Overcoming Barriers of a Remote Compliance Audit

By

Elisha M. Parsons

Bachelor of Science

in

Information Security & Intelligence

Ferris State University, 2018

Advisor:

Dr. Greg Gogolin

Full Professor

Accounting, Finance, and Information Systems Department

Spring, 2020

Ferris State University

Big Rapids, MI

Table of Contents

Abstract

This study reviews the current remote audit capabilities, mainly pertaining to HIPAA and PCI compliance, however, some of the broader ideas may be applied to remote auditing in general. Recognizing the global pandemic caused by COVID-19, many people are working remotely, including IT auditors who, at times, must conduct in-person observations to ensure compliance. Working from home best practices are discussed, along with responsibilities and tasks that may be completed by both the employer and the employee. This document provides an overview of HIPAA and PCI compliance and analyzes how certain barriers of working from home may impact an audit. To assist present and future auditors, this study explores how to overcome those barriers and how these solutions may be applied to HIPAA and PCI compliance.

Chapter 1

Introduction

Right now, around the globe, we are experiencing a global pandemic from COVID-19, a virus that causes a respiratory illness that can cause fever, cough and shortness of breath. Many people are fighting for their lives; some young, but many more are elderly. Governments and policy makers are doing what they believe to be right for the people they govern in order to overcome this crisis. In extreme cases, COVID-19 can also cause pneumonia, multi-organ failure and even death (Center for Disease Control and Prevention, 2020).

Elderly individuals and individuals with pre-existing medical conditions, especially respiratory conditions, are much less likely to recover than someone in good health. Governing bodies in the United States and around the world have issued stay-at-home orders, advise self-isolation if one is experiencing symptoms and social distancing when in public to help minimize the spread of this disease.

In addition, many companies and organizations around the world are only requiring essential employees to continue to go to work, causing many to now be unemployed, while others can work remotely. Many employers previously had the capability for their employees to work remotely, but this does not necessarily mean that their infrastructure can support nearly all their employees to work remotely.

Infrastructure aside, there are many other things to consider when a company with tens of thousands of employees suddenly transitions to working remotely such as the security of all the external endpoints at home. Employees now have company data offsite whether it is on a company owned device or a personal device that they are now leveraging for remote work during

the crisis. Depending on the nature of the data, it may be subject to compliance requirements per an industry standard or federal law.

Background

Ensuring these companies and organizations are continuing to meet the compliance requirements is crucial to the confidentiality, integrity and availability of the customer and organizational data. Before the global crisis, most of the data used by employers—and the employees themselves—were in more centralized locations such as on company-owned property or in the cloud by a third-party provider. Having all the data in one location makes it much easier for an audit team to evaluate the compliance requirements as opposed to if the data is literally spread across the globe.

Problem Statement

During this time when most white-collar employees are working remotely, they are advised by their employer to not leave their homes, and in some cases, not permitted to travel by local governments. Although the capability to work from home is there, many companies and organizations may struggle with securing remote working capabilities and ensuring that their data is secure while employees are working remotely. It also has the potential to greatly impact the quality of work that some individuals can perform due to the limitations of not being in the environment they are used to physically working in. Depending on the work that is required, compliance auditors are required to observe certain procedures or behaviors to ensure compliance.

Therefore, the problem addressed in this study is in what ways can governance, risk and compliance (GRC) teams around the world ensure that compliance standards are still being met

while not being able to physically view and verify that different security controls are in place during a global crisis such as the pandemic caused by COVID-19.

Purpose of the Study

The purpose of this study is to define effective means to ensure the confidentiality, integrity and availability of company data while employees work remotely. In addition, this study will focus more heavily on the work of GRC teams and how the current pandemic has impacted their deliverables in ensuring companies and organizations are maintaining PCI and HIPAA compliance during the global crisis. The objective of this study is to evaluate and bring to light possible solutions for GRC and audit teams so that compliance can be maintained throughout the global crisis while many employees are working remotely.

Rationale

The results of this analysis may help future GRC and audit teams to better perform remote audits during a crisis when it is necessary. This is not intended to be guide to replace in-person audits with remote audits, but may be used as a reference during a scenario when the option of performing an in-person audit is limited or hindered by global crisis such as the one caused by COVID-19. In such a scenario, a trust but verify mindset may be needed for normal business functions to continue without completely halting the entity.

Research Questions

1. How could a company or organization effectively respond to a global crisis in which most of its employees must work remotely while keeping security in mind?
2. How might GRC deliverables be impacted during global crisis when a company or organization would still need to maintain PCI or HIPAA compliance requirements?

Nature of the Study

The nature of this study is to explore possible solutions for GRC teams to implement when performing a compliance audit remotely during a global crisis. Many of the potential problems when performing a remote audit make it difficult for an auditor to evaluate certain compliance requirements or organization behaviors without physically being at the location being audited. While some actions can be performed remotely, others require physical verification that a certain control is in place.

Significance of the Study

While the effects of COVID-19 can be seen around the world, people have been advised by different governing bodies to avoid contact with others as much as possible. In response, companies and organizations are struggling to continue normal business. This study will explore different challenges experienced by GRC and audit teams during a global crisis and how to overcome some of those challenges. Recently discovering my own interest for GRC and compliance auditing, this study has given me the opportunity to explore this interest of mine, while applying my knowledge of information security to best practices when working remotely.

