TO FIND YOUR PHI
One of the first steps in protecting PHI is determining how much of it you have, what type you have, where it can be found in your organization, what systems handle it and who you disclose it to. You should interview personnel to document those systems and who has access to them.

You probably are not aware of every task and situation that your employees encounter on a daily basis or every aspect of their individual jobs. Interviewing personnel is one of the best ways to get further insight into how you are interacting with and using PHI on a regular basis. It may help you discover access to systems or certain disclosures that you were not aware of.

RYAN MARSHALL
SecurityMetrics HIPAA Fulfillment Manager | HCISPP
IDENTIFY VULNERABILITIES, THREATS, AND RISKS

To find your vulnerabilities, examine flaws in your components, procedures, design, implementation, and internal controls. For example, a vulnerability could be a flaw in building designs that might lead to PHI being stolen.

To discover your threats, figure out the potential for a person, group, or thing to trigger a vulnerability. For instance, what would happen if you have a disgruntled employee? Would they be able to get back into the system and obtain PHI after they were fired?

Lastly, you need to know your risks. Think about the probability that a particular threat may take advantage of a specific vulnerability. For example, if you use a Windows XP machine with access to the Internet, there is an extremely high probability that a hacker will exploit security flaws (due to the discontinued support for WinXP) using malicious software and gaining access to PHI. In this scenario, the vulnerability is using an outdated OS, the threat is the potential of a hacker exploiting it, and the risk is high because it is easy to do and hackers look for organizations with outdated systems.

Consider these categories in particular as you think about your vulnerabilities, threats, and risks:

- **Digital**: (e.g., weak passwords, shared ID credentials)
- **Physical**: (e.g., not shredding PHI, inaccessibility of facility)
- **Internal**: (e.g., workforce members)
- **External**: (e.g., hackers, thieves)
- **Environmental**: (e.g., fires, hurricanes, storms)
- **Negligent**: (e.g., unknowing employee, accidental loss)
- **Willful**: (e.g., disgruntled former employee, ex-spouse, and/or family members)
THIRD-PARTY SCANS AND TESTS
It’s difficult, if not impossible, to find every weakness in your organization on your own. To take your security to the next level and to avoid weaknesses in your IT system, consider implementing additional services such as:

• Internal and external vulnerability scans—automated testing for weaknesses inside and outside your network.

• Penetration test—live, hands-on testing of your system’s weaknesses and vulnerabilities.

• Nmap scanning—a simple network scan that identifies open ports and services on your network.

ANALYZE YOUR HIPAA RISK LEVEL
You need to decide what risks could and will impact your organization. Risk and impact prioritization is a crucial part of your Risk Analysis that will eventually translate to your Risk Management Plan.

To analyze your risk level, consider the following:

• **Likelihood of happening:** Just because you are threatened by something, doesn’t necessarily mean it will have an impact on you. For example, organizations in Florida and Colorado technically could both be affected by a hurricane. However, Florida-based organizations have a higher hurricane risk level.

• **Potential impact:** How would this particular risk effect your organization? For example, while a computer screen might accidentally show PHI to a patient in the waiting room, it probably won’t have as big of an impact as an attacker accessing your unsecured WiFi.

Every vulnerability and associated threat should be given a risk level. The typical designations are ‘high,’ ‘medium,’ and ‘low.’ Documenting this information gives you a prioritized list of security issues.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

RISK ANALYSIS– MAPPING OUT YOUR COMPLIANCE

As we work with individual entities, we find that because they attempt to perform a Risk Analysis with only in-house talent, a non-security professional, or an unqualified third party, many vulnerabilities and risks are missed.

In one instance, we were brought in to perform a Risk Analysis only six months after a different third party had completed an incomplete Risk Analysis. Within the first hour of review, we found major holes in their firewall that were overlooked, as well as other major problems. A complete and thorough Risk Analysis is critical to start securing your patient information.

An in-house Risk Analysis can be a great first step toward HIPAA compliance, but if your staff is pulled too thin (as they almost always are), you probably won't see accurate results. Most IT staff members don't want to show the boss their own security blunders.

BRAND BARNEY
SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
CREATE YOUR RISK MANAGEMENT PLAN

The Risk Analysis outcome should directly feed into a Risk Management Plan. The Risk Management Plan is the compliance step that works through issues discovered in the Risk Analysis and provides a documented instance proving your active acknowledgment (and correction) of PHI risks.

There are many ways to approach the Risk Management Plan, but ultimately the process will consist of three main steps:

- Plan how you will evaluate, prioritize, and implement security controls.
- Implement security measures that address the greatest areas of risk (or your biggest ROI) first (e.g., fix firewall rules).
- Test the security controls you’ve implemented and be sure to keep an eye out for new areas of risk.

THE HIPAA SECURITY RULE REQUIRES YOU TO COMPLETE A RISK ANALYSIS AND RISK MANAGEMENT PLAN AT LEAST ONCE A YEAR.
IMPLEMENT YOUR RISK MANAGEMENT PLAN

After a plan is created to address Risk Analysis concerns, it’s time to implement it. Starting with the top-ranked risks first, identify the security measure that fixes that problem. For example, if your risk is that you still use Windows XP, your security measure would be to update your computer system or work with your vendor to properly mitigate the proposed risk.

Another important part of the Risk Management Plan is documentation. If you don’t document, you can’t prove to HHS in a meaningful way that you’ve performed a comprehensive Risk Analysis. They will want to see your Risk Analysis documentation, your Risk Management Plan, and regular progress on addressing the items identified in that Risk Management Plan.

AS FAR AS HHS IS CONCERNED, IF IT’S NOT DOCUMENTED IT NEVER HAPPENED.

Although specific items included in a Risk Management Plan vary, the following points are industry best practices:

- **Determine security measures**: You need to determine appropriate security measures and resolutions to mitigate each line item contained in your Risk Analysis.

- **Risk level**: Each vulnerability discovered should be assigned a risk level, based upon benefit, ROI, budget, and internal and external resources). You can get some of this information from the Risk Analysis, but may have to estimate the rest based on current breach and hacker activity.

- **Date completed**: Including a completion date is great for both HHS documentation and your own records.

- **Completed by**: This is great for practices where two or more people (such as a doctor and office manager) are completing a Risk Management Plan together.

- **Notes section**: It’s helpful to include a comments section next to each requirement, especially what policy and procedure the item is associated with and how you will implement the task.

Your Risk Management Plan should be your foundation for your Security Rule compliance efforts. Updating and implementing your Risk Management Plan should be an on-going process, especially when new systems and/or processes are added to the PHI environment.
PERMANENTLY DESTROYING PHI

Once you start working on your RMP, place high priority on removing any unnecessary patient data. If you delete sensitive information (like patient health records, Social Security Numbers, etc.) on your computer, they’re probably still on your computer and accessible to attackers.

Take special note, when you empty the Recycle Bin or Empty Trash, it doesn’t actually wipe the file(s) off your computer. It simply marks the file as acceptable to overwrite and is generally no longer visible to the user. For the average user, those files are nearly impossible to retrieve because the operating system deletes the references to the file. Your computer can’t find that file for you anymore, but the file still exists. For those with more advanced computer skills (such as hackers), that data is still accessible by looking at the unallocated disk space.

Think of the Trash or Recycle Bin like putting sensitive documents in the trashcan next to your desk. You can easily retrieve those documents if you need to. All you do is pull them out of the trashcan.

The HHS regulations (e.g., 45 CFR 164.310(d)(2)(i) and (ii)) state, “the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored.”

The HHS has determined that for electronic PHI, clearing (i.e., using software or hardware products to overwrite media with non-sensitive data) is the best ways to securely delete sensitive patient healthcare data on systems still in use.

When thinking about how to permanently delete files off your network, don’t forget about any archived data, including:

- Time Machine backups
- Cloud backups
- External hard drive backups
- CD or DVD backups
- Email backups
- FTP backups
- Server backups
- Mirror backups
- Offsite backups
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

PERMANENTLY DELETING FILES
Most people know how to destroy physical sensitive data (e.g., shredding, burning, pulping, etc.), but when it comes to securely destroying electronic data, most healthcare professionals don’t know where to begin (e.g., options, tools, procedures).

If media is magnetic (e.g., tapes, hard drives), it should be degaussed and/or demagnetized. Make sure to use an appropriately sized and powered professional grade degausser to ensure no data recovery is possible. You can also physically destroy the media in an almost endless amount of ways. One organization ground up their hard drives and dissolved them in a sulfuric acid solution.

If you plan to re-use or sell the media, use a repetitive overwrite method, also known as erasure or wiping. This is when you overwrite the data with randomized with 1’s and 0’s. There are many free overwrite tools available and most modern operating systems have features for securely deleting data.

If you use a solid state drive or flash memory, you’ve got several options. You can use an ATA Secure Erase command to wipe or reset the data; some manufacturers supply software that will enable you to perform secure erasures (though some have flaws). But the only sure way to destroy data on a solid state drive or in flash memory is to physically destroy it.

RYAN MARSHALL
SecurityMetrics HIPAA Fulfillment Manager | HCISPP
**ENCRYPTING PHI**

If you need to keep data and permanently deleting isn’t an option, you need to encrypt PHI. This is because if an attacker is able to break into your network devices, encryption renders files useless by masking them into an unusable string of indecipherable characters.

With this danger in mind, HIPAA requires healthcare entities to “implement a method to encrypt and decrypt electronic protected health information” in requirement §164.312(a)(2)(iv). All electronic PHI that is created, stored or transmitted in systems and work devices must be encrypted (e.g., mobile phone, laptop, desktop, flash drive, hard drive, etc.).

As previously mentioned, you need to make sure that you adequately map out where PHI is created and enters your environment, what happens once PHI enters (and where it is stored), and exits your environment or organization. Although HIPAA regulations don’t specify the necessary encryption, industry best practice would be to use AES-128, Triple DES, AES-256, or better.

Due to the complexity of encryption rules, healthcare organizations often use third parties to ensure encryption of PHI, partly because organizations are required to keep the tools for decryption on another device or location.

**FULL DISK ENCRYPTION**

Historically, one of the largest reported threats to ePHI (electronic patient health information) has been loss or theft of a physical device. While employing adequate physical security and media movement procedures is the first line of defense to prevent these types of incidents; they still sometimes occur despite a Covered Entity’s best efforts in those areas.

Encryption is the best way to protect you from penalties associated with a breach when a device is lost or stolen. The HITECH act of 2009 modified the HIPAA Breach Notification Rule by stating that if a device is lost or stolen, the loss is not reportable as a breach if the data can be proven to have been rendered unreadable by either secure destruction, or encryption.

Disk encryption for laptops and desktops is very easy to put into use and usually comes with no additional cost as most current operating systems come equipped with the capability.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

ENCRYPTION—THE REQUIRED ADDRESSABLE

Even though the HIPAA regulations indicate that encryption is an addressable item, the HHS has made it very clear it’s viewed as required.

Let me tell you what doesn’t count as encryption. I have run into several healthcare professionals who showed me their spreadsheets of PHI saying, “See, I encrypt it when I make the cell smaller and the numbers change to ‘###’.” Just to be clear, this is not encryption.

Three common data handling processes that are often confused: masking, hashing, and encrypting. Let me break them down for you:

• Masking is hiding part of the data from view. It is still there in clear text, you just can’t see all of it on the screen. You use this to hide parts of the patient information not needed by a specific workforce member.

• Hashing is running the data through a mathematic algorithm to change it into something indecipherable. You cannot undo a hashed value to get back to the original data. Generally, healthcare entities don’t hash PHI.

• Encrypting is similar to hashing because data is run through a mathematic algorithm; however, you use an encryption key that has a paired decrypting key. This way the data is safely stored and the only way to see the data is by using the decryption key to unlock it. Currently, the strongest, most common encryption algorithm is AES-256. Whenever implementing encryption, always use the strongest algorithm your system can handle. Remember that many older algorithms are not acceptable (e.g., rc4, DES).

Anywhere PHI is stored you should have encryption enabled so the data requires a decryption key to view it. Most computer systems can automatically handle encryption if they are properly configured.

TREVOR HANSEN

SecurityMetrics | CISSP | CDCDP | QSA
HIPAA COMPLIANT EMAILS

Patient data needs to be encrypted, especially when you send patient data outside of your organization. According to the HHS Breach Portal, over 100 organizations since 2009 have had PHI stolen because of inadequate email encryption. Healthcare organizations must “implement a mechanism to encrypt electronic protected health information whenever deemed appropriate” in requirement §164.312(e)(2)(ii), such as when sending unencrypted PHI in unprotected email services (e.g., Gmail, Outlook, AOL, etc.).

Organizations can send PHI via email, if it is secure and encrypted. According to the HHS, “the Security rule does not expressly prohibit the use of email for sending ePHI. However, the standards for access control, integrity and transmission security require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to ePHI.”

Due to how interconnected emails are and the struggles to properly secure it through encryption, consider avoiding the transmission of PHI via email whenever possible.

If you need to send emails, the use of patient portals is preferred for sending information to patients, and secure file transfer options are preferred for covered entity to covered entity or covered entity to business associate communications.

As a general rule, free and Internet-based web mail services (e.g., Gmail, Hotmail, AOL) are not considered secure for the transmission of PHI.

If you are determined to use an Internet-based email service, ensure they sign a Business Associate Agreement (BAA) with you. Microsoft and Google recently stated they will sign BAAs. However, a BAA only goes so far, and you are still ultimately responsible. The Omnibus Rule states the covered entity is still responsible for ensuring the business associate does their part. If found in violation of HIPAA, both parties are liable for fines. The BAA typically only covers their systems that touch PHI; you’re in charge of protecting the rest of the chain.
EMAIL DATA
We interviewed 53 healthcare professionals (who were responsible for HIPAA compliance) about email compliance. Throughout this section, you’ll find results from this survey:

ORGANIZATIONS SEND EMAILS CONTAINING PATIENT DATA

If you send emails containing patient data, make sure that you have adequate security in place (e.g., patient portal, email encryption).

ORGANIZATIONS ENCRYPT EMAILS CONTAINING PATIENT DATA

Emails containing patient data need to be encrypted.
EMAIL SECURITY

EMAIL PASSWORDS
Make sure access to your email account is protected by complex, strong passwords (e.g., passphrases). For example, a password should not be found in a dictionary in any language. It should contain at least eight upper and lower case letters, numbers, and special characters. Passwords should be changed every 90 days.