Professionally, I hope to provide some insight as well as things to consider for people to be able to effectively and securely work from home when their specific position may require them to be somewhere in person. With a focus in GRC deliverables, employees currently evaluating the compliance requirements of their organization, or a third-party organization, will most likely have insufficient or inadequate means to acquire data to ensure the compliance of an organization

Definition of Terms

- MFA (Multi-Factor Authentication): Using two or more factors to authenticate a user (National Institute of Standards and Technology, 2019). A factor of authentication may include something you know, something you have, something you are, somewhere you are or something you do (Dias, 2017).
- Risk Based Decision Making: A decision making process in which a risk-reward methodology is applied to each possible option of a decision (Risktec, 2005).
- Telework Security Policy: A remote working security policy.
- MDM (Mobile Device Management): Software security solution used by IT organization to help manage mobile device applications and configuration settings (PCMag, n.d.).
- WPA2 and WPA3 (Wi-Fi Protected Access version 2 and version 3): Security standard for wireless internet capable devices.
- CIRT (Cyber Incident Response Team): A team of Security Analysts who develop, recommend, coordinate mitigation efforts and respond to computer security incidents (NIST, n.d.).
- PAN (Primary Account Number): The long 14 to 15-digit number generated for a payment card.
- ePHI (electronic Protected Health Information): Information including medical records and health insurance plan information.

Assumptions

It is assumed that the reader of this document has a basic understanding of technology along with information security best practices. It is also assumed that a simple understanding of compliance audits is understood.

Limitations

Research for this topic began in mid-March of 2020 and ended mid-April of 2020. Previously, there was very limited guidance and instructions by compliance agencies and audit firms on how to properly and successfully perform a remote audit due to government stay-at-home orders. New procedures and guidelines for auditors to follow are being released nearly every day. Before the pandemic truly set in, auditors were still required to physically assess certain compliance requirements as directed by compliance agencies.

Chapter 2: Literature Review

This literature review establishes best practices for working from home securely. It outlines what companies and organizations could do in order to better secure their data and customer data while still allowing their employees to be productive while working remotely. Furthermore, it discusses the requirements of HIPAA and PCI compliance while outlining what aspect of these two compliance standards may be subject to physical inspection during a compliance audit.

Securely Working from Home

In light of the transition from standard work-from-work to millions of people around the world working from home, the Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA) have provided some general guidelines for employers and employees to follow when working remote for the time being (Fein, Anderson, Canter, & Skeath, 2020). Although some of these guidelines may seem like common knowledge to some, it is always good to review as items can always be missed and frequently updated.

Company responsibilities. The company or organization should define a remote working security policy before employers are permitted to work remotely (Fein, Anderson, Canter, & Skeath, 2020). This policy should define which and what kind of devices can and cannot be used to work remotely (Fein, Anderson, Canter, & Skeath, 2020). Implementing risk based decision making into risk management will help govern which devices are allowed to be used offsite and which devices should remain onsite (Fein, Anderson, Canter, & Skeath, 2020). This will aid the policy makers in creating a tier-based list of devices, categorizing each device in terms of risk and then permitting which data should be allowed to be remotely access via that device (Fein, Anderson, Canter, & Skeath, 2020). As a suggestion, company owned laptops would typically have the most access to company data and resources while employee owned mobile phones would have the least amount of access (Fein, Anderson, Canter, & Skeath, 2020).

Employers should configure company-owned devices with a VPN to encrypt data in transit from the employee working from home, to the internal corporate network (Fein, Anderson, Canter, & Skeath, 2020). If there is no official corporate-provided VPN, it would be worthwhile to supply employees with a list of company-approved VPN solutions.

It is important to assume that all external environments are threats (Fein, Anderson, Canter, & Skeath, 2020). Keeping this in mind, an organization may consider limitting the data available on remote devices in addition to limiting how the data can be remotely accessed by these remote devices (Fein, Anderson, Canter, & Skeath, 2020). Adding MFA to an account used to access sensitive information will make it inherently more difficult for a wrongdoer to access the account. Encrypting telecommunications and data in transit will help mitigate eavesdropping attacks and man-in-the-middle attacks (Fein, Anderson, Canter, & Skeath, 2020). Ensuring remote workstations are configured with anti-malware software can help protect the endpoint

(Fein, Anderson, Canter, & Skeath, 2020). Additionally, the use of network access controls and proper network segmentation on the corporate network will make it more difficult for an adversary to gain access to critical internal systems (Fein, Anderson, Canter, & Skeath, 2020).

Company-owned devices are going to be more easily managed by the employer, inherently making them easier to secure compared to employee owned devices (Maddox, 2018). Through the company's MDM solution, the appropriate department should apply device updates to the OS and applicable applications, encrypt data and enforce password and acceptable use policies.

Moving on to remote access servers that are kept onsite; these assets should be fully patched, enforce a telework security policy and be managed by authorized administrators that can only access these servers by a secure host (Fein, Anderson, Canter, & Skeath, 2020). This telework or remote work security policy should define the following:

- Required equipment, operating system, and applications software (Hirsch, n.d.)
- Guidelines for the physical security of the equipment (Hirsch, n.d.)
- Measures that must be taken to protect the integrity and security of corporate data (Hirsch, n.d.)
- Employee login and account restrictions, if any (Hirsch, n.d.)
- Applications and data which may or may not be accessed remotely (Hirsch, n.d.)
- Disaster recovery, in case of theft, corruption, or destruction of equipment and/or data (Hirsch, n.d.)
- Support and maintenance guidelines and schedules, whether upgrades and support will be provided by the corporate IT staff or a third party (Hirsch, n.d.)

- Employee accountability and responsibility for data integrity and confidentiality (Hirsch, n.d.)
- Appropriate Personal Use policy if applicable (Hirsch, n.d.)
- Should pre-existing policies be modified to accommodate the new telework/remote work policy (Fein, Anderson, Canter, & Skeath, 2020)

Employers should provide employees with instructions on where to find security policies and who to reach out to with questions (Fein, Anderson, Canter, & Skeath, 2020). This can save a manager time if an employee has a specific question regarding security policies. Employers should also conduct regular security training for employees to raise security awareness that includes how to report a security incident (Fein, Anderson, Canter, & Skeath, 2020).