EMAIL DISCLAIMERS
Email disclaimers and confidentiality notices are not a free ticket to send PHI-filled unencrypted emails. That’s not their purpose. A disclaimer on your emails should merely inform patients and recipients that the information is PHI and should be treated as such. Your legal department can assist with the verbiage. The key to remember is that no disclaimers will alleviate your responsibility to send ePHI in a secure manner.

SECURING DIFFERENT TYPES OF EMAILS

IN-OFFICE EMAILS
Emails sent on your own secure server do not have to be encrypted. From nurse to doctor, office manager to nurse, surgeon to lab tech, etc. However, if you use remote access you must follow typical encryption rules. Options like Outlook Web Access can easily leak PHI, are difficult to properly secure, and should be avoided.

DOCTOR-TO-DOCTOR EMAILS
Do you have to encrypt an email if it’s going to another doctor? The answer is, unless that doctor is in your office, on your own secure network and email server, it needs to be encrypted. Remember, you are in charge of proper encryption during transmission.

PERSONAL EMAILS
Doctors sometimes work on cases using home computers, and then email the PHI back to their work email. Unless each of those emails is secured with encryption, this doctor just made a huge mistake.

PROVIDERS CAN EXCHANGE EMAILS WITH PATIENTS AND STILL BE HIPAA COMPLIANT, AS LONG AS THEY ARE SENT SECURELY.
MASS EMAILS
Don’t send any. If you need to send mass messages, use a mail merge program or HIPAA compliant service (think business associate) which creates a separate email for each recipient. The danger of using BCC? Email addresses aren’t usually hidden to the bad guys.

REPLY EMAILS
If someone replies to your email, is that communication secure? Technically, that’s not your concern. HIPAA states that the entity/person conducting the transmission is the liable party. So, if the replier is not a covered entity or business associate, it’s impossible for them to violate HIPAA. If the replier is a covered entity or business associate, the protection of that data is now their problem, not yours. As soon as you reply back, however, then you are again liable for the security of that transmission.

PATIENT EMAILS
How do you protect messages initiated by patients? According to HHS, the health-care provider can assume (unless the patient has explicitly stated otherwise) that email communications are acceptable to the individual. Providers should assume the patient is not aware of the possible risks of using unencrypted email. The provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications. Remember, you must provide alternate secure methods of providing the information to the patient.

ORGANIZATIONS EMAIL PATIENT DATA TO THE FOLLOWING INDIVIDUALS

<table>
<thead>
<tr>
<th></th>
<th>10%</th>
<th>26%</th>
<th>43%</th>
<th>63%</th>
<th>39%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doctors outside of their network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CE outside of their network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA outside of their network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Themselves</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Only send patient data to those who need this information.*
ALTERNATIVES TO EMAIL

Due to the nature of email and the struggles to properly secure it, we recommend avoiding it whenever possible. Some alternatives include:

PATIENT PORTALS

The use of patient portals is preferred for sending information to patients, and secure file transfer options are preferred for covered entity to covered entity or covered entity to business associate communications.

Patient portals are designed for healthcare professionals to safely access their PHI online any time necessary. Not only do patient portals allow covered entities to securely communicate with other covered entities or business associates, but also patients can easily access their own information (e.g. medication information). Some portals even allow patients to contact their healthcare provider about questions, set-up appointments, or even request prescription refills.

CLOUD-BASED EMAIL SERVERS

Use a secure cloud-based email platform (e.g., Office365, NeoCertified), which hosts a HIPAA compliant server. It’s important to connect to the server via HTTPS so you have an encrypted connection between you and your email server. Unfortunately, this option does not control the email transmission from the cloud server to the recipient’s server or workstation, so though it seems attractive, we only recommend this option when all senders and all recipients have accounts on the same cloud-based email service.

ENCRYPTED EMAIL SERVICES

Services (e.g., Zixmail, Paubox Encrypted Email) actually encrypt the message all the way from your workstation to the recipient’s workstation. If the recipient is not an email service client, the system will notify them of the email and the recipient can then connect securely to the encrypted email server to retrieve the message.

ORGANIZATIONS USE THE FOLLOWING EMAIL TECHNOLOGY
MOBILE DEVICE SECURITY

Like sending emails, mobile devices require additional security measures to make sure patient data is protected. Mobile devices often don’t have the same security policies as workstations and servers. Because of this, mobile devices may not be protected with technology like firewalls, encryption, or antivirus software.

In addition, when a healthcare provider uses their own personal smartphone or tablet to access patient data (i.e., BYOD procedures), these devices are vulnerable due to other apps on the device. With each downloaded app, the risk grows.

Think about others accessing that mobile device outside the office. For example, sometimes physicians, dentists, office managers, etc., let their kids play with their personal/work smartphone, then someone accidentally downloads a malicious app that can read the keyboard patterns of the user. The next time the doctor accesses his patient data, that malware may steal the password to the EHR.

MOBILE DEVICE DATA

We interviewed 53 healthcare professionals (who were responsible for HIPAA compliance) about mobile devices. Throughout this section, you’ll find results from this survey.

EMPLOYEES USE PERSONAL MOBILE DEVICES TO ACCESS PATIENT DATA

![Chart showing 17% of employees use personal mobile devices to access patient data, while 83% do not.]

Ideally, employees should use organization-owned mobile devices to access patient data, instead of their own mobile devices.
EMPLOYEES USE ORGANIZATION-OWNED MOBILE DEVICES FOR NON-OFFICE RELATED ACTIVITIES

If mobile devices are used to access, create, transmit, receive, or store PHI, they should not be used for other non-office related activities (e.g., checking personal emails, downloading apps).

SECURITY TIPS

Because of all these issues that come along with the convenient BYOD strategy, there are a few precautions you should follow to comply with HIPAA and ensure patient data security.

The best mobile security practice is: don’t implement a BYOD strategy. That said, we realize that can be impractical.

Protecting and securing health information while using a mobile device is a healthcare provider’s responsibility. To address these concerns, consider using the National Institute of Standards and Technology (NIST) mobile guidelines for healthcare security engineers and providers.

FOLLOW BASIC MOBILE SECURITY PRACTICES

There are some obvious things you should and shouldn’t do with your patient data while using your mobile device. For example:

- Accept all OS and app updates immediately. Just like computers, mobile devices must be patched often to eliminate software or hardware vulnerabilities found after initial release.
- Never connect to unsecured Wi-Fi.
- Use discretion when downloading apps. Even if apps look legitimate, they may be infected with malware that could compromise patient data, and cause a serious data breach.
- Don’t jailbreak your device. Jailbreaking your device removes a lot of its built-in security. While this may let you do more with your device, it also leaves it more vulnerable to attacks.
• Make sure the devices you plug your mobile device into (e.g., your home computer, work laptop, etc.) are secure. If your computer/network isn’t secure, it could act as a portal for hackers to gain access to your mobile device.

• Implement an 8-character password/pin with a special character and alphanumeric on your mobile device, where applicable. It’s not foolproof, but it’s another layer of security.

• Connect to your EHR via secured remote access, either a virtual private network (VPN) or through multi-factor authentication.

• Encrypt your data. If you have sensitive data on your mobile device, make sure it’s encrypted. Patient data will then remain secure, even if malware steals it.

• Use mobile vulnerability scanning. You can’t prevent what you don’t know about. A vulnerability scanner like SecurityMetrics Mobile for your mobile device can help discover weaknesses.

• Establish mobile device policies. Whether your company owns the devices, or your employees use their own, you need to have security policies set up that address the use of mobile devices.

• Train employees on mobile device policies. Your employees should know about malware and take the right measures to avoid it. Make sure to include mobile device security in your training.

• Remote wipe devices immediately after they have been lost and/or stolen, when applicable. This remotely erases the sensitive data on mobile devices.

Even though mobile devices can be hard to fit into a traditional network or data security model, they need to be considered. It’s critical to include them in your information security planning.

**ORGANIZATIONS HAVE A MOBILE DEVICE POLICY**

![Diagram showing survey results: 55% Yes, 39% No, 6% Don’t know.]

*Organizations that use mobile devices need to have a mobile device policy (e.g., BYOD policy, policy for work tablets).*
IF YOU DON’T SECURE MOBILE DEVICES, YOUR COMPANY’S SENSITIVE DATA IS AT RISK.

IMPLEMENT MOBILE ENCRYPTION
If you can, avoid storing sensitive information on mobile devices to limit the threat of a data breach altogether.

Most mobile encryption services are not as secure and reliable as other devices because most mobile devices themselves aren’t equipped with the most secure encryption. Mobile technology is only as secure as a device’s passcode. For example, Apple’s Data Protection API only encrypts the built-in mail application on iPhones and iPads, and only after you enable a passcode. Encryption does not apply to calendars, contacts, texts, or anything synchronized with iCloud. Some third party applications that use Apple’s Data Protection API are also encrypted, but this is rare.

If someone were to jailbreak your mobile device, information protected by the Data Protection API would remain encrypted only if the thief didn’t know the decryption key. Android’s encryption program works similarly, requiring a password to decrypt a mobile device each time it’s unlocked.

Additionally, if you backup your mobile device on your hard drive, ensure the backups are encrypted.

Although HIPAA regulations don’t specify the required encryption, industry best practice would be to use AES-128 or Triple DES encryption (or better).

ORGANIZATIONS USE MOBILE ENCRYPTION

Mobile devices require the same restrictions and encryption processes as other work devices like desktop or laptop computers.
PHYSICAL ACCESS

CONTROL PHYSICAL ACCESS TO YOUR WORKPLACE

In addition to protecting your ePHI, make sure to protect physical PHI. Many healthcare organizations don’t always worry as much about the physical aspect. While many foundational security issues may have been addressed, organizations are likely to have overlooked details such as:

- Unlocked office / storage doors
- Window blinds
- Reception desks
- Lack of screensavers and privacy monitors
- Theft of devices/hardware
- Malware in left-behind devices

Employees may think physical security only applies after hours. However, most data thefts occur in the middle of the day, when staff is too busy with various assignments to notice someone walking out of the office with a server, company laptop, phone, etc.

THE MAJORITY OF PHYSICAL DATA THEFTS TAKE LESS THAN ONLY MINUTES IN PLANNING AND EXECUTION.

To help control physical threats, create a physical security policy that includes all rules and processes involved in preserving onsite business security. For example, if you keep confidential information, products, or equipment in the workplace, keep these items secured in a locked area. If possible, limit outsider office/business access to one monitored entrance, and (if applicable) require non-employees to wear visitor badges at all times.

Don’t store sensitive information or documents in the open. For example, reception desks are often filled with information like passwords written on sticky notes, computers without privacy monitors, and patient records lying out in the open.
You also need to control employee access to sensitive areas, which must be related to an individual’s job function. To comply with this requirement, you must document:

- Who has access to secured environments and their business need.
- What, when, where, and why devices are used
- A list of authorized device users
- Locations where the device is and is not allowed
- What applications can be accessed on the device

Access documentation must be kept up-to-date, especially when individuals are terminated or their job role changes.

Keep an up-to-date inventory of all removable devices including a list of authorized users, locations the device is assigned or is not allowed, and what applications are allowed to be accessed on the device. Best practice is to not allow these devices to leave the office, but if they do, consider attaching external GPS tracking technology and remote wipe on all laptops, tablets, external hard drives, flash drives, and mobile devices.

In addition, make sure all workstations have an automated timeout/logout on computers and devices (e.g., a password-protected screensaver pops up on a computer after a set amount of time). This helps discourage thieves from trying to access data from these workstations when employees aren’t there.

**ORGANIZATIONS HAVE AUTOMATIC TIMEOUTS/LOG OUTS ON WORKSTATIONS**

*All workstations need to have an automated timeout/logout (i.e., a password-protected screensaver enabled after a time of disuse.*)
PHYSICAL SECURITY BEST PRACTICES
Most physical security risks can be prevented with little effort. Here are some suggestions:

- While working on your risk analysis, look for physical security risks
- Lock all office doors when not in use day and night
- Require passwords to access computers and mobile devices (encrypt your data or don’t have data on devices)
- Use screensavers and privacy monitors on computers
- Install and use blinds in all office windows
- Keep logs of who goes in and out
- Keep track of devices that go in and out
- Have policies in place for stolen equipment (Make sure to have a good Incident Response Plan and know your Breach Notification Policy front and back.)
- Train staff against social engineering
- Limit access to PHI through role-based access.
- Have staff report suspicious people and devices
- Make sure all reception desks protect PHI from prying eyes
- Monitor sensitive areas with video cameras and store the video logs for appropriate durations

TRAIN EMPLOYEES OFTEN
While you may understand how to protect sensitive information and your own proprietary data, your employees may not. That’s why regular security trainings are so important.

Social engineering is a serious threat to both small and large organizations. A social engineer uses social interaction to gain access to private areas, steal information, or perform malicious behavior, and employees can fall for their tricks more often than you think.

For example, if a man walked into your storefront and said he was there to work on your network and needed you to lead him to the server room, would your employees think twice to further identify him and verify his presence?

Train your employees to question everything. It’s better to be safe than sorry. Establish a communication and response policy in case of suspicious behavior. Train employees to stop and question anyone who does not work for the company, especially if the person tries to enter the back office or network areas.
HIPAA COMPLIANT FIREWALLS

Network firewalls (e.g., hardware, software, and web application firewalls) are vital for your HIPAA compliance efforts. A firewall’s goal is to filter potentially harmful Internet traffic from the Internet to protect valuable PHI. Simply installing a firewall on your organization’s network perimeter doesn’t make you HIPAA compliant.

HARDWARE FIREWALLS

A hardware firewall (or perimeter firewall) is typically installed at the perimeter of an organization’s network to protect internal systems from the Internet. Hardware firewalls are also often used inside the environment to create isolated network segments separating networks who have and don’t have access to PHI.

In summary, a hardware firewall protects environments from the outside world. For example, if an attacker tries to access your systems from the outside, your hardware firewall should block them.

**PROS**

- Most robust security option
- Protects an entire network
- Can segment internal parts of a network

**CONS**

- Generally more expensive
- Difficult to configure properly
- Needs to be maintained and reviewed regularly

SECURE NETWORKS RELY ON HARDWARE, SOFTWARE, AND WEB APPLICATION FIREWALLS.
SOFTWARE FIREWALLS

You also need a firewall between systems that store PHI and all other systems, even internal ones. Software firewalls are used to protect a single host from internal threats, particularly mobile devices that can move "outside" of the secure corporate environment.