One critical step in preparing for a company-wide work-from-home order is to identify essential personnel (Fein, Anderson, Canter, & Skeath, 2020). Essential personnel may include IT Support Staff who operate command centers, data center operators, CIRT members and employees who work in customer service centers (Fein, Anderson, Canter, & Skeath, 2020).

Employees should be made aware of all security policies, where to find them and who to reach out to with questions.

Employee responsibilities. Employees may be responsible for their own home network configuration and its security. Employers should provide users with some basic guidelines for how to secure their home networks before connecting a company-owned device. Employees should be using WPA2 or WPA3 wireless access point security configurations along with strong passwords that are not the default password provided when the ISP setup the home network. If there is no employer-provided VPN, the employee may want to consider a VPN based on a list of employer-approved VPN options (Fein, Anderson, Canter, & Skeath, 2020).

While working from home, employees should be mindful of the physical security of their company-owned or personally owned devices used to access the corporate network (Fein, Anderson, Canter, & Skeath, 2020). These items may be addressed in the employer's Physical Security Policy and may include responsibilities such as locking one's computer when one steps away from their desk and not leaving a company-owned device in an unsupervised or unlocked vehicle in view of someone from outside. Employees should be made aware that these policies still apply to employees when working from home.

Employees should know all security policies, where to find them and who to reach out to with questions.

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) is a US law passed in 1996 is designed to protect customer and patient medical records and health insurance plan information. For an entity to be considered HIPAA compliant the entity must meet a set of security requirements revolving around the security of ePHI. HIPAA is generous in giving healthcare entities a list of requirements to be met and leaves a lot of the more technical details at the discretion of the healthcare entity.

During the current global crisis caused by COVID-19, HIPAA must still be followed, however, there are some exceptions put in place that will be discussed.

HIPAA requirements. There are two different categories of requirements; required and addressable. Required safeguards are, well, required to be implemented, while addressable safeguards are required unless there is a justifiable reason not to implement them.

Technical controls. The required technical safeguards that must be implemented to be HIPAA compliant are encryption of ePHI, whether at rest or in transit, to NIST encryption

standards when it moves beyond an internal firewall, audit controls, activity logs and authentication mechanisms (HIPAA Journal, n.d.). Encrypting ePHI will make it more difficult, but not impossible, for an attacker to access the data if obtained. Audit controls and activity logs should be used to track ePHI activity such as access, attempted access and what the user has done with the data once accessed.

One addressable technical safeguard is an authentication mechanism when accessing ePHI (HIPAA Journal, n.d.). This safeguard can be deduced to giving each user their own specific login credentials to help track user activity when accessing ePHI. Messages containing ePHI must also be encrypted if they go beyond an internal firewall (HIPAA Journal, n.d.).

Physical controls. It is required that the healthcare entity have a policy for the positioning and use of workstations (HIPAA Journal, n.d.). Having computer monitors positioned in such a way where customers and patients are unable to see what is displayed can help protect ePHI data. Additionally, adding privacy screens will also minimize the ability for others to view the screen. This policy should also outline the physical access to these machines that contain ePHI data. These may include locked doors, glass dividers and employee-only areas. A second required policy should outline controls for mobile devices (HIPAA Journal, n.d.). These controls should focus on exactly how ePHI data is removed from mobile devices (HIPAA Journal, n.d.). This is beneficial if a device no longer needs to be used by the organization, or if a device used by someone needs to be purged of all its data to be reused by another employee.

HIPAA outlines two different addressable physical controls. The first states that there should be limited access to the facility (HIPAA Journal, n.d.). These controls may include locked doors, RFID access cards to doors, mantraps, etc. Limiting the physical access to the facility of unauthorized personnel is the goal. The second addressable physical control supplied by HIPAA

is an inventory of hardware (HIPAA Journal, n.d.). This list must be maintained along with a record of where each item is located (HIPAA Journal, n.d.). Additionally, if a piece of equipment is to be moved, an exact copy of ePHI must be created before it is moved (HIPAA Journal, n.d.). This will help prevent data loss if something were to happen to the equipment in transit. It will also make the data continually available while the equipment is being moved. Having these files stored on the network will make them readily available to those who need it.

Administrative safeguards. HIPAA outlines four required administrative requirements. These include conducting risk assessments, introducing a risk management policy, developing a contingency plan and restricting third-party access to ePHI data (HIPAA Journal, n.d.). These implementation specifications are somewhat unique because they require dedicated individuals to oversee that these controls are in place. In accordance with conducting risk assessments, the designated Security Officer must "…identify every area in which ePHI is being used, and to determine all of the ways in which breaches of ePHI could occur." (HIPAA Journal, n.d.). This allows for a single point of contact when one has questions or concerns regarding risk assessments.

Under the risk management policy, risk assessments must be conducted on a regular basis that measure risk within the organization. However, when an employee fails to comply, they must be disciplined according to a sanctions policy listed under the risk management policy (HIPAA Journal, n.d.). Due to the nature of COVID-19, some sanctions have been waived.

A contingency plan must be enacted in the event of an emergency and should include details about how to continue normal business functions (HIPAA Journal, n.d.). One critical aspect of this is to continue to maintain the security, confidentiality and availability of ePHI data while the entity is still operating in emergency mode (HIPAA Journal, n.d.). These critical

processes and procedures may include encryption of all ePHI, secure access measures such as VPN capabilities, and physical security measures such as card readers, security cameras and keypad entry doors. Maintaining physical access to data and records is critical if there are additional network outages.

HIPAA also requires restricting third-party access to ePHI data, both during and not during an emergency (HIPAA Journal, n.d.). Some third parties may include parent companies, contractors or other business partners. The use of Business Associate Agreements should occur, and all entities with access to ePHI should sign these documents to demonstrate their understanding and compliance (HIPAA Journal, n.d.). Additionally, sanctions and legal proceeding should occur if these agreements are broken.