Many computers come preinstalled with software firewalls, but for computers connecting to PHI remotely, a personal firewall is required. For example, if a receptionist accidentally clicks on a phishing email scam, their computer’s software firewall should stop the malware from infecting the computer.

**PROS**
- Better facilitates mobile workers outside the corporate network
- Less expensive
- Easier to maintain

**CONS**
- Doesn’t protect an entire network
- Fewer security options

WEB APPLICATION FIREWALLS

Web application firewalls (WAFs) should be implemented in front of public-facing web applications to monitor, detect, and prevent web-based attacks. Even though these solutions can’t perform the many functions of an all-purpose network firewall, (e.g., network segmentation), they specialize in one specific area: monitoring and blocking web-based traffic.

A WAF can protect web applications visible or accessible from the Internet. Your WAF must be up to date, generate audit logs, and either block cyberattacks or generate a cyber security alert if an imminent attack is suspected.

**PROS**
- Immediate response to web application security flaws
- Protection for third party modules used in web applications
- Deployed as reverse proxies

**CONS**
- Requires more effort setting up
- Possibly break critical business functions (if not careful)
- May require some network re-configurations
FIREWALL DATA
We interviewed 52 healthcare professionals (who were responsible for HIPAA compliance) about firewalls, asking questions ranging from firewall types, managed firewalls, firewall rules, and firewall logs. Throughout this section, you’ll find results from this survey.

TYPES OF FIREWALLS ORGANIZATIONS USE

All networks (whether small or large) need both a hardware and software firewall.

FIREWALL CONFIGURATION
CONFIGURATION ISSUES
After installation, you likely need to spend some time setting up your firewall. The easiest way to configure your firewall is by restricting and controlling the flow of traffic as much as possible, specifically around networks with PHI access.

IF YOUR FIREWALL ISN’T CONFIGURED AND MAINTAINED PROPERLY, YOUR NETWORK IS NOT SECURE.
Depending on how complex your environment is, you might require many firewalls to ensure all systems are separated correctly. The more controls you have, the less chance an attacker has at getting through unprotected Internet connections.

Establish your firewall rules or Access Control Lists (ACLs). The ACLs will help the firewall decide what it permits and denies into and out of your network. Firewall rules typically allow you to whitelist, blacklist, or block certain websites or IP addresses.

When no ACLs have been configured, everything is likely allowed in or out of the network. Rules are what give firewalls their security power, which is why they must constantly be maintained and updated to remain effective. Remember, your firewall is your first line of defense, so you should dedicate some time to make sure it’s set up correctly and functioning properly.

**NETWORK FIREWALL(S) MANAGED BY A SECURITY PROFESSIONAL OR THIRD PARTY**

Though not required, managed firewall(s) can help organizations with complex firewall rules and firewall management.

**FIVE BASIC FIREWALL CONFIGURATION BEST PRACTICES**

**SET SECURITY:** Set security settings for each switch port, particularly if using segmentation

**ESTABLISH RULES:** Update firewall rules if your applications and/or systems don’t have proper security hardening in place (e.g., out-of-date software, default accounts and passwords)

**USE VPNS:** If using remote access, set up virtual private networks (VPNs)

**INBOUND/OUTBOUND RULES:** Decide what traffic comes in and out of your network

**ADD/CLOSE SWITCH PORTS:** Segment different networks with switch ports (e.g., Internet, office, EMR)
TEST AND MONITOR CONFIGURATION
No matter the size of your environment, things change over time. Firewall rules will need to be revised over the course of a few months and at least every six months. Use vulnerability scans and penetration tests to find weaknesses in your network. Vulnerability scans are great weekly, monthly, or quarterly insight into your network security, while penetration tests are a more thorough way to deeply examine network security.

HOW OFTEN FIREWALL RULES ARE REVIEWED

A security professional should regularly review your firewall rules (e.g., at least quarterly).

CONSIDER NETWORK SEGMENTATION
Healthcare organizations often setup large flat networks, where everything inside the network can connect to every-things else. They may have one firewall at the edge of their network, but that’s it. Generally, the more places that have access to patient information, the higher the chances for a HIPAA violation or data breach.

Firewalls can be used to implement segmentation within an organization’s network. When you create networks with PHI access (e.g., EMR systems) firewalled off from the rest of the day-to-day business traffic, you can better ensure patient data is only sent to known and trusted sources.

For example, you install and configure a multi-interface firewall at the edge of your network. From there, you create one interface on the firewall dedicated just to the systems that store/process/transmit PHI data. If that interface doesn’t allow any other traffic into or out of any other zones, this is proper network segmentation.

Segmentation can be extremely tricky, especially for those without a technical security background. Consider having a security professional double check all your segmentation work (e.g., segmentation checks).
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

FIREWALL BEST PRACTICES

Large healthcare organizations typically have firewalls in place, at least at the perimeter of their network (e.g., hardware firewalls). But be careful when selecting firewalls, making sure they support the necessary configuration options to protect critical systems and provide segmentation between the networks that do and do not have PHI access.

Smaller organizations sometimes struggle to understand firewall basics, and they often do not have the necessary in-house expertise to configure and manage them correctly and securely. If this is the case, a third party service provider should be contracted to provide assistance, rather than simply deploying a default configuration and hoping for the best.

It may seem obvious, but leave as few holes as possible in your firewall. Rules should be as specific as possible for your network(s); don’t just allow access to all Internet connections. For example, if you have third parties that remotely support your networks, limit their inbound access and time-frames they can access your network. Then spend time to review your firewall rules and configuration.

Firewalls are a first (and often the only) line of defense, and strict attention needs to be given to the logs and alerts they generate. Often, the volume of log data can be overwhelming, so organizations don’t look through them. But it’s important (and required) to review firewall logs daily in order to identify patterns and activity that indicate attempts to breach security. There are many good software packages available to help merchants deal with the volume of log data and to more easily pick out the important data that requires you to take action.

For firewall implementation and maintenance, remember to follow these three practices:

1. Write strict firewall rules
2. Pay attention to what logs tell you
3. Review firewall configurations frequently, adjust as necessary, and document everything

TREVOR HANSEN
SecurityMetrics | CISSP | CDCDP | QSA
WIRELESS NETWORKS (WI-FI)

Most healthcare organizations have wireless networks (i.e., Wi-Fi). Wi-Fi access has also become a waiting room norm. The problem is many offices don't have their Wi-Fi set up correctly with adequate encryption, turning this free patient asset into a liability.

This is also the case if you do not segment guest and non-guest wireless networks with a firewall. For example, if you don't, you have probably allowed impermissible disclosure of patient data and don't even know it. Guest wireless networks should always be segmented from your non-guest wireless network by a firewall.

For example, if your Wi-Fi network name was DrSwenson, you should set up another Wi-Fi network exclusively for patients named DrSwensonGuest. Nurses, office managers, and physicians should only use DrSwenson, and patients should only use DrSwensonGuest.

In addition, make sure that only staff can connect to your non-guest network(s) with approved devices, and these devices follow your BYOD policies.

WIRELESS SECURITY TIPS

WPA2 ENCRYPTION

Security best practice is to set up your Wi-Fi with WPA2. Since 2006, WPA2 has been the most secure wireless encryption standard. Avoid using outdated WEP encryption, as it is easy to compromise.

UNIQUE PASSWORD

Another important safety aspect is to make sure the Wi-Fi password used is secure. Don't use the default password or username that comes with the wireless router.

SCAN ROGUE WIRELESS ACCESS POINTS

Rogue wireless access points can allow attackers unauthorized access to secure networks, granting them the access to attack your network remotely.

Consequently, it is vital to scan for rogue wireless access points, particularly if they are attached to your non-guest network. This helps you identify which access points need to be changed.
SYSTEM CONFIGURATION STANDARDS

SYSTEM HARDENING
Any system with access to PHI needs to be hardened before use; the goal of hardening a system is to remove any unnecessary functionality and to configure the system in a secure manner.

For example, organizations should address all known security vulnerabilities and be consistent with industry-accepted system hardening standards. Some good examples of hardening guidelines are produced by the following organizations:

• Center for Internet Security (CIS)
• International Organization for Standardization (ISO)
• SysAdmin Audit Network Security (SANS) Institute
• National Institute of Standards Technology (NIST)

SYSTEM CONFIGURATION MANAGEMENT
Consistency is key when trying to maintain a secure environment. Once system hardening standards have been defined, it is critical that they are applied to all systems in the environment in a consistent fashion. After each system or device in the environment has been appropriately configured, you still aren’t done. Many organizations struggle to maintain standards over time, as new equipment or applications are introduced into the environment.

This is where it pays to maintain an up-to-date inventory of all types of devices, systems, and applications connected to PHI. However, the list is not any good if it doesn’t reflect reality. Make sure someone is responsible for keeping the inventory current and based on what is actually in use. This way, applications or systems that are not approved to access PHI can be discovered and addressed.

Many organizations, especially larger ones, turn to one of the many system management software packages on the market to assist in gathering and maintaining this inventory. These applications are able to scan and report on hardware and software used in a network and can also detect when new devices are brought online. These tools are often also able to “enforce” configuration and hardening options, alerting administrators when a system is not compliant with your internal standard.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

SYSTEM CONFIGURATION
You’re required to use industry accepted configuration or hardening standards when setting up your servers, firewalls, or any system in-scope for HIPAA.

Examples of system hardening practices include disabling services and features you don’t use, uninstalling applications you don’t need, limiting systems to perform a single role, removing or disabling default accounts, and changing default passwords and other settings. Permitting anything unnecessary to remain on a system opens you up to additional risk and possible vulnerability.

The key to system configuration and hardening is consistency. Once you have documented a standard that meets the requirements of your environment, make sure processes are in place to follow the standard as time goes on. Keep your standard and process up to date to take into account changes to your business or requirements.

Automated tools can simplify the task of enforcing configuration standards, allowing administrators to quickly discover systems that are out of compliance.

JEN STONE
SecurityMetrics | MSCIS | CISSP | QSA
REGULAR SYSTEM UPDATES AND PATCHES

Application developers will never be perfect and technology constantly changes, which is why updates to patch security holes are frequently released. Once a hacker knows he can get through a security hole, he passes that knowledge on to the hacker community who then exploits this weakness until the patch has been updated. Consistent security updates are crucial to your security posture.

Patch all critical components in the PHI flow pathway, including:

- Internet browsers
- Firewalls
- Application software
- EHR/EMR
- Databases
- Operating systems

Older Windows systems in particular can make it difficult for merchants to remain secure, especially when the manufacturer no longer supports a particular operating system or version (e.g., Windows XP, Windows Server 2003). Operating system updates often contain essential security enhancements specifically intended to correct recently exposed vulnerabilities. When organizations fail to apply such updates and patches to their operating systems, the vulnerability potential increases exponentially.

Be vigilant about consistently updating the software associated with your system. Don’t forget about critical software installations. To help you keep up to date, ask your software vendors to put you on their patch/upgrade email list.

The more systems, computers, and apps your company has, the more potential weaknesses. Vulnerability scanning is arguably the easiest way to discover software patch holes that cybercriminals would use to exploit, gain access to, and compromise an organization.

ESTABLISH SOFTWARE DEVELOPMENT PROCESSES

If you develop in-house applications, you must use very strict development processes and secure coding guidelines. Don’t forget to develop and test applications in accordance with industry accepted standards like the Open Web Application Security Project (OWASP).

BE VIGILANT ABOUT CONSISTENTLY UPDATING THE SOFTWARE ASSOCIATED WITH YOUR SYSTEM.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

SYSTEM UPDATING AND SOFTWARE DEVELOPMENT
This requirement is made up of two parts. The first part is system component and software patching, and the second part is software development.

System Administrators have the responsibility to ensure all system components (servers, firewalls, routers, workstations, etc.) and software are updated with critical security patches within 30 days of when they are released to the public. If not, these components and software are vulnerable to malware and/or security exploits.

One reason systems or software might be excluded from updates is because they simply weren’t able to communicate with the update server (e.g., WSUS, Puppet), possibly resulting from a network or system configuration change that inadvertently broke the communication. It’s imperative that System Administrators are alerted when security updates fail.

When developing software (e.g., web applications), it’s crucial companies adopt the OWASP standard. This will guide them in their web application development process by enforcing secure coding practices and keep software code safe from malicious vulnerabilities (e.g., cross-site scripting, SQL injection, insecure communications, etc.).

Insecure communications, for example, has been in the spotlight recently since SSL and TLSv1.0 are no longer considered acceptable forms of encryption when data is being transmitted over open, public networks.

Companies need to embrace the idea of change control for their software development and system patching/updating. There are a four requirements detailed of what a proper change control process should contain:
  • All changes must have a documented explanation of what will be impacted by the change.
  • All changes must have documented approval by authorized parties.
  • Any changes to a company’s production environment must undergo proper iterations of testing and QA before being released into production.
  • The change control process must always include a back-out or roll-back procedure in case the updates go awry.

MATT GLADE
SecurityMetrics | CISSP | QSA
SECURE USER ACCESS

CHANGE DEFAULT PASSWORD WEAKNESSES

Unknown to many organizations, medical devices are often installed and used without changing their default passwords. However, most default passwords and settings are well known throughout hacker communities and are easily found via a simple Internet search. When defaults aren’t changed, it provides attackers an easy gateway into a system. Changing vendor defaults on every system with exposure to patient data protects against unauthorized users.

In one SecurityMetrics forensic investigation, it was discovered that a third party IT vendor purposely left default passwords in place to facilitate easier future system maintenance. Default passwords might make it easier for IT vendors to support a system without having to learn a new password each time; but convenience is never a valid reason to forego security, nor will it defray liability.

WEAK PASSWORDS AND USERNAMES

Even if default passwords are changed, if a username and password aren’t sufficiently complex, it will be that much easier for an attacker to gain access to an environment. An attacker may try a brute-force attack against a system by entering multiple passwords (via an automated tool entering thousands of password options within a matter of seconds) until a password works.

Remember, secure passwords should be changed every 90 days, and have at least 10 characters including an upper and lower case letter, number, and special character. Passwords that fall short of these criteria can easily be broken using a password-cracking tool. In practice, the longer and more characters a password has, the more difficult it will be for an attacker to crack a password.

Instead of common usernames (i.e., admin, administrator, the company name, or a combination of the two), organizations should have unique usernames.

SAMPLE OF COMMON BAD USERNAMES AND PASSWORDS:

USERNAME:
ADMIN, USERNAME, TEST, ADMIN1, SYSADMIN, DEFAULT, GUEST, PUBLIC

PASSWORD:
PASSWORD1, ADMIN1234, MONKEY!, TEST1234, CHANGEME!, LETMEIN1234
EMPLEYEEHES HAVE UNIQUE ID CREDENTIALS

We interviewed 42 healthcare professionals (who were responsible for HIPAA compliance) about patient data access. Throughout this section, you’ll find results from this survey, such as the following graph:

All employees should have their own login IDs and passwords for computer, software, and physical access.

Although organizations may have ID credential policies in place (e.g., requiring a unique ID credential and complex password), employees often do not follow these policies.

Employees might have unique ID credentials, but they often share it with other workforce members, thinking that they can share usernames and passwords with individuals that have access within their system, such as nurses, providers, and receptionists. For example, if a doctor has shared their credentials with their receptionists to help with documentation or access information for patients, these employees don’t really have unique ID credentials.

CONVENIENCE IS NEVER A VALID REASON TO FOREGO SECURITY, NOR WILL IT DEFRAY LIABILITY.
UNIQUE ID AND PASSWORDS
This requirement is all about having unique ID information. For example, you must have your own unique ID credentials and account on your laptop, with strong password cryptography. Don’t use generic accounts, shared group passwords, or generic passwords.

Today we see broader adoption of multi-factor authentication even outside the HIPAA realm, which is great for security. This can include your personal email, Gmail, Dropbox, and other services.

Security professionals recognize that passwords are no longer a great way to secure data. They are simply not secure enough, but are still required. You need to set strong, long passwords. A password should be at least 10 characters long and complex with at least an alphabetic and numeric character.

An easy way to remember complex passwords is by using passphrases. For example, pick a phrase like “I eat oranges on Tuesday mornings” and add in some numbers and special characters. Your passphrase might look like this: “Ieootm@1235!”

In addition to strong passphrases, password manager software can help you use different passwords for all your accounts. Some password managers can even work across multiple devices and sync across the Cloud.

You really need different passwords for different services, so if one service gets compromised, it doesn't bleed into other passwords for other sites. For example, if your email account password is compromised and you use the same password across devices and websites, you have a major security problem on your hands.

BRAND BARNEY
SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
ROLE-BASED ACCESS CONTROL

According to HIPAA requirement §164.312(a)(1), you’re required to have a role-based access control system, which grants access to PHI and systems to individuals and groups on a need-to-know basis. Configuring administrator and user accounts prevents exposing sensitive data to those who don’t have a need-to-know.

HIPAA requires a defined and up-to-date list of the roles with access to PHI. On this list, you should include each role, the definition of each role, access to data resources, current privilege level, and what privilege level is necessary for each person to perform normal business responsibilities. Users must fit into one of the roles you outline.

HAVE A DEFINED AND UP-TO-DATE LIST OF THE ROLES WITH ACCESS TO SYSTEMS WITH PHI ACCESS

User access isn’t limited to your normal office staff. It applies to anyone who needs access to your systems or the area “behind the desk,” like that IT guy you hired on the side to update your EMR software. You need to define and document what kind of user permissions they have.

EXAMPLE USER ACCESS ROLES

- Receptionist
- Provider
- Medical student
- Staff nurse
- Nursing manager
- Third party IT
- Physician assistant
- Night security
- Specialist
- Radiologist
- Administrator
- Dentist
- Volunteer
LIMITED ACCESS BETWEEN INTERNET AND PATIENT DATA STORAGE SYSTEMS

Limit all computers or electronic devices with PHI access to only go to necessary websites (e.g., disable access to media websites like Facebook, Twitter, Gmail, etc.).

HOW TO IMPLEMENT ACCESS CONTROLS

**Electronic systems access:** Usernames are a great way to segment users by role. It also gives you a way to track specific user activity. The first question you need to ask yourself is, does each staff member have a unique user ID? If not, that’s a great place to start.

**Physical access:** Make sure anyone not on your regular staff is escorted around the office by a staff member. For patients, don’t leave them unattended with logged-in equipment. For everyone else, document their name, reason for being at your organization, what company they’re from, and what they look like. If you haven’t worked with this person before, call the company and verify their name and physical description.
SECURING YOUR REMOTE ACCESS

REMOTE ACCESS BASICS
Remote access applications (e.g., GoToMyPC, LogMeIn, pcAnywhere, or RemotePC) allow healthcare employees to work from home. Doctors often prefer to access patient data outside of the office, and some IT and billing teams use remote access to access the healthcare network offsite.

Remote access is great for workforce convenience, but often causes issues for security. Often, remote access is not properly implemented with adequate security, such as implementing multi-factor authentication (e.g., a password and an auto-generated SMS).

Attackers commonly target organizations that use remote access applications. If a remote access application is vulnerable, it allows an attacker to completely bypass firewalls and gain direct access to office and patient data.

A remote access attack typically looks like the following:
1. Scan the Internet for vulnerable IP addresses
2. Run a password-cracking tool on each IP address found
3. Upload malware
4. Copy PHI Data
5. Potentially use the compromised system to attack other computers or networks

HIPAA Security Rule §164.308(a)(4) and HIPAA Privacy Rule §164.508 require organizations to "develop and implement policies and procedures for authorizing ePHI access," such as only allowing PHI access to trained workforce who have proper authorization and need to access PHI.

HHS further explains that organizations must "establish remote access roles specific to applications and business requirements. Different remote users may require different levels of access based on job function." HHS recommends that organizations using remote access should implement multi-factor authentication to access systems containing PHI.
REMOTE ACCESS DATA
We interviewed 42 healthcare professionals (who were responsible for HIPAA compliance) about remote access. Throughout this section, you’ll find results from this survey, such as the following graph:

ORGANIZATIONS ALLOW REMOTE ACCESS INTO THEIR NETWORK

If you use remote access, make sure to implement adequate security, such as multi-factor authentication and proper firewall configuration.

ENABLE MULTI-FACTOR AUTHENTICATION
Remote access can be secure as long as it uses strong encryption and requires two independent methods of authentication (i.e., multi-factor authentication). Be sure to enable strong/high encryption levels in your remote access configuration.

Multi-factor authentication makes things difficult for attackers. If you implement a password and four-digit PIN sent through SMS to your phone, an attacker would have to learn your password and have your cell phone before being able to gain remote access to your systems.

Configuring multi-factor authentication requires two of the following three factors:

- Something only the user “knows” (e.g., a username and password)
- Something only the user “has” (e.g., a cell phone, bar code, or an RSA SecureID token)
- Something the user “is” (e.g., a fingerprint, ocular scan, voice print, or other biometric)
A few examples of effective multi-factor authentication remote access authentication include:

1. The remote user enters their username and password, and then must enter an authentication code that is sent to them on their cell phone.

2. Access to the remote access application is blocked to the outside. The remote user must call in to the location and speak with an authorized manager who recognizes them by voice. The onsite manager then opens a remote session. The remote user must then enter their username and password.

If you use remote access, make sure to implement adequate security, such as two-factor authentication.

IF A REMOTE ACCESS APPLICATION CONFIGURATION ONLY REQUIRES THE USER TO ENTER A USERNAME AND PASSWORD, THE APPLICATION HAS BEEN CONFIGURED INSECURELY.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

REMOTE ACCESS– SECURITY’S DOUBLE-EDGED SWORD
The benefits of being able to connect to patient data from home or the coffee shop is a temptation for most healthcare professionals. Some insist it is a vital component to delivering quality, timely care.

Unfortunately, attackers commonly target organizations that use remote access applications. Plus, remote access is often poorly configured and doesn’t have proper safeguards, which if compromised, an attacker can completely bypass firewalls and gain access to office and patient data.

For instance, the Target breach occurred when attackers first gained access to Target through a poorly protected remote access application. With a computer and Internet connection, a malicious attacker can scan the entire Internet in less than a day looking just for open remote access ports.

To stop these attacks, first make sure that remote access is only provided to individuals who absolutely need it. Employees should never share remote access credentials (or any credential for that matter). One of the best ways of correctly determining who should have access is by setting up user privileges by role. First, define roles that respond to your organization’s structure (i.e., hospitals may have dozens of different roles, physician offices likely less than 10). Each role should then be assigned the minimum amount of access required for an employee to perform their job.

Next, you need to implement multi-factor authentication. Using a single factor (a password and username) makes it easy for attackers to gain access. However, by implementing strong authentication processes (e.g., multi-factor authentication), you can keep remote access secure.

One example may be that you use a password and username in conjunction with a security token that regularly generates a new, unique access code (e.g., four-digit PIN sent through SMS to your phone). This makes it so an attacker would have to learn your password and have your cell phone before being able to gain remote access to your systems.

RYAN MARSHALL
SecurityMetrics HIPAA Fulfillment Manager | HCISPP
LOGGING AND LOG MANAGEMENT

HIPAA REQUIREMENTS FOR LOGGING

Event, audit, and access logging is a requirement for HIPAA compliance. HIPAA requires you to keep logs of each of your systems for a total of six years. These three HIPAA requirements apply to logging and log monitoring:


- **Section 164.312(b):** Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

- **Section 164.308(a)(1)(ii)(D):** Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

ORGANIZATIONS STORE LOGS

We interviewed 52 healthcare professionals (who were responsible for HIPAA compliance) about logging and reviewing logs. Throughout this section, you’ll find results from this survey, such as the following graph:

ORGANIZATIONS STORE FIREWALL LOGS

HIPAA requires that organizations enable logging and log alerting on critical systems (e.g., unauthorized connection attempt).
IMPLEMENT LOGGING AND ALERTING

System event logs are recorded tidbits of information regarding the actions taken on computer systems like firewalls, operating systems, office computers, electronic health record (EHR) systems, printers, etc.

LOGS ARE ONLY USEFUL IF THEY ARE REGULARLY REVIEWED.

Log monitoring systems oversee network activity, inspect system events, alert of suspicious activity, and store user actions that occur inside your systems. They are like a watchtower lookout alerting you to future risks, providing data that informs you of a data breach. The raw log files are also known as audit records, audit trails, or event logs.

Most systems and software generate logs including operating systems, Internet browsers, workstations, anti-malware, firewalls, and IDS. Some systems with logging capabilities do not automatically enable logging, so it’s important to ensure all systems have logs turned on. Some systems generate logs, but don’t provide event log management. Be aware of your system capabilities and potentially install third-party log monitoring and management software.
ESTABLISHING LOG MANAGEMENT

Businesses should review their logs daily to search for errors, anomalies, or suspicious activity that deviate from the norm.

From a security perspective, the purpose of a log alert is to act as a red flag when something bad is happening. Reviewing logs regularly helps identify malicious attacks on your system. Given the large amount of log data generated by systems, it’s impractical to manually review all logs each day. Log monitoring software takes care of that task by using rules to automate log review and only alert on events that might reveal problems. Often this is done using real-time reporting software that alerts you via email or text when suspicious actions are detected.

Often, log monitoring software comes with default alerting templates to optimize monitoring and alerting functions immediately. However, not everyone’s network and system designs are exactly the same, and it’s critical to take time to correctly configure your alerting rules at the beginning.

SOMEONE IS ASSIGNED TO REVIEW LOGS DAILY

![Circle chart showing the distribution of responses to the question of whether someone is assigned to review logs daily. 44% say yes, 32% say no, and 24% do not know.]

A security professional or third party should review firewall logs daily.
LOG MANAGEMENT SYSTEM RULES

Here are some event actions to consider when setting up your log management system rules:

- Password changes
- Unauthorized logins
- Login failures
- New login events
- Malware detection
- Malware attacks seen by IDS
- Scans on your firewall’s open and closed ports
- Denial of service attacks
- Errors on network devices
- File name changes
- File integrity changes
- Data exported
- New processes started or running processes stopped
- Shared access events
- Disconnected events
- New service installation
- File auditing
- New user accounts
- Modified registry values
To take advantage of log management, look at your security strategy and make sure these steps are taken care of:

• Decide how and when to generate logs.
• Secure your stored logs so they aren’t maliciously altered by cybercriminals or accidentally altered by well-intentioned employees.
• Assign an employee you trust to review logs daily.
• Set up a team to review suspicious alerts.
• Spend time to create rules for alert generation (don’t just rely on a template).
• Store logs for at least one year (or as long as legally required), with at least three months readily available.
• Frequently check log collection to identify necessary adjustments.

Regular log monitoring means a quicker response time to security events and better security program effectiveness. Not only will log analysis and daily monitoring demonstrate your willingness to comply with HIPAA requirements, it will also help you defend against insider and outsider threats.

Organizations should review their logs daily to search for errors, anomalies, or suspicious activity that deviates from the norm.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

AUDIT LOGS AND LOG MONITORING
Given the large amount of log data generated by systems, it’s virtually impossible to manually analyze logs beyond one or two systems, especially reviewing logs all day. Log monitoring software takes care of that task by using rules to automate log review and only alert on events that might reveal problems.

You likely need Security Information and Event Management (SIEM) tools to sift through logs and dig down into problems. In the past, SIEM systems were only utilized in enterprise organizations, but now, smaller organizations are beginning to realize system monitoring can help identify attacks.

Organizations often struggle with good log review processes. Using SIEM tools can enable you to have real-time alerting to help you recognize current attacks. If you really do have a problem, you can then initiate your incident response plan (IRP).

Also, remember that in order to correlate events over multiple systems, you must synchronize system times. All systems should get their system times from one or two internal timeservers, which in turn receive time from a trusted external source.

RYAN MARSHALL
SecurityMetrics HIPAA Fulfillment Manager | HCISPP
VULNERABILITY SCANNING

PROTECT YOUR NETWORK FROM ATTACKERS
Not only should you use security tools to monitor your systems in real time (e.g., logging), you need to know your network environment and find out weaknesses through tools like vulnerability scans. Vulnerability scans assess computers, systems, and networks for security weaknesses, also known as vulnerabilities. These scans are typically automated and give a beginning look at what could possibly be exploited. Vulnerability scans can be instigated manually or on an automated basis, and will complete in as little as several minutes to as long as several hours.