Moving on to addressable specifications, HIPAA outlines that a secure employee training procedure be in place, different avenues for reporting security incidents and the testing of the contingency plan may occur (HIPAA Journal, n.d.). Employee training should be performed in a secure and documented fashion. All attendees should be accounted for and should have increased awareness of general security practices pertaining to HIPAA, ePHI and the organization itself. Attendees should also learn how to identify suspicious and malicious activity (HIPAA Journal, n.d.). Increasing the general populous' knowledge of information security is the first step in securing an organization as humans are known to simply make mistakes.

During the training, one topic that would be ideal to cover is how to report a possible security incident. Hopefully, the report is filed before the occurrence of a breach to better contain the incident. Organizations will typically already have one or more methods of reporting incidents, but it should be made clear exactly how to report a security-related incident as opposed to an employee or customer safety related incident.

Testing the contingency plan is also suggested by HIPAA, although it should take place unless there is an alternative in place (HIPAA Journal, n.d.). Some things to consider include the availability of backups, as well as an evaluation of which processes and procedures are deemed critical as this may change over time.

Current exceptions. In light of the current global pandemic, President Donald J. Trump and the Secretary of Health and Health and Human Services, Alex M. Azar waived sanctions for certain requirements of the HIPAA Privacy Rule (U.S. Department of Health & Human Services, 2020). Below is a list of the following Privacy Rule requirements and patient rights where sanctions are waived:

- Employees of the healthcare entity are no longer required to obtain the patient's permission before speaking with family and friends caring for the patient (U.S. Department of Health & Human Services, 2020).
- The healthcare entity is not required to honor a request to opt out of the facility directory (U.S. Department of Health & Human Services, 2020).
- The healthcare entity is not required to distribute a notice of their privacy practices (U.S. Department of Health & Human Services, 2020).
- The healthcare entity is not required to honor the patient's right to privacy restrictions (U.S. Department of Health & Human Services, 2020).
- The healthcare entity is not required to comply with a patient's request for confidential communications (U.S. Department of Health & Human Services, 2020),

It is important to note that these waivers are only applicable if the healthcare entity meets a few requirements. The healthcare entity must be operating in a location where a public health

emergency has been declared (U.S. Department of Health & Human Services, 2020). This first requirement ultimately leaves it up to state, local or even the federal government so entities cannot abuse this declaration. The healthcare entity must have already instituted their disaster protocol (U.S. Department of Health & Human Services, 2020). This will require the healthcare entity to focus on what is critical to it, allowing to focus on the most basic of needs for it to move through the crisis. The final requirement is that the waiver only applies to the healthcare entity for up to 72 hours after the implementation of the entity's disaster protocol (U.S. Department of Health & Human Services, 2020). This waiver may be used to help healthcare entities to get on their feet during this crisis as most hospitals are severely overrun with positive cases of COVID-19.

It is important to note that if a healthcare entity utilizes the waiver, they must still implement security safeguards to protect patient information (U.S. Department of Health & Human Services, 2020). This ensures, that even during the time of a crisis, security practices are still implemented. This is incredibly important as the number of internet users has increased due to the many stay-at-home orders and social distancing practices that many state and local governments have put in place (Fidler, 2020). Additionally, people working from home should implement and follow secure working practices to protect company data.

PCI Compliance

Unlike HIPAA, PCI lays out many more specific requirements that an entity seeking compliance must meet. Their requirements revolve around four key ideas: (1) protect cardholder data; (2) maintain a vulnerability management program; (3) implement strong access control measures; (3) regularly monitor and test networks; and (4) maintain an information security policy (PCI Security Standards Council, 2008). Notice how many of these broad categories relate

to HIPAA compliance as many of these are also discussed, although not in depth, by HIPAA. Furthermore, PCI dissects these four key topics into more specific requirements.

Maintain a secure network. PCI requires the company or organization to install and maintain a firewall and router configuration (PCI Security Standards Council, 2008). This will help the entity protect cardholder data but will also allow for a more formalized testing structure when the time comes. The entity should also whitelist network connections to disallow untrusted connections to network components that handle cardholder data. The components handling cardholder data should be in a separate network environment from other components directly connected to the internet to eliminate public access. Restricting public network access to these crucial components will inherently make it more difficult for attackers to gain remote access to the network components handling cardholder data.

PCI also require organizations to not use vendor-supplied defaults for systems such as usernames, passwords and configurations (PCI Security Standards Council, 2008). This goes for all vendor-supplied parameters, hardware or software, to protect not only cardholder data, but company data as well. One way to get started is to create a set of organization-wide standards for configuring new systems. This can act as a good basis for configuring new systems while helping to secure the whole network.

Protect cardholder data. PCI strongly suggests to never store cardholder data, but if an entity must, then the data must be encrypted and unreadable (PCI Security Standards Council, 2008). The organization's data retention policy should be applied to cardholder data, and the organization should never store sensitive authentication data (PCI Security Standards Council, 2008). Additionally, wherever the PAN is stored, it should be unreadable, and, if displayed, the maximum number of characters that may be displayed are the first six and the last four (PCI

Security Standards Council, 2008). This not only helps to hide the data when it is stored, but also when it is displayed on a monitor or mobile device during a customer purchase, it will make it more difficult for people who are shoulder surfing to gather their account information for malicious use.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name[1]	Yes	Yes[1]	No
	Service Code[1]	Yes	Yes[1]	No
	Expiration Date[1]	Yes	Yes[1]	No
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2 / CVC2 / CVV2 / CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

Table 1: Cardholder date elements and how to store them (PCI Security Standards Council, 2008.).

As seen in Table 1, data elements categorized as Sensitive Authentication Data must never be stored (PCI Security Standards Council, 2008). These data contain unique transaction information, as well as unique card data.