Vulnerability scans are a passive approach to vulnerability management because they don’t go beyond reporting on vulnerabilities that are detected. It’s up to the organization’s risk or IT staff to patch discovered weaknesses on a prioritized basis or confirm that a discovered vulnerability is a false positive (looks like a vulnerability but isn’t applicable to your environment), then rerun the scan until it passes.

Although HIPAA does not specifically state the necessity of vulnerability scans, this data security best practice is considered by almost every security expert as one of the best ways to find potential vulnerabilities.

SECURITY TIPS
Because cybercriminals discover new ways to hack businesses daily, organizations are encouraged to regularly scan their systems. External vulnerability scans should be ongoing or at least completed quarterly to help locate vulnerabilities. You should also ensure an external vulnerability scan occurs when your system is changed or updated in any way.

After scan completion, a report will typically generate an extensive list of vulnerabilities found and references for further research on the vulnerability. Some even offer directions on how to fix the problem. Remember that the vulnerability scan does not change your system or fix problems, so make sure that you fix any required changes needed for your system.

The report reveals any identified weaknesses, but sometimes includes false positives. Sifting through real vulnerabilities and false positives can be a chore, but it’s important to manually check each vulnerability to make sure you’re not at risk.

Vulnerability scanning isn’t just about locating and reporting vulnerabilities. It’s also about establishing a repeatable and reliable process for fixing problems, based on risk and effort required. Failing scan results that aren’t remediated renders security precautions worthless.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

VULNERABILITY SCANS – MORE BANG FOR THE BUCK

Vulnerability scans can and should be run frequently (monthly or quarterly). These passive scans run against and analyze all your internal and external ports for exploitable vulnerabilities.

Attackers constantly scan your systems looking for new vulnerabilities, so you should do the same on all of your own systems. Any issues found should be remediated immediately and rescanned as quickly as possible.

Based on what I see when I meet with entities, a high percentage of breaches could have been prevented through regular scanning and remediation.

MATT GLADE
SecurityMetrics | CISSP | QSA
THE BASICS OF PENETRATION TESTING
In addition to performing vulnerability scans, you should perform penetration testing to help prevent attacks. Penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would. In simple terms, analysts attempt to break into your company’s network to find security holes.

Specifically, penetration testers will first run automated scans and then manually test your website, patient portal, or other Internet-facing networks and applications to see if there is a way into your patient data using common hacker tools. If found, the testers report these vulnerabilities to you with recommendations on how to better defend the systems.

Penetration testing is particularly helpful for organizations developing their own applications, as it’s important to have code and system functions tested by an objective third party. This helps find vulnerabilities missed by developers.

Depending on your security needs, you may need to do both an internal and external penetration test. An internal penetration test is when penetration testers test systems (without PHI access) within your organizational network (i.e., perspective of someone inside your network). An external penetration test is when penetration testers test from a perspective of an open public network (Internet) outside of your organizational network (i.e., perspective of a hacker over the Internet).

A PENETRATION TEST IS AN EXHAUSTIVE, LIVE EXAMINATION DESIGNED TO EXPLOIT WEAKNESSES IN YOUR SYSTEM.

Typically, penetration test reports contain a long, detailed description of attacks used, testing methodologies, and suggestions for remediation. Make sure to take adequate time to address the penetration test report’s advice and fix the located vulnerabilities on a prioritized basis.
DIFFERENCES BETWEEN VULNERABILITY SCANNING VS. PENETRATION TESTING

Some mistakenly believe vulnerability scanning or antivirus scans are the same as a professional penetration test.

Here are the two biggest differences.

1. A vulnerability scan is automated, while a penetration test includes a live person actually digging into the complexities of your network.
2. A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify, then attempt to exploit vulnerabilities to get access to secure systems or stored sensitive data.

Vulnerability scans are great weekly, monthly, or quarterly insight into your network security, while penetration tests are a more thorough way to deeply examine network security.

PREPARING FOR YOUR PENETRATION TEST

DECIDE WHO’S PERFORMING YOUR PENETRATION TEST

You need to decide who is performing your penetration test (e.g. in-house or third party).

Penetration testers should be well versed in:
- Black hat attack methodologies (e.g., remote access attacks, SQL injection)
- Internal and external testing (i.e., perspective of someone within the network, perspective of hacker over Internet)
- Web front-end technologies (e.g., Javascript, HTML)
- Web application programming languages (e.g., Python, PHP)
- Web APIs (e.g., restful, SOAP)
- Network technologies (e.g., firewalls, IDS)
- Networking protocols (e.g., TCP/UDP, SSL)
- Operating systems (e.g., Linux, Windows)
- Scripting languages (e.g., Python, Pearl)
- Testing tools (e.g., Nessus, Metasploit)
- Segmentation testing
If you use an in-house penetration tester, they must use correct penetration testing methodologies when conducting your test (e.g., NIST 800-115, OWASP Testing Guide, etc.). They also need to be aware of general vulnerabilities and threats prevalent in the industry and design tests to check for issues in your networks and applications.

If you hire a third party, make sure the penetration tester you select uses the correct methodology and that you act on the report they give you (i.e., fix the problems they find). Then collect information for your penetration tester such as: have you experienced a vulnerability in past 12 months (e.g., Ransomware)? Did you make changes? Tell your penetration tester about all this information so they can design tests to validate your changes.

**HOW OFTEN SHOULD YOU GET A PENETRATION TEST?**

First, establish what your organization considers a major change. What might be a major change to a smaller organization is only a minor change in a large environment. For any organization size, if you bring in new hardware or start accepting patient data in a different way, that constitutes a major change.

Whenever large infrastructure changes occur, you’ll want to perform a formal penetration test to see if that change added any new vulnerabilities, in addition to annual penetration tests.

During your Risk Analysis process, you may have discovered that you need more frequent and/or specific penetration tests (e.g., web application testing, segmentation checks).

**PERFORM A PENETRATION TEST AT LEAST YEARLY AND AFTER MAJOR NETWORK CHANGES.**
COST OF PENETRATION TESTING

With any security service, cost may vary widely based on several variables, such as:

- **Complexity**: the size and complexity of your environment and network devices are probably the biggest factors of your penetration test quote. A more complex environment requires more labor to virtually walk through the network and exposed web applications looking for every possible vulnerability.

- **Methodology**: each penetration tester has a different way they conduct their penetration test. Some use more expensive tools than others, which could raise the price. That’s not necessarily a bad thing. More expensive tools could reduce the time of your test, and produce higher quality results.

- **Experience**: penetration testers with more experience will be more expensive. Just remember, you get what you pay for. Beware of penetration testers that offer prices that are too good to be true. They probably aren’t doing a thorough job. Look for penetration testers with credentials behind their name like CISSP, GIAC, CEH, and/or OSCP.

- **Onsite**: most penetration tests can be done offsite; however, in rare cases that involve very large/complex environments, an onsite visit could be required to adequately test your business security. Onsite visits are also required if you request a physical security or social engineering penetration test.

- **Remediation**: some penetration testers include remediation assistance and/or retesting in their price. Others provide test results and disappear.

With everything above accounted for, typically penetration tests start around $4,000 but can rise well above $20,000.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

PENETRATION TESTING BEST PRACTICES

Even though organizations may understand the necessity for an annual penetration test, organizations often claim no significant infrastructure changes have been made because the cost or time of a full-blown penetration test seems overwhelming.

My advice is this: first establish what your organization considers a major change. What might be a major change to a smaller organization is only a minor change in a large environment. For either size organization, if you bring in new hardware or start accepting patient data in a different way, that constitutes a major change.

The next step is to establish an assessment policy. Some organizations designate a department separate from the infrastructure team to conduct self-assessments. Others hire penetration testers to conduct the assessments.

BRAND BARNEY

SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
HIPAA BREACH NOTIFICATION RULE
BREACH NOTIFICATION RULE INTRODUCTION

Even organizations with the strictest data security and IT policies could easily go the way of recent victims like Anthem, Premera Blue Cross, and TRICARE without proper care and upkeep to their data security programs. Last year, medical and healthcare entities accounted for 35.5% of reported data breaches.

The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured patient data.

If you’re a covered entity, your statements must be sent to affected patients by first-class mail and/or email in less than 60 days after the breach. If 10 or more individuals’ information is out-of-date or insufficient (or the breach affects more than 500 residents of a state or jurisdiction), post the statement on your website for at least 90 days and/or provide notice in major print or broadcast media in the affected area.

Covered entities also need to notify the Secretary of the HHS about the breach. If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. If a breach affects 500 or more individuals, covered entities must notify the Secretary of the HHS within 60 days following a breach (if not immediately).

If you’re a business associate, notify affected covered entities after discovering the data breach immediately (and no later than 60 days after discovering the breach). Identify each individual affected by the breach and send this information to all affected covered entities.

A LITTLE KNOWN FACT: COVERED ENTITIES ARE JUST AS LIABLE IF THEIR BUSINESS ASSOCIATE IS FOUND TO BE IN BREACH OF HIPAA REQUIREMENTS
HOW TO MANAGE A HEALTHCARE DATA BREACH

Now that you know what you’re required to do, you need to know security best practices. The following steps will help you successfully stop information from being stolen, mitigate further damage, and restore operations as quickly as possible.

START YOUR INCIDENT RESPONSE PLAN

If you suspect a data breach, here’s your objective: stop information from being stolen and repair your systems so a breach won’t happen again. This begins by executing your incident response plan (IRP).

The HHS states that an “impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the protected health information or to whom the disclosure was made
- Whether the protected health information was actually acquired or viewed
- The extent to which the risk to the protected health information has been mitigated.”

A well-executed incident response plan can minimize breach impact, reduce fines, decrease negative press, and help you get back to business more quickly. In an ideal world, you should already have an incident response plan prepared and employees trained to quickly deal with a data breach situation.

For some reason, however, most breached organizations SecurityMetrics has investigated didn’t have an incident response plan at the time of the incursion.

With no plan, employees scramble to figure out what they’re supposed to do, and that’s when big mistakes are made. (e.g., wiping a system without first creating images of the compromised systems to learn what occurred and to avoid re-infection).

SET YOUR INCIDENT RESPONSE PLAN INTO MOTION IMMEDIATELY ON LEARNING OF A SUSPECTED DATA BREACH.
PRESERVE EVIDENCE

When a healthcare organization becomes aware of a possible breach, it’s understandable to want to fix it immediately. However, without taking the proper steps and involving the right people, you could inadvertently destroy valuable forensic data. Investigators use this information to determine how and when the breach occurred, and what to recommend in order to properly secure the network against the current attack or similar future attacks.

When you discover a breach, remember:

• Don’t panic
• Don’t make hasty actions
• Don’t wipe and re-install your systems (yet)
• Do follow your incident response plan

CONTAIN THE BREACH

Your first priority at this point in time is to isolate the affected system(s) to prevent further damage until your forensic investigator can walk you through the more complex and long-term containment. Implement the following 10 steps to contain a data breach:

1. Disconnect from the Internet by pulling the network cable from the firewall/router to stop the bleeding of data. If a mobile device (e.g., laptops, external hard drives, flash drives, and/or mobile devices) is stolen or lost, remote wipe devices once you find out about the loss.

2. Document the entire incident. This documentation should include the following information:

   • How you learned of the suspected breach
   • The date and time you were notified, how you were notified
   • What you were told in the notification
   • All actions you take between now and the end of the incident
   • The date and time you disconnected systems in the PHI environment from the Internet
   • If and when you disabled remote access
   • If and when you changed credentials/passwords
   • All other system hardening or remediation steps taken
3. Disable (do not delete) remote access capability and wireless access points. Change all account passwords and disable (not delete) non-critical accounts. Document old passwords for later analysis.

4. Change access control credentials (usernames and passwords) and implement highly complex passwords: 10+ characters that include upper and lower case, numbers, and special characters. (Avoid passwords that can be found in any dictionary, even if you are substituting special characters in place of letter characters.)

5. Segregate all hardware devices in the electronic medical record (EMR) from other critical devices. Relocate these devices to a separate network subnet and keep them powered on to preserve volatile data.

6. Quarantine instead of deleting (removing) identified malware found by your antivirus scanner for later analysis and evidence.

7. Preserve firewall settings, firewall logs, system logs, and security logs (take screenshots if necessary).

8. Restrict Internet traffic to only critical servers and ports outside of the EMR. If you must reconnect to the Internet before an investigator arrives, remove your EMR from any devices that must have Internet connectivity until you consult with your forensic investigator.

9. Contact the HHS within appropriate and required time-frames (if you haven’t already) and let them know what happened.

10. Consider hiring a law firm experienced in managing data breaches. It won’t be cheap, but they may help you avoid pitfalls that could damage your organization’s reputation. Your law firm may hire a forensic firm to immediately investigate and ensure you’ve properly contained the breach.
START INCIDENT RESPONSE MANAGEMENT

ASSEMBLE YOUR INCIDENT RESPONSE TEAM

A data breach is a crisis that must be managed through teamwork. Assemble your incident response team immediately. (Hopefully you’ve already met and discussed roles during crisis practices and initiated your incident response plan.)

Your team should include a team leader, lead investigator, communications leader, C-suite representative, office administrator, human resources, IT, attorney, public relations, breach response experts, and a business associate representative (if applicable). Each brings a unique side to the table with a specific responsibility to manage the crisis. In smaller organizations, some people might fulfill multiple roles.

BREACH NOTIFICATION RULE

Remember, if you’re a covered entity, your statements must be sent to affected patients by first-class mail and/or email in less than 60 days after the breach. If 10 or more individuals’ information is out-of-date or insufficient (or the breach affects more than 500 residents of a state or jurisdiction), post the statement on your website for at least 90 days and/or provide notice in major print or broadcast media in the affected area.

Covered entities also need to notify the Secretary of the HHS about the breach. If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. If a breach affects 500 or more individuals, covered entities must notify the Secretary of the HHS within 60 days following a breach (if not immediately).

If you’re a business associate, notify affected covered entities after discovering the data breach immediately (and no later than 60 days after discovering the breach). Identify each individual affected by the breach, as well as any information necessary for statements. Send this information to affected covered entities.
CONSIDER PUBLIC COMMUNICATIONS
Proper communication is critical to successfully managing a data breach, and a key function of the incident response team is to determine how and when notifications will be made.

Identify in advance the person within your organization (perhaps your inside legal counsel, newly hired breach management firm, C-level executive, etc.) who is responsible for ensuring the notifications are made timely. Your public response to the data breach will be judged heavily, so think this through.

STALLING MAY NOT BE IN YOUR BEST INTEREST
Your patients will discover if you keep important breach information from them. If the media marks your organization untrustworthy for withholding information, that label could end up hurting you worse than the other effects of the data breach. Some organizations fall into the, “Let’s make sure we know exactly what’s going on before we say anything at all” trap, but excessive delays in releasing a statement may be seen as an attempted cover-up.

Providing some information is usually better than saying nothing at all. You can always provide updated statements as needed on your website. In all cases regarding public statements, seek the guidance of your legal counsel.

MAKE SURE EMPLOYEES DON’T ANNOUNCE THE BREACH BEFORE YOU DO
Poorly informed employees can often circulate rumors—true or not. As a team, establish your media policy that governs who is allowed to speak to the media. Designate a spokesperson and ensure employees understand they are not authorized to speak about the breach.

Depending on your particular circumstances, you may find it beneficial to withhold from the rank and file employees the fact that your company has suffered a data breach until shortly before any public statements are made.

DISCLOSURES OF THE BREACH BOTH WITHIN THE COMPANY AND TO THE PUBLIC SHOULD BE IN ACCORDANCE WITH ADVICE FROM YOUR LEGAL COUNSEL.
GET YOUR STATEMENTS TOGETHER
Your incident response team should craft specific statements that target the various audiences, including a holding statement, a press release, a patient statement, and an internal/employee statement. These should be communicated to appropriate parties that could potentially be affected by the breach, such as business associates, third-party contractors, stockholders, law enforcement, and ultimately patients.

Your statements should nip issues in the bud by addressing questions like:
- Which locations are affected by the breach?
- How was it discovered?
- What personal data is at risk?
- How will it affect patients and the community?
- What services or assistance (if any) will you provide your patients?
- When will you be back up and running, and what will you do to prevent this from happening again?

Explain that you are committed to solving the issue and protecting your patient’s information and interests. Where you deem appropriate, you could offer an official apology and perhaps other forms of assistance such as ID theft monitoring.

INVESTIGATE AND FIX YOUR SYSTEMS
Now comes the hardest part: investigating and fixing everything. Luckily, you’re not alone. If you hire a forensic investigator, they will perform the majority of the investigation and then provide recommendations on how to repair your environment to ensure this doesn’t happen again.

BRING AFFECTED SYSTEMS BACK ONLINE
After the cause of the breach has been identified and eradicated, you need to ensure all systems have been hardened, patched, replaced, and tested before you consider re-introducing the previously compromised systems back into your PHI environment. During this process, ask yourself these questions:
- Have you properly implemented all of the recommended changes?
- Have all systems been patched, hardened, and tested?
- What tools/reparations will ensure you’re secure from a similar attack?
- How will you prevent this from happening again? (Who will respond to security notifications and be responsible to monitor security, Intrusion Detection System, and firewall logs?)
BE PREPARED FOR COSTS

Data breaches have serious financial consequences. Obviously, the financial examples presented below will change based on your size, how much patient data was stolen, how hackers got into your organization, if you were willfully aware of your vulnerabilities, etc.

If breached, you may only be liable for a few of these fines, or you could be expected to pay even more than listed below. Depending on the size of your breach, you may have to pay the following:

### HIPAA BREACH FINES

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>HHS fines</td>
<td>Up to $1.5 million/violation/year</td>
</tr>
<tr>
<td>Federal Trade Commission fines</td>
<td>$16,000/violation</td>
</tr>
<tr>
<td>State attorney generals</td>
<td>$150,000 – $7 million</td>
</tr>
<tr>
<td>Business associate changes</td>
<td>$5,000+</td>
</tr>
<tr>
<td>Lawyer fees</td>
<td>$5,000+</td>
</tr>
<tr>
<td>Technology repairs</td>
<td>$2,000+</td>
</tr>
<tr>
<td>Class action lawsuits</td>
<td>$1,000/record</td>
</tr>
<tr>
<td>Breach notification costs</td>
<td>$1,000+</td>
</tr>
<tr>
<td>On-going credit monitoring for affected patients</td>
<td>$10-$30/record</td>
</tr>
<tr>
<td>ID theft monitoring</td>
<td>$10-$30/record</td>
</tr>
<tr>
<td>Patient Loss</td>
<td>40%</td>
</tr>
</tbody>
</table>

**TOTAL POSSIBLE COST** $180,000-$8.3 MILLION+

MAKE SURE IT DOESN'T HAPPEN AGAIN

A key part of a successful breach response is what you learned from the breach. After the dust has settled, assemble your incident response team once again to review the events in preparation for a potential attack. Incorporate the lessons you’ve learned and ask, “How can we improve the process next time?” And then revise your incident response plan. Don’t forget to communicate your commitment to data security to the media, even after you’ve repaired the damage.
INSTALL AND MONITOR FILE INTEGRITY MONITORING SOFTWARE
If you haven’t already, install file integrity monitoring software (FIM) on all critical systems because it’ll alert you when changes to important files have been made.

For example, you can see that yesterday at 3AM a file was added to an obscure file when no one was updating your system. Chances are, it’s malware that was added when you visited an infected website and it wasn’t detected by anti-malware. After doing a little searching following discovery, it’s much easier to remove that piece of malware off your system.

You should regularly review (at least daily) and monitor logs generated by your FIM software. Set up logs that alert system administrators in an event of suspicious activity. If a system detects suspicious activity, such as when a new software program is installed in an odd location, or if someone attempts to log in 300 times in a row, log alerting can tip off the internal IT team to begin an investigation.

INSTALL INTRUSION DETECTION SYSTEMS
One of the reasons healthcare data breaches are so prevalent is from a lack of proactive, comprehensive security systems dedicated to monitoring system irregularities, such as intrusion detection systems (IDS), host intrusion detection systems (HIDS), network intrusion detection systems (NIDS), etc.

Using this software can help identify a suspected attack and help you locate security holes in your network that gave the attackers access in the first place. Without the knowledge derived from IDS logs, it can be very difficult to find system vulnerabilities, or determine if patient health data was accessed/stolen.

Intrusion detection systems should be implemented in every single hospital, doctor’s office, clearinghouse, or any other location sensitive data is received, transmitted or even stored.

By setting up alerts on an IDS, you can be alerted as soon as suspicious activity occurs and be able to significantly mitigate compromise risk within your organization, and you may even stop a breach in its tracks.
From a legal standpoint, a healthcare organization could also use the information stored by their IDS in a breach court case to show they did as much as possible to contain the breach.

Additionally, forensic investigators, like SecurityMetrics forensic investigators, use information gleaned from client IDS tools to investigate breaches, such as how the hacker got in, how long they remained in the system, and when they exported data. This helps determine exactly how much patient data was exported, and what the organization must do to secure system vulnerabilities.

Keep in mind that an IDS isn’t preventive. Similar to private investigator, an IDS doesn’t interfere with what it observes. It simply follows the action, takes pictures, records conversations, and alerts the client. For more preventative measures you might consider an Intrusion Prevention System (IPS), which is an extension of IDS and is usually paired together. However unlike IDS, it will prevent and block many intrusions that are detected.

AN IDS COULD HELP YOU DETECT A SECURITY BREACH AS IT’S HAPPENING IN REAL TIME.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

SETTING UP YOUR INTRUSION DETECTION SYSTEM

Here are the steps you should follow to correctly use an IDS:

• **First, purchase an IDS.** There are a variety of different tools on the market and each tool will need to be carefully reviewed before a decision is made. I often ask my clients do they want a NIDS or HIDS (Network or Host based). I advise that a combination of both should be used for any organization looking to take their security seriously. When choosing your IDS/IPS it’s best to get help from a security consultant and make sure that your security team is always involved.

• **Install it on the outside of your network to detect external attacks.** Don’t just integrate your IDS to secure your EHR. Using pivot attacks, hackers can hack into unrelated or unprotected areas of your network and easily hop onto more secured areas of your network (like your EHR) from there.

• **Don't forget about internal attacks.** Whether the threat is a fired workforce member who wants to get back at the organization, or an attacker who plugs a malware-filled USB into an exam room computer after nonchalantly walking in the office, an internal IDS should be configured to detect internal activities to prevent an attack from the inside.

• **Configure alerts.** Configure the intrusion detection system to alert you as soon as suspicious activity occurs. Discuss what alerts should be configured with your security advisor, internal team, and vendor.

• **Form a task force.** You need a team to manage this important part of your security strategy. Whether it’s the responsibility of your data loss prevention team, IT team, or a mash up of security-related department heads, a group must be formed to take charge. Their activities could include identification of suspicious activity alerts, ensuring regular scheduled IDS updates, incident response planning, and/or alert monitoring.

• **Constant alert monitoring.** Many hospital IT departments may already have a network intrusion detection system in place, but aren’t regularly checking it. This is mistake #1, and can cost you a swift breach recovery. If you don’t check your IDS, or alerts aren’t being sent to you, you might as well not have it.

• **Have an action plan.** What happens when your IDS actually identifies an attack? You may also have an intrusion prevention system in place that may or may not be active and preventing illicit traffic. If not, your task force must form an action plan, and follow your tested and approved incident response plan (e.g., how to identify the threat, which appropriate persons to notify, how to contain the threat, etc.).

MATT GLADE
SecurityMetrics | CISSP | QSA
HIPAA PRIVACY RULE
PRIVACY RULE INTRODUCTION

The Privacy Rule addresses appropriate PHI use and disclosure practices for healthcare organizations, as well as defines the right for individuals to understand and regulate how their medical information is used.

The HIPAA Privacy Rule:

• Spells out administrative responsibilities
• Discusses written agreements between covered entities and business associates
• Discusses the need and implementation for privacy policies and procedures
• Describes employer responsibilities to train workforce members and implement requirements regarding their use and disclosure of PHI

Healthcare is often exceptional at following most of the Privacy Rule. Your privacy practices are likely posted throughout your workplace; however, there are still some instances where employees leak PHI to the public (such as 2015’s case of football star Jason Pierre-Paul), but these cases are more rare than common.

Make sure to train your employees at least quarterly. You might consider breaking training into sections and hold them quarterly, making it easier to remember and implement procedures. Your workforce is also more likely to be up to date on all rules and regulations.

Training doesn’t have to be lengthy and detailed (e.g., a 20 minute PPT presentation). Instead, keep it simple and fun. Make sure that employees know their goal is to protect patient.
MINIMUM NECESSARY

A large portion of the Privacy Rule is based on the **minimum necessary requirement**, which states that only those who need to see PHI to do their jobs should get to see it, and unless you have a specific need for the information, access must be restricted. For example, a receptionist (or someone that doesn’t provide direct patient care) probably doesn’t need to see the X-rays of a patient to do his or her job.

LIMIT ACCESS TO PHI

The HHS states “if a hospital employee is allowed to have routine, unimpeded access to patients’ medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard.”

It’s a covered entity’s responsibility to limit who within the organization has access to each specific part or component of PHI. The easiest way to take charge of the data is by creating individual user accounts on a network. In the ideal scenario, each user account in a network, EHR, or computer system, would be given certain privileges based on the job title or role of the user.

For example, a doctor’s privilege would get access to all PHI in their patient database because they need it to do their job, while an IT admin would have restricted access to PHI because they’re not involved with patient care.
The minimum necessary also applies to the information shared externally with third parties and subcontractors. Organizations are required to limit how much PHI is disclosed based on job responsibilities and nature of the third party’s business. Remember passing too much PHI to a business associate or third party could get your organization slapped with a fine. Be careful about how much data you send and receive.

However, both covered entities and business associates have a minimum necessary responsibility under HIPAA. That means either party can be fined by the HHS for misapplying (or completely disregarding) the minimum necessary rule. For example, if a business associate demands more data than is necessary from its covered entities, they could be fined for ignoring the rules.

To avoid these issues, covered entities and business associates should assess their responsibilities concerning minimum necessary data accordingly:

- **Covered entity responsibility**: determine what data is the minimum necessary to send, and then only send that data and nothing else.
- **Business associate responsibility**: only accept and use the minimum necessary data.

**BY LIMITING PHI ACCESS TO THE SMALLEST NUMBER OF PEOPLE POSSIBLE, THE LIKELIHOOD OF A BREACH OR HIPAA VIOLATION DECREASES SIGNIFICANTLY.**
HEALTHCARE SECURITY
SPECIALIST’S PERSPECTIVE

MINIMUM NECESSARY BASICS
Minimum necessary is a core principle of the Privacy Rule, and it affects a large amount of decisions surrounding the privacy and security of PHI.

The goal of this requirement is to limit the amount of PHI that an organization uses, discloses or requests to the minimum necessary to accomplish the intended purpose. You can extend this philosophy to how much and what types of PHI an organization creates as well. Every time you grant employee access to PHI or receive a request to send PHI to another organization or individual, ask yourself what is the minimum amount of information required to accomplish the requested task.

Yes, it's difficult, but you need to find balance when applying Minimum Necessary. That is between maintaining patient health and safety along with respecting their individual rights vs protecting their privacy.

There are several exceptions to Minimum Necessary: disclosures from one healthcare provider to another for purposes of treatment, patient and any authorized party requests, and uses and disclosures to the HHS Secretary and for any legal purposes.

RYAN MARSHALL
SecurityMetrics HIPAA Fulfillment Manager | HCISPP
NOTICE OF PRIVACY PRACTICES

Most healthcare professionals are familiar with Notices of Privacy Practices (NPPs) as being part of HIPAA. Most patients have seen them, and most Covered Entities have them in place and know what they are for. But the most common errors in NPPs are updating how the organization deals with a refusal to acknowledge receipt of privacy practices by a patient and making sure all foreign language versions (e.g., Spanish NPPs) are up to date.

NPPs are legal documents and are commonly created by groups other than the Entities themselves. They are usually provided to them by insurance companies or malpractice attorneys or sometimes a healthcare association. While there is nothing wrong with having NPPs supplied by external parties, they do need to accurately reflect your privacy practices and need to be updated when changes to the law occur.

An example would be the change to requirements for uses of PHI for marketing purposes that the Omnibus Rule introduced in 2013. Some NPPs created before 2013 had marketing disclosure practices that would now be a violation of the new requirements.

All NPPs need to be displayed in a prominent location at your organization where a patient would encounter them. If you own a website, it must be published there as well. NPPs must be provided to the patient at first encounter and an attempt to have the patient sign an acknowledgement of receipt form must be made.