Not only is it necessary to protect cardholder data while it is stored, it is also a necessity to protect this data while it is in transit. PCI SSC suggests to use security protocols such as SSL/TLS while transmitting cardholder data over public networks, and any device connected to an environment handling cardholder data (PCI Security Standards Council, 2008). Following these guidelines will help to protect cardholder data while it is moving throughout the network. When configuring the network to handle PCI data, the company or organization should not use WEP as it is not as secure as WPA2 or WPA3, which should be used instead.

Maintain vulnerability management program. An organization's vulnerability management should continually be testing the PCI environment for weaknesses and vulnerabilities (PCI Security Standards Council, 2008). "This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy" to ensure maximum security overtime (PCI Security Standards Council, 2008).

Anti-virus software must be used on all systems when possible (PCI Security Standards Council, 2008). This software must also be kept up to date to evolve with the ever-changing world of malware. Key endpoints to install anti-virus software on include employee laptops, servers and mobile devices that may come in contact with PCI data. Furthermore, having anti-malware software running on devices throughout the organization will help maintain a secure environment for all connected devices.

An organization utilizing third-party software to handle PCI data must install patches to critical systems as soon as possible, as they are required to have the most up to date software on these systems within one month of the update being released (PCI Security Standards Council, 2008). Other systems that need to be updated should be updated based on risk, with the highest risk software updated first (PCI Security Standards Council, 2008). Updating software to non-PCI systems using a risk-based methodology will help the organization mitigate the most critical vulnerabilities first.

When the organization is developing its own software, it is required that they do so by incorporating information security best practices in mind (PCI Security Standards Council, 2008). Software developer teams, software security teams and security architects should be mindful of OWASP Top 10 security vulnerabilities. Training these employees on how to resolve security vulnerabilities may help save time in the development process. Additionally, providing

these individuals with contact information for people in the organization who may know is a step in the right direction. Automated dynamic and static code scanners should help software developers identify vulnerabilities, and many, provide some basics remediation steps.

Finally, developing and implementing change control procedures for system components will help track who is responsible for what changes, and it is required for PCI compliance (PCI Security Standards Council, 2008). Some change control procedures may include a log of network equipment changes and code management systems such as GitHub or Bitbucket. Tracking such changes will help reviewers and auditors know who to contact if needed, as well as team members who may have questions about a particular change.

Implement access control measures. Access control measures should prevent physical or digital access to cardholder data by unauthorized personnel or users (PCI Security Standards Council, 2008). These measures may include physical or technical safeguards such as locked doors, role-based access and network access controls. As per required by PCI, cardholder data access should be based on a strict need-to-know basis, meaning that all should be denied access by default, unless their role requires access to such data (PCI Security Standards Council, 2008). Although it may be expensive, separation of duties is important in this scenario. Many people in an organization may wear several different hats, so to speak, but ensuring that those different hats do not overlap in such a way to give a specific employee the ability to go through a singular process alone is critical to security within an organization.

Restricting physical access to cardholder data to personnel is required by PCI (PCI Security Standards Council, 2008). These measures may include mantraps, security cameras or locked doors that require a RFID access card. These measures should be applied to any location that houses cardholder data (PCI Security Standards Council, 2008). Some locations to consider

may be datacenters, locations where backups are stored and the office or campus itself. If a visitor is to be on-site, they are required to sign-in on a visitor log that must be retained for at least three months (PCI Security Standards Council, 2008). Maintaining a list of people who have been in and out of locations containing cardholder data should help various teams verify who was where during an incident.

One security implementation that may help with separation of duties within an organization is the PCI requirement to give each user with access to cardholder data a unique user ID or username in addition to a passphrase or MFA (PCI Security Standards Council, 2008). This may make it easier for people to view overlapping access that could allow the user to complete and approve a procedure all on their own. It is important to note that any remote access requires MFA to authenticate each user, direct hire employee or a third-party employee or contractor, before they gain access to network systems (PCI Security Standards Council, 2008). Giving each user their own login credentials, coupled with MFA, will help ensure that the user logging in is who they say they are. Credentials to critical systems must also be maintained in a secure fashion by rendering all passwords unreadable while stored and in transit (PCI Security Standards Council, 2008). This will help ensure that even if a malicious user has network access, traversing through the network to critical infrastructure components will be more difficult.

Monitor and test networks. In an effort to help prevent malicious users from gaining access to systems or performing malicious activities, PCI requires regular monitoring and testing of network components (PCI Security Standards Council, 2008). PCI strongly encourages, and often times requires, the use of audit trails when it comes to system configurations, changes and monitoring (PCI Security Standards Council, 2008). These logs should be used for analysis to

discover errors, misconfigurations and unauthorized access. Down the line, these logs can be used by auditors to track user and administrative actions.

When testing networks, companies and organizations operating under PCI compliance must regularly test security controls to ensure proper and sufficient controls are in place to prevent malicious activities (PCI Security Standards Council, 2008). Organizations should practice both internal and external penetration tests and vulnerability assessments to find vulnerabilities and security controls that can be improved (PCI Security Standards Council, 2008). Additionally, an IDS and IPS will help find all wireless devices being used to help identify malicious activities (PCI Security Standards Council, 2008). Implementing these practices within an organization is the first step but ensuring that these activities are being carried out in a standardized fashion throughout the lifetime of the organization is critical.

Maintain information security policy. Maintaining an information security policy for all employees and contractors to follow will give them the opportunity to rise and meet the standards expected of them by the organization (PCI Security Standards Council, 2008). This information security policy should include an array of details under risk assessments, operational security procedures and security awareness training (PCI Security Standards Council, 2008). It is important to maintain this document in such a way that it is available to all employees and subcontractors and can be easily understood by all. If people are unable to read this document and understand it, it will be significantly more difficult for them to follow its instructions. Finally, these documents should be revised annually, at a minimum, for any edits that may be needed to improve security.

Chapter 3: Remote Auditing

Taking what has been outlined by HIPAA and PCI compliance, audit practices will now be applied. These audit practices will focus on the remote aspect of an audit, and how an audit team could potentially replace certain aspects of a typical in-person audit with remote alternatives.

Benefits of Remote Audits

With advancements of technology over the years, working remotely is much for feasible and, during times of a pandemic, required. Performing a remote audit has a few benefits for employees performing the audit, and the organization as a whole.

There are many ways a company or organization can save by performing a remote audit, such as travel expenses and travel time. An auditor will no longer need to physically be at the location that the audit is being performed, which may help with a lot of the logistics planning between the two parties (Gallo, 2020). This allows for meetings and interactions to be handled remotely as opposed to booking meeting rooms and interrupting the host organizations employees' normal workday.

Additionally, the audit team, while working remotely, will be more efficient (Gallo, 2020). The auditing team will be working in a place where they feel comfortable in a place they are used to. Their equipment, such as a desk, external monitors, will also be there. If working from their normal office location, high-speed internet should also be available if the organization being audited does not have it available (Gallo, 2020). Being more comfortable will increase productivity, thusly, reducing the time spent on the audit itself, saving time.

Drawbacks of Remote Auditing

There are many drawbacks of a remote audit. The ones that will be discussed in this section include human interaction, technology issues, auditor experience and remote audit accuracy and validity. These areas outline some of the reasons why remote audits are not always considered to be valid audits by compliance agencies. Each area provides unique challenges that an auditor may have to overcome for a remote audit to be as successful as possible.

Human interaction. By performing a remote audit, the most obvious drawback is the lack of human interaction. This makes it more difficult to properly evaluate processes and procedures. Having documentation is one thing, but properly following that documentation is a different animal.

This lack of involvement may cause employees of the host organization to be overlooked or ignored. Reaching out to someone via Skype or email may not be successful depending on the filtering options the host organization has in place. Even while communicating through instant messaging or email, nonverbal aspect of a conversation cannot be used by either party. This poses a serious threat to the true meaning of a message as nonverbal communication is prevalent in society (Lapakko, 2007).

Technology. As helpful as technology can be, it does not always work properly. Network connections and remote access to systems that need to be audited need to work properly in order for a remote audit to be successful (Gallo, 2020). VPNs could go down, or issues with instant messaging platforms may be encountered, among other things, that can put the audit on hold until the issues are resolved.

Auditor experience. An auditee performing a remote audit should have prior experience of how to properly perform an audit. Prior knowledge will also give them the foundation they

need to know what is considered to be sufficient audit evidence and what is not (Gallo, 2020). This should give them an idea of who to contact and when to contact them as communications from key people may be far and few between.

Remote audit accuracy. Trusting the accuracy of the audit may feel uneasy for some and rightfully so. However, this is the best some organizations can do considering the devastating impact COVID-19 has had around the globe. In some instances, a walkthrough may be necessary to verify that certain network components are wired correctly, to conduct interviews of key employees in charge of processes and verify that procedures are being followed correctly.

Remote audit validity. The biggest, and the most notable drawback is that remote audits are not recognized by all accreditation bodies (Gallo, 2020). Luckily, HIPAA has guidelines for performing a remote audit, or desk audit as they call it (U.S. Department of Health & Human Services, 2016). Regarding PCI, the agency has created a blog to provide further details on how a remote audit should be carried out by auditors (Leach, 2020).

Overcoming the Drawbacks of Remote Audits

Taking the drawbacks laid out above, this section will discuss how an auditor could work with the host organization to ensure the audit is as successful and as accurate as possible. The challenges will be addressed individually, as above, although some points may overlap as one solution may be applicable to more than one drawback.

Human interaction. Creating awareness in the host organization that an audit is being performed may help employees be more conscious that they may be contacted by the auditor (Gallo, 2020). When possible, it may be beneficial for an auditor to reach out to a local, approved subcontractor to verify necessary physical controls are in place and report back to the

auditor (Leach, 2020). This reduces the risk of acquiring an illness and saving travel time while still ensuring a third-party is verifying that compliance requirements are being met.

Certain processes and procedures may need to be observed by the auditor to ensure the actions are being performed correctly and accurately. This can be overcome by going the route of an approved subcontractor, or via a video call. Depending on the technology available, the host organization may have robots used for video calls to allow the auditor to move around the office as if they were present, or simply video call a person of interest and watch them perform the action.

Technology. Ensuring that remote connections are properly configured before an audit begins will help save time for the auditor as they may be able to point out issues or errors in their configuration before the audit begins. The auditor must be vigilant in their connection evaluation and feel confident that they will be able to complete the audit based on the resources provided to them. Designating a few key people in a contact sheet to reach out to in case of a failure may also save time for the auditor.

Auditor experience. Don't hire new people and expect them to be able to perform a remote audit without prior experience. Having a mentor program, or at least someone to guide newcomers or people new to the remote audit experience, may help less experienced auditors to gain their footing during these trying times.

Remote audit accuracy. When performing an audit, it is important to document everything. During a remote audit, however, an auditee may find themselves documenting more, untraditional items such as conversations taken place via email or instant messaging. These conversations may contain further clarification as to why or why not certain items are completed, or additional details on how procedures are being followed.

The auditor should ensure that the evidence they have gathered is true and supports the audit—the same as they would with an on-site audit. However, truly trusting a certain section of evidence may cause the audit to fall short. In this case, the auditor should document their shortcomings after performing the audit to the best of their ability.

Remote audit validity. There should be a mutual trust between the auditee and the auditor, especially during a remote audit. If a process or procedure is being fibbed, the auditee should not try and hide the fact that what the organization is doing is wrong or immoral. In cases where the auditor is unable to verify that an aspect of the audit is compliant, this should be documented, and a follow-up may be required. An in-person or on-site visit could be scheduled later, in accordance with government restrictions, in this event to further validate the accuracy of what has been documented. The auditor should trust what is given to them as accurate, but later, verify that it truly is accurate either with additional interviews or an on-site visit.