A patient is not required to sign the acknowledgment form and cannot be denied any service as a result of refusal to sign. When a patient refuses to sign, documentation should show that an attempt was made and the reason it was not accepted.

NPPs must contain how your organization intends to use and disclose PHI, what the individual’s rights with respect to information, and how the individual can exercise them, including how to file a complaint. NPPs should include what your legal duties are with respect to this information including a statement that they are legally required to protect the privacy of the information. NPPs also must contain contact information for your policies.
BUSINESS ASSOCIATE CONCERNS

After the 2013 HIPAA Final Omnibus Rule, HIPAA compliance for both covered entities and business associates has become an even more important compliance best practice. The HIPAA Final Omnibus Rule requires covered entities to implement or update a business associate agreement (BAA) for all relationships wherein the business associate creates, receives, maintains, or transmits electronic patient information.

In these new or revised BAAs, covered entities, business associates, and subcontractors agree to share responsibility for patient data protection and breach notification.

The HHS makes it clear that covered entities must 'obtain satisfactory assurance' that each BA safeguards the patient data it receives or creates on behalf of the covered entity. That means covered entities must assist their BA in achieving HIPAA compliance.

Whether compromised from within your system or the system of a BA, your organization can be liable for up to $50,000 per violation per day as a result of any breach of your patient data. And that’s just HHS penalties. That doesn’t include civil action, cost of mitigation, and loss of patient trust that may come as a result of breach.

With these consequences in mind, remember that you should only share minimal need-to-know data with your business associates, and regularly validate that they are handling your patient’s PHI in a HIPAA compliant manner. That should keep your liability to a minimum. Next, covered entities should do all they can to reduce risks by implementing a BA compliance program. Such a program should gauge your liability, help you locate BAs, discover what BAs do with your PHI, and help them work towards compliance.

CREATE YOUR BA COMPLIANCE PROGRAM

Your business associate plan should evaluate all existing BA security practices in order to help you address the riskiest vendors first. Then, risk and compliance managers should design, implement, and monitor a mass risk evaluation of business associate networks.

A plan that starts with the highest risk BAs and tracks related progress will help you prove your effort to address BA compliance if the HHS decides to audit your organization.
The first step in your action plan should identify all parties (BAs and subcontractors) that must become HIPAA compliant. Next, ask your BAs for proof they’ve completed a risk analysis and are up to date with their risk management plan. If not, either recommend a trusted source to help or stop using their services. Just remember patient data is too valuable to do business with BAs that choose to ignore compliance best practices.

Next, classify business associates according to their use of patient data. Determine how much liability each BA holds by asking a set of risk-evaluating questions such as:

- Is the BA internal system connected to the Internet? If yes, are those external IPs scanned for vulnerabilities?
- How does the BA obtain protected PHI from you and what data is received?
- What is the quantity of the data received?
- How is the data stored, protected, backed up and destroyed by the BA?

After this quick risk snapshot, you will clearly be able to categorize individual risk levels that determine which BAs put your patient data in the highest risk. Based on the risk ranking from the preliminary risk analysis, you can then start to customize compliance measures to enable BA HIPAA compliance.

REMEMBER THAT HIPAA REGULATIONS REQUIRE YOU TO TAKE ACTION IF YOU KNOW OR BELIEVE A BUSINESS ASSOCIATE IS NOT HIPAA COMPLIANT.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

MONITOR YOUR BUSINESS ASSOCIATES’ COMPLIANCE

Every covered entity with business associates is required to obtain assurances that their BAs treat patient data the way the HHS wants them to, and the way you want them to. Whether you choose to personally audit each BA, or require documented data security procedures, take the initiative to secure the future of your organization and safety of patient data.

As your business associates progress towards compliance, track their success to ensure an approved level of compliance. As the riskiest BAs reach compliance, begin to reach out toward medium-risk BAs to start the process with them. Don’t forget to reevaluate every BA’s plan and associated vulnerabilities each year. Encourage continual education and training programs such as regular HIPAA security webinars or even an email newsletter.

BRAND BARNEY

SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
HIPAA DOCUMENTATION

A large part of your HIPAA compliance process should be spent on documentation.

When a healthcare organization doesn’t have documentation, their HIPAA compliance program is effectively directionless. Without a recorded comparison of last year’s security plan, this year’s efforts are pointless. If done correctly, documentation creates a baseline security standard for every process, workforce member, and system at your organization.

Here are three reasons that proper documentation is crucial to reach HIPAA compliance:

1. **Your future:** If you document your hard work this year, you’re making next year’s job that much easier. You’re going to save time and money, which means less overall stress for you and your team. Updating already existing documentation is much easier than starting from scratch.

2. **Your legacy:** If you move on to bigger and better career opportunities, documentation will give your successor a great view into the environment.

3. **The HHS:** If the HHS comes knocking, proper documentation will show your compliance efforts. If you can prove how you’re working toward full HIPAA compliance in your documentation, they will likely be more lenient. Remember to make sure you’re actually implementing the policies you’re documenting. If you haven’t implemented anything in your documentation, this is a major detriment to you, your PHI, and your organization.
How to Meet HIPAA Documentation Requirements

Many organizations are confused on what exactly they should be documenting and how they should be documenting it. Generally speaking, you should record the who, what, when, where, how, and why of everything relating to PHI in your environment. It should demonstrate in writing where you are today, where you've progressed over the years, and what your plan is for the future.

Your documentation should answer questions, such as:
- What is your security stance in general?
- What are your risks and vulnerabilities?
- How secure are your workstations?
- Do your workforce members understand how to safeguard PHI?
- What is the state of your location's physical security?
- How does BYOD factor into your security strategy?
- What have you learned during your HIPAA compliance process?
- Who are the responsible parties?
- How are systems configured?
- What is your authorization and approval processes?

To answer those broad questions, dive into the detailed answers of more specific and/or technical questions, such as:
- Who holds your encryption keys, and how do you secure them? Where are they stored? What are those key holder’s responsibilities and role-based access level?
- Who has access to your firewalls? How are those firewalls configured? Which systems do those firewalls surround? Are they up to date? Do you have a change control process?
- Do you use FTP? How is it configured? Do you have vendor documentation for FTP?
- What are the roles and responsibilities of those that impact the security of your PHI environment? Do you have this detailed for daily, weekly, monthly, quarterly, and yearly tasks (where applicable)?
DOCUMENTS YOU SHOULD START WORKING ON

If you haven’t already guessed, HIPAA documentation requirements go far beyond policies and procedures. If you’re looking for ideas on what you should be documenting at your organization, here’s a sample list to get you started:

• HIPAA Risk Management Plan
• HIPAA Risk Analysis
• PHI location documentation (e.g., a PHI map)
• Notice of Privacy Practices
• How you’ve eliminated third party risks
• Software development lifecycles
• Business associate agreements (BAA) and/or enforceable consent agreements (ECA)
• How the environment is coping with identified vulnerabilities
• Incident response plan/breach response plan
• Current/future goals and milestones
• Explanation of unimplemented addressable implementation standards
• Work desk procedures
• Training logs
• Compliant processes and procedures
• List of authorized wireless access points
• Inventory of all in-scope devices including physical location, serial numbers, and make/model
• Electronic commerce agreements
• Trading partner security requirements
• Lists of vendors
• Lists of employees and their access to systems
• Diagram of your physical office, including exit locations
• Disaster recovery book
• Employee handbook
• Policies and procedures for the Security Rule, Privacy Rule, and Breach Notification Rule
UPDATE YOUR HIPAA DOCUMENTATION

The biggest disservice you could do while meeting HIPAA documentation requirements is to spend weeks gathering paperwork, and then place it on a shelf until next year.

HIPAA DOCUMENTATION IS ONLY AS GOOD AS ITS ACCURACY AND IF IT REMAINS UP TO DATE.

In order to keep your HIPAA document collection up to date, you must constantly revise and add to it.

Just like all your other weekly activities, documentation should be an ongoing part of your entire business-as-usual security strategy. Try to examine and adjust at least one piece of documentation each week or as you make organizational updates. Don’t pile it into one day or one month at the end of the year.
HIPAA TRAINING

Most workforce members aren’t malicious, but they often don’t know what is required of them. If you don’t give your workforce members specific rules and train them on those rules, they won’t be able to keep PHI secure. Workforce member training and education will remind them that security is important and stop any bad security behaviors.

Another reason HIPAA workforce member training is so important is to keep workforce members aware of the most up-to-date security policies and practices. Threats to the healthcare industry are constantly changing, which means security practices should follow. If workforce members are only trained once, they probably won’t be able to keep up to date with your constantly changing security best practices and certainly won’t keep up with the threats.

WORKFORCE MEMBERS ARE CONSIDERED THE WEAKEST LINK IN PHI SECURITY AND HIPAA COMPLIANCE BY MOST SECURITY PROFESSIONALS.

You need to train your employees regularly (at least quarterly). You might consider breaking training into sections (e.g., monthly small and easy trainings), making it easier to remember and implement procedures. Your workforce is also more likely to be up to date on all rules and regulations, as well as protect your patient’s sensitive data.

One of the biggest areas organizations fail is through Security Rule compliance. Most workforce members do not understand their responsibilities when it comes to protecting electronic PHI, assuming they have no critical role in security because IT and/or administration have everything secured.

However, take malware as an example; without proper training, your staff may log on to a personal email or social media account containing a malicious link, select the link, and inadvertently download malware. Consider having specific training about the following topics:

- Password management
- Social engineering
- Phishing
- Social media compliance
- Security updates/reminders
- Log-in monitoring
- Physical workstation security
- HIPAA privacy and security rules
- Disposal of data, media and equipment
HIPAA TRAINING DATA

We interviewed 53 healthcare professionals (who were responsible for HIPAA compliance) about HIPAA training. Throughout this section, you’ll find results from this survey, such as the following graph:

**HOW OFTEN ORGANIZATIONS TRAIN THEIR EMPLOYEES**

- **Annually**: 60%
- **Semi-annually**: 15%
- **Quarterly**: 10%
- **Monthly**: 8%
- **Never**: 5%
- **Don’t know**: 2%

*Employees should receive regular training about HIPAA best practices (e.g., quarterly, monthly).*

**ORGANIZATIONS TRAIN EMPLOYEES ON THE FOLLOWING HIPAA RULES**

- **HIPAA Security Rule**: 70%
- **HIPAA Breach Notification Rule**: 70%
- **HIPAA Privacy Rule**: 74%

*Employees should be trained on all HIPAA standards (e.g., Security Rule, Breach Notification Rule, Privacy Rule).*
TRAINING BEST PRACTICE

Implement a continuous training approach by soaking data security best practice information into messages that go to workforce members. Make it part of the employee newsletter. Send regular emails that run through real-life scenarios. Put tips on bulletin boards. New hires should be indoctrinated in your HIPAA compliance campaign as soon as possible.

Your educational campaigns should also remind readers that HIPAA compliance doesn’t just happen within the walls of your organization. Hackers can steal information on the subway or by eavesdropping a phone call at the grocery store. Even sharing too much information on social media can easily lead to a cyber security attack.

THE REGULAR ROUTINE OF WORK MAKES IT EASY FOR EMPLOYEES TO FORGET CRUCIAL SECURITY INFORMATION LEARNED DURING TRAININGS.
Conduct workforce member training in the manner that works best for your organization. As you set up your training plan, here are some tips to consider:

- Provide training as a mandatory part of new hire orientation
- Require monthly or quarterly training of all staff members or develop a weekly educational program (annual training isn’t enough)
- Keep a repository of policies and procedures (keep these updated and inform staff of updates)
- Develop a verification process to ensure training completion
- Document dates and times when workforce members complete their training
- Evaluate your training program effectiveness each quarter
- Reduce costs by making training part of your comprehensive educational program

**ORGANIZATIONS TEST EMPLOYEES ON HIPAA TRAINING**

- Yes: 39%
- No: 51%
- Don't know: 10%

**HOW OFTEN ORGANIZATIONS TEST EMPLOYEES ON HIPAA TRAINING**

- Annually: 37%
- Quarterly: 19%
- Never: 4%
- Don't know: 40%

Regularly test employees on HIPAA-related training (e.g., quarterly).
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

HIPAA TRAINING BEST PRACTICES

If you think your workforce members know how to secure patient data and what they’re required to do, you’re sadly mistaken. In fact, most breaches originate from healthcare workforce members. Although most healthcare workers aren’t malicious, they often either forget security best practices or don’t know exactly what they’re required to do.

Unfortunately, many hackers will take advantage of human error to gain access to sensitive data. For example, thieves can only steal laptops if workforce members leave them in plain sight unattended. Hackers can only access networks because workforce members set up easy-to-guess passwords. Improper disposal only happens when staff decide to throw PHI away instead of shredding it. And the list goes on.

To help protect sensitive data, employees need to be given specific rules and regular training to know how to protect PHI. Regular training (e.g., brief monthly training) will remind them of the importance of security, especially keeping them up to date with current security policies and practices. Here are some tips to help get employees prepared:

- Set monthly training meetings: focus each month on a different aspect of data security, such as passwords, social engineering, email phishing, etc.
- Give frequent reminders: these could be sent out in an email, newsletter, during standup meetings, and/or HIPAA security webinar that includes tips for employees.
- Train employees on new policies ASAP: newly hired employees should be trained on security and HIPAA policies as quickly as possible.
- Make training materials easily available: Intranet sites are a great way to provide access to training and policy information.
- Create incentives: reward your employees for being proactive.
- Regular test employees: create an environment where employees aren’t afraid to report suspicious behavior.

BRAND BARNEY

SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
HOW TO PREPARE FOR A HIPAA AUDIT

First, remember that HIPAA auditors are not your enemy; they want to help you make your organization more secure for your workforce members and your patients. But if you aren’t prepared for the audit, a mandated audit can quickly become a nightmare for you.

WHY ARE YOU GETTING AUDITED?

A HIPAA audit is not necessarily the result of a whistleblower or a possible HIPAA violation. It’s mainly for OCR to assess and gain an understanding of how healthcare providers are doing in HIPAA compliance, and if any changes need to be made.

There are a few reasons why your organization may be getting an audit. Here are the primary audit triggers:

- **At random**: the OCR conducts random audits on organizations to see how healthcare entities are doing with HIPAA compliance
- **Complaints**: A customer, or even an employee can file a complaint with the HHS, which may lead to an audit.
- **Self-reported breach**: If you have had a breach, you have a much higher chance of being audited.