Overcoming HIPAA Barriers and Drawbacks

In 2016, the U.S. Department of Health and Human Services provided auditors with a document specifically outlining key questions for an auditor to ask depending on the type of audit. HIPAA guidelines for performing desk audits, or remote audits. It contains three distinct sections: (1) the first guides the auditor through a HIPAA Privacy audit; (2) the second provides details regarding a HIPAA Security Audit; (3) lastly, the third section gives instruction for gathering evidence for a HIPAA Breach Audit (See Appendix). This document will be discussed in further detail, along with the challenges and drawbacks previously explored.

When an entity is subject to a desk audit, that entity has 10 business days to provide the requested documentation in order to complete the audit (U.S. Department of Health & Human Services, 2016). These documents are very well laid out, and provide the auditor with question

and answer scenarios, as well as what to look for in each document to ensure compliance (See Appendix). Providing this kind of guidance for remote audits, although it was not initially intended to fully replace an on-site audit, is incredibly valuable during this time.

When requesting documents to be reviewed, it would be a good security measure to acquire these documents through a secure sharing portal to ensure their integrity. Additionally, points of contact based on the type of audit being conducted should help save some of the auditor's time. Although these desk audits will not be as in-depth as a standard, on-site audit, the documentation reviews performed by the auditor should be adequate for them to verify that a procedure is being followed via a video call or other remote session.

If a website is being maintained by the company or organization being audited, online documents and procedures for reviewing, updating and sharing those documents should be reviewed (See Appendix). The auditor should also review these documents in a similar fashion as discussed above.

Overcoming PCI Barriers and Drawbacks

Troy Leach, the Senior Vice President, Engagement Officer, PCI SSC, says "All measures should be taken to ensure the results of a remote assessment are commensurate with those resulting from an onsite assessment" (Leach, 2020). This may, unfortunately, require additional time despite the auditor working in a location that they are comfortable with. This may be due to the added time between communications and gaining proper, reliable remote access to systems being audited. Unfortunately, PCI still requires observation of some compliance elements such as network and system configurations. This can be done fairly easily while remote by creating network diagrams or remoting into a particular device and view how it is configured.

Leach recognizes the fact that auditors are unable to travel to perform on-site audits (Leach, 2020). He states that there should be no negative effects of remote auditing, and that "…special precautions may be necessary to ensure that personnel being interviewed and system components being examined are the same as if the assessor was onsite" (Leach, 2020). Auditors should be using video calls when performing employee interviews in order to get as close to an in-person interaction as possible.

When observing different procedures or implementations of security controls, the collection of evidence must provide the same level of assurance as if it was an on-site audit. In order to achieve this, special accommodations may need to be made to ensure that video calling is supported by the entity being audited in order to achieve maximum clarity between the parties involved.

Chapter 4: Conclusion and Suggestions for Further Study

Due to the impact COVID-19 has had around the world, many people are required to stay home and work remotely, causing in-person or on-site audits to be less likely to occur. The suggestions provided by compliance governing agencies when it comes to remote audits is limited as this is the first time a global pandemic has occurred during this age of technology.

Remote audits are generally frowned upon by these agencies due to their nature of being incomplete or inaccurate. However, even during this age of technology, there are limited resources available for auditors and auditees to properly go about performing a remote audit.

In the future, as technology advances, compliance requirements, and how to verify compliance, should adjust with technology. The amount of analysis and research in this space of IT audits before the onset of the pandemic was quite limited. During the course of the past few months, many resources provided by audit firms and compliance agencies have provided

guidance on how to approach a remote audit successfully. Unfortunately, this could have been something considered long ago.

Being vigilant and proactive is the key here. Understanding what may happen in the future, and adjusting to that possibility, within reason, will not only help advance society, but could increase the overall mood of humanity while working remotely.

Nowadays, more and more people are working remotely for the convenience and savings, but many compliance requirements are not approached with this mindset. Working remotely is possible through many new advancements in technology, and this industry, being so tightly woven in with technology, should acknowledge that and address it accordingly. My hope is that people who want to work remotely, can. More standards for remote work should be put into place in order to achieve this.

References

Center for Disease Control and Prevention. (2020, March 20). *What you need to know about coronavirus disease 2019 (COVID-19)*. Retrieved from Center for Disease Control and Prevention: https://www.cdc.gov/coronavirus/2019-ncov/downloads/2019-ncov-factsheet.pdf

Dias, R. (2017, December 8). *The 5 factors of authentication*. Retrieved from Medium: https://medium.com/@renansdias/the-5-factors-of-authentication-bcb79d354c13

Fein, A., Anderson, T., Canter, L., & Skeath, C. (2020, March 20). *COVID-19 cybersecurity advice: FTC, NIST, and CISA release guidance on secure teleworking and Critical infrastructure jobs*. Retrieved from Inside Privacy: https://www.insideprivacy.com/covid-19/covid-19-cybersecurity-advice-ftc-nist-and-cisa-release-guidance-on-secure-teleworking-and-critical-infrastructure-jobs/

Fidler, D. P. (2020, March 30). *Cybersecurity in the time of COVID-19*. Retrieved from CFR: https://www.cfr.org/blog/cybersecurity-time-covid-19

Gallo, I. (2020, January 27). *What are benefits and barriers when performing remote audits?* Retrieved from Advisera: https://advisera.com/9001academy/blog/2020/01/27/remote-audit-benefits-and-barriers-for-iso-standards/

HIPAA Journal. (n.d.). *HIPAA compliance checklist*. Retrieved from HIPAA Journal: https://www.hipaajournal.com/hipaa-compliance-checklist/

Hirsch, J. L. (n.d.). *Telecommuting: Security policies and procedures for the "work-from-anywhere" workforce*. Retrieved from Global Information Assurance Certification Paper:

https://www.giac.org/paper/gsec/323/telecommuting-security-policies-procedures-work-from-anywhere-workforce/100918