All covered entities and their business associates are eligible for a HIPAA audit. This may include health service providers, health care clearinghouses, health plans, and many business associates of these entities.

HOW DOES THE AUDIT WORK?

OCR will do desk and onsite audits. These audits will look at compliance with specific requirements of the Privacy, Security, or Breach Notification Rules.

For the desk audit, selected entities will be sent an email, asking for documents and other data. Once you’ve submitted your information, be prepared for an onsite audit.

The onsite audits will involve someone going to your organization and examining how your organization is complying with HIPAA. These audits will examine a broader scope of requirements from the HIPAA rules and will be more comprehensive.

Auditees will then receive audit reports, which they can respond to any findings that were discovered in the audits. They will then receive a final report, which will describe how the audit was conducted, discuss any findings from the audit, and contain entity responses to the findings. This report should be provided 30 days after the auditee’s response.
AUDIT PREPARATION
BEST PRACTICES

HAVE DOCUMENTATION READY
This is probably one of the most important things to prepare for your audit. Having the proper documentation ready will make your audit go much faster and help you avoid costly penalties, which is why documentation has been mentioned so much in this guide.

HIPAA documentation isn’t something you can create overnight. Here are the top 5 pieces of documentation auditors look for.

1. EMPLOYEE TRAINING DOCUMENTATION
Your workforce members are among your weakest links in your organization, so you should be devoting more time to training. And this training should all be written down. Training helps workforce members remember important security practices to keep PHI secure.
   - Regular training for all employees
   - Verification process to ensure training completion
   - High quality content presented during training
   - Training completion dates for each staff member
   - Evaluation process for training program effectiveness

2. POLICIES AND PROCEDURES
Policies aren’t just paperwork. They outline in writing what you promise to do to protect your patient’s medical data.
   - Privacy Rule policies (e.g., use and disclosure of PHI, NPP)
   - Security Rule policies (e.g., password requirements, encryption)
   - Breach notification policies (e.g., incident management, breach processes)
   - Frequent updates to policies and procedures
   - Where policies are stored and how they are disseminated to staff

3. BUSINESS ASSOCIATE AGREEMENTS (BAA)
Providers and third parties agree to share responsibility for patient data protection, but it’s still the primary responsibility of the provider to ensure PHI protection.
   - Recently signed agreements for all business associate relationships
   - Agreements updated to include Omnibus language
• Satisfactory assurance that each business associate safeguards patient data
• Business associate risk evaluation
• Annual reevaluation of contracts

4. HIPAA RISK ANALYSIS
A HIPAA risk analysis identifies potential security threats that put your patients’ data and your organization at risk.
• Lists of employees with their access to PHI
• Flow diagram of PHI in your environment
• Lists of systems with access to PHI (e.g., servers, workstations, laptops)
• Identified vulnerabilities, threats, and risks to patient data
• Risks, prioritized based on likelihood of occurrence and potential impact

5. HIPAA RISK MANAGEMENT PLAN
A HIPAA risk management plan is simply your outlined strategy for mitigating risks found in your risk analysis.
• Organizational HIPAA goals
• Each vulnerability and assigned risk level
• HIPAA security control to do’s
• Dates completed and employee that completed it
• Notes that address unimplemented guidelines

CONDUCT INTERNAL AUDITS
Conducting audits within your organization can help you find resolvable problems in your security before your audit. It's best to do these audits periodically to find new issues that may appear.

Organizations should engage a third party security expert to help with conducting a proper security assessment. A security assessor will have experience in HIPAA (and many other security mandates) and will be able to see your organization from an external view (which is what malicious attackers are doing).
HIPAA BUDGET

To become HIPAA compliant, you’ll need to spend money. The cost of HIPAA compliance entirely depends on your organization. Here are a few variables that will factor in to the cost of your overall compliance.

- **Your organization type:** Are you a hospital, business associate, electronic health information exchange (HIE), healthcare clearinghouse, or another type of healthcare provider? Each will have varying amounts of PHI and varying risk levels.

- **Your organization size:** Typically, the larger the organization, the more vulnerabilities it has. More workforce members, more programs, more processes, more computers, more PHI, and more departments means more HIPAA cost.

- **Your organization’s culture:** If data security is one of upper management’s top priorities, increasing security costs probably isn’t a major internal struggle. In other cases, management is very hesitant to dish out budgets to HIPAA, because they don’t understand their organization’s security liabilities.

- **Your organization’s environment:** The type of medical devices, the brand of computers, the kind of firewalls, the model of backend servers, etc. can all affect HIPAA compliance cost.

- **Your organization’s dedicated HIPAA workforce:** Even with a dedicated HIPAA team, organizations usually require outside assistance or consulting to help them meet HIPAA requirements.

The following are estimated HIPAA budgets:

<table>
<thead>
<tr>
<th>SMALL COVERED ENTITY</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scanning</td>
<td>$1K</td>
</tr>
<tr>
<td>Training and policy development</td>
<td>$2K</td>
</tr>
<tr>
<td>Risk Analysis and Management Plan</td>
<td>$2K</td>
</tr>
<tr>
<td>Remediation</td>
<td>$1K</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$6K+</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MEDIUM/LARGE COVERED ENTITY</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scanning</td>
<td>$1K</td>
</tr>
<tr>
<td>Training and policy development</td>
<td>$2K</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>$5K</td>
</tr>
<tr>
<td>Risk Analysis and Management Plan</td>
<td>$20K</td>
</tr>
<tr>
<td>Onsite audit</td>
<td>$40K</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$68K+</strong></td>
</tr>
</tbody>
</table>

Keep in mind this budget doesn’t include remediation security measures, such as firewalls, encryption, updating systems and equipment, etc. However, this is far cheaper than paying for a data breach, which can easily cost anywhere from $180,000 to 8.3 million and above.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

OVERCOMING MANAGEMENT’S BUDGET CONCERNS

If you’re having problems communicating budgetary needs to management, conduct a risk assessment before starting the HIPAA process. NIST 800-30 is a good risk assessment protocol to follow. At the end of this assessment, you have an idea of the probability of a compromise, how much money might be lost if compromised, and the impact a breach might have on your organization (e.g., brand damage).

Simply put, find a way to show how much a lack of security will cost the organization. For example, “if someone gains access through a designated system, this is how much it will damage our brand and cost our organization.” Consider asking marketing or accounting teams for help delivering the message in more ‘bottom-line’ terms. If possible, work with your HIPAA to come up with security controls to address the requirements to gather information on what tools you may need to implement.

JEN STONE

*SecurityMetrics | MSCIS | CISSP | QSA*
CONCLUSION
TOP-DOWN SECURITY

Unless someone is in charge of HIPAA on management’s side (not just IT), HIPAA compliance won’t happen. In last year’s SecurityMetrics HIPAA Security Rule Report, data shows that C-Suite often believes they are 10% or even 20% more compliant with most HIPAA policies than what the IT and Compliance and Risk Officers (who actually handle these HIPAA tasks) believe.

Often, C-Suite expects their staff to be fully compliant with HIPAA standards, but the IT, Compliance, and Risk workforce are not given adequate resources to implement security best practices. In some cases, these individuals do not have enough expertise to fully address specific aspects of HIPAA compliance (e.g., external vulnerability scans). This usually forces those in charge of HIPAA compliance to cut corners in their security measures or not even address the issues at all.

Security is not a bottom-up process and you can’t just tell IT to ‘get us compliant.’ because checkbox attitudes lead to breach. Management at the highest level (e.g., CEO, VP, CTO, CIO) must understand that HIPAA initiatives should come from the top and be pushed down.
HEALTHCARE SECURITY SPECIALIST’S PERSPECTIVE

HEALTHCARE SECURITY
My experience is that executives aren’t listening to their staff about their current compliance state, and staff doesn’t fully understand how to translate the HIPAA regulations into specific controls.

Moving forward, entities need to outsource or bring information security experts on-board to obtain solid security advice.

Budgets should have more emphasis on security. I’ve seen large organizations spend hundreds of thousands of dollars on new medical equipment, then balk at an important security tool costing only a few thousand. Some make the argument that equipment saves lives or improves patient well-being. What happens to your patients well-being when you lose their PHI and an identity thief destroys their credit, or has procedures done under their name, health plan ID, and SSN?

Compliance officers need to better understand the risks, and then find ways to convey that information appropriately to the executive team. Often, a third party can help add credibility. Entities and the executives, in particular, must begin committing the appropriate budget and personnel resources to adequately secure PHI.

BRAND BARNEY
SecurityMetrics Security Analyst | HCISPP | CISSP | QSA
CONTRIBUTORS

BRAND BARNEY  WINN OAKEY
RYAN MARSHALL  CHAD HORTON
TREVOR HANSEN  STEVE SNELGROVE
MATT GLADE  BRYSON LAY
JEN STONE  JONATHON BOYER
DAVID ELLIS  CARLOS ESPINO
ARIEL MCKENNA  BRANDEL POULSEN
DAVID PAGE  JASON LELAND
GEORGE MATEAKI  JON CLARK
MARK MINER  COLLIN MANGUM
MATT HALBLEIB  HEATHER MOON
MICHAEL SIMPSON  LINDSEY HOOLEY
THOMAS MCCRARY  ERIC SMITH
TERMS AND DEFINITIONS

ACL (Access Control List): a list of instructions for firewalls to know what to allow in and out of systems.

AES (Advanced Encryption Standard): government encryption standard to secure sensitive electronic information

BA (Business Associate): a person or entity that performs certain functions that involve the use or disclosure of PHI (e.g., CPA, IT provider, billing services, coding services, laboratories.)

BAA (Business Associate Agreement): a contract between a covered entity and business associate to safeguard PHI and comply with HIPAA.

Breach: an impermissible use or disclosure of protected health information resulting in significant risk of financial, reputational, or other harm to the affected individual.

CISO (Chief Information Security Officer): similar to a CSO, but with responsibility for IT rather than entity-wide security.

Covered Entity (CE): a health plan, health care clearinghouse, or health care provider that electronically transmits health information (e.g., doctors, dentists, pharmacies, health insurance companies, company health plans.)

CSO (Chief Security Officer): company position with responsibility towards HIPAA compliance, PCI compliance, physical security, network security, and other security protocols.

EHR (Electronic Health Record): digital chart that contains a patient’s comprehensive medical history from multiple healthcare providers.

EMR (Electronic Medical Record): digital chart that contains a patient’s medical history from a single practice used for diagnosis and treatment.

ePHI (Electronic Protected Health Information): health information sent or stored electronically protected by the HIPAA Security Rule.

FIM (File Integrity Monitoring): a way of checking software, systems, and applications in order to warn of potential malicious activity (i.e., when a file is changed).

Federal Information Processing Standards (FIPS): US federal government standards for computer security that are publicly announced (e.g., encryption standards).

FW (Firewall): system designed to screen incoming and outgoing network traffic.
HHS (United States Department of Health and Human Services): the federal organization that created HIPAA.

HIPAA (Health Insurance Portability and Accountability Act): a federal mandate that, among other things, requires organizations to keep patient data secure through a myriad of privacy and security procedures, policies, and actions.

HITECH Act (Health Information Technology for Economic and Clinical Health): 2009 legislative act that, among other things, implements a series of fines to enforce HIPAA compliance and requires business associates to adhere to the same level of HIPAA compliance as covered entities.

HTTP (Hypertext Transfer Protocol): A method of communication between servers and browsers. (See: HTTPS)

HTTPS (Hypertext Transfer Protocol Over Secure Socket Layer): A secured method of communication between servers and browsers

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): a system used to monitor network traffic and report potential malicious activity.

IRP (Incident Response Plan): policies and procedures to effectively limit the effects of a security breach

IT (Information Technology): anything relating to networks, computers, and programming, and the people that work with those technologies.

MFA (Multi-factor Authentication): two out of three independent methods of authentication are required to verify a computer or network user. The three possible factors are:

- Something you know (such as a username and password)
- Something you have (such as an RSA token or cell phone which gives you a new code for each login)
- Something you are (such as fingerprint or iris scan)

NAC (Network Access Control): restricts data that users, apps, and programs can access on a computer network.

NIST (National Institute of Standards and Technology): federal technology agency that assists in developing and applying technology, measurements, and standards.

NVD (National Vulnerability Database): a repository of all known vulnerabilities, maintained by NIST.

OCR (Office for Civil Rights): the federal organization responsible for enforcing HIPAA compliance.
OWASP (Open Web Application Security Project): a non-profit organization focused on software security improvement, often heard in the context of “OWASP Top 10”, a list of top threatening vulnerabilities.

PHI (Protected Health Information): information that can be linked to a particular person (i.e., past, present, or future health condition or healthcare provision) such as patient name, social security number, and medical history.

RA (Risk Analysis): an assessment of the potential vulnerabilities, threats, and possible risk to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate.

RBAC (Role-Based Access Control): the act of restricting users’ access to systems based on their role within the organization.

Risk: the likelihood a threat will trigger or exploit a vulnerability, and the resulting impact on an organization.

RMP (Risk Management Plan): the strategy to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.

SFTP (Secure File Transfer Protocol): a secure way to encrypt data in transit.

SSL (Secure Socket Layer): Internet security standard for encrypting the link between a website and a browser to enable transmission of sensitive information (predecessor to TLS).

Threat: the potential for a person, event, or action to exploit a specific vulnerability.

TLS (Transport Layer Security): (See SSL)

VPN (Virtual Private Network): technical strategy for creating secure tunnels over the Internet. Vulnerability: a flaw or weakness in procedure, design, implementation, or security control that could result in a security breach.

WEP (Wired Equivalent Privacy): an outdated and weak security algorithm for wireless networks.

WPA (Wi-Fi Protected Access): security protocol designed to secure wireless computer networks.

WPA2 (Wi-Fi Protected Access II): (see WPA)

3DES (Triple Data Encryption Standard): a secure encryption standard that encrypts data three times.
ABOUT SECURITYMETRICS

SecurityMetrics is a global leader in data security and compliance that enables businesses of all sizes to comply with financial, government, and healthcare mandates. Since its founding date, the company has helped over 800,000 organizations protect their network infrastructure and data communications from theft and compromise with exceptional value to customers worldwide. Among other services, SecurityMetrics offers HIPAA and PCI audits, penetration tests, security consulting, data discovery, and forensic analysis, and vulnerability scanning.

www.securitymetrics.com/hipaa-audit

801.705.5656