Lapakko, D. (2007, January). *Communications is 93% nonverbal: An urban legend proliferates*. Retrieved from Minnesota State University: College of Education: https://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=1000&context=ctamj

Leach, T. (2020, March 11). *Remote assessments and the Coronavirus*. Retrieved from PCI Security Standards Council: https://blog.pcisecuritystandards.org/remote-assessments-and-the-coronavirus

Maddox, T. (2018, April 3). *How to write a good security policy for BYOD or company-owned mobile devices*. Retrieved from ZDNet: https://www.zdnet.com/article/how-to-write-a-good-security-policy-for-byod-or-company-owned-mobile-devices/

National Institute of Standards and Technology. (2019, December 9). *Back to basics: Multi-factor authentication (MFA)*. Retrieved from NIST: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

NIST. (n.d.). *Computer incident response team (CIRT)*. Retrieved from NIST: Computer security response center: https://csrc.nist.gov/glossary/term/computer_incident_response_team

PCI Security Standards Council. (2008). *PCI quick reference guide*. Retrieved from PCI Security Standards: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

PCMag. (n.d.). *Mobile device management*. Retrieved from PCMag Encyclopedia: https://www.pcmag.com/encyclopedia/term/mobile-device-management

Risktec. (2005). *Risk-based decision making*. Retrieved from Risktec Knowledge Bank: https://www.risktec.tuv.com/wp-content/uploads/2018/09/risk-based-decision-making.pdf

U.S. Department of Health & Human Services. (2016, December 1). *HIPAA Privacy, Security, and Breach Notification Audit Program*. Retrieved from Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

U.S. Department of Health & Human Services. (2016). *OCR 2016 HIPAA desk audit guidance on selected protocol elements*. Retrieved from U.S. Department of Health & Human Services: https://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

U.S. Department of Health & Human Services. (2020, March). *COVID-19 & HIPAA a bulletin limited waiver of HIPAA sactions and penalties during a nationwide public health emergency*. Retrieved from U.S. Department of Health & Human Services: https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf

Appendix

OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
P55	Privacy	§164.520 (a)(1) & (b)(1)	Notice of Privacy Practices Content requirements	Does the covered entity have a notice of privacy practices? If yes, verify the current notice contains all the required elements. • Header 164.502(a)(1) – Permitted uses and disclosures Does the covered entity include in its notice a description of the following permitted uses and disclosures? • To the individual • For treatment, payment, or health care operations (with at least one example of a use and disclosure for each purpose) • For public health and safety issues • For research purposes • To comply with the law • To respond to organ and tissue donation requests • To work with a medical examiner or funeral director • To address workers' compensation, law enforcement and other government requests • To respond to lawsuits and legal actions. Pursuant to an agreement under, or as otherwise permitted by § 164.510 – Uses and disclosures requiring an opportunity to agree or object: (i) For facility direct (ii) For involvement in the individual's care and notification purposes. 64.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required Does the covered entity include in its notice the following uses and disclosures for which an authorization or opportunity to agree or object is not required: • As required by law • For public health activities • Disclosures about victims of abuse, neglect or domestic violence • For health oversight activities • Disclosures for judicial and administrative proceeding • Disclosures for law enforcement purposes • About decedents • For cadaveric organ, eye or tissue donation purposes • For research purposes • To avert a serious threat to health or safety • For specialized government functions. 164.514 (f)(1) – Standard: Uses and disclosures for fundraising. Required Statements: • A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization • A statement that the individual may revoke an authorization If the covered entity intends to engage in any of the following activities, separate statements for certain uses or disclosures involving fundraising o A statement that genetic information cannot be used to decide whether coverage can be given or at what price o A statement that information can be disclosed to a plan sponsor for plan administration. Individual rights: Does the notice of privacy practices contain a statement of the individual's rights and a description of how the individual may exercise the following rights:	Upload a copy of all notices posted on website and within the facility, as well as the notice distributed to individuals, in place as of the end of the previous calendar year.	Q; Do you wish to receive pictures of the Notices hanging on the walls in addition to receiving the uploaded paper copies? A; Yes. Please ensure that the text is readable. Q: Is Request for NPP duplicate? one request under "Right to Access" (subsection 4, and then under "Notice of Privacy Practices" subsection 1 A: Yes, the entity Notice(s) of Privacy Practices is requested in two places within the Privacy section. The documents will be reviewed for overall compliance with the content requirements for Notice in P55.1. In P65.4, the the audit will assess whether the access policies and procedures are congruent with the notice description of the access right. Q: How about NPP translated version. would you like us to submit that as well? A: Yes, provide all versions of the Notice of Privacy Practices

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
				• Obtain a copy of the individual's health and claims records • Request that the covered entity correct health and claims records • Request confidential communications • Ask the covered entity to limit what it uses or shares • Obtain a list of those with whom the covered entity has shared information • Obtain a copy of the privacy notice • File a complaint with the entity and the Secretary of HHS CE Duties: Does the covered entity notify individuals of its legal duties with respect to their PHI, which are: • To maintain the privacy and security of their PHI • To notify affected individual(s) if a breach occurs that compromised the privacy or security of their information • To follow the duties and privacy practices described in the notice • The covered entity will not use or share information other than as described here unless authorized in writing. Authorization may be revoked at any time, in writing. Does the notice state that disclosures will be made: • to the Secretary of HHS for HIPAA rules compliance and enforcement purposes Complaints: The notice must contain a statement that the individual has a right to complain to the CE and to the Secretary if they believe their privacy rights have been violated with a brief description of how to file a complaint with the covered entity and a statement of no retaliation for filing a complaint. Contact: The notice must contain the name or title and telephone number of a person or office to contact for further information. Effective date: The notice must contain an effective date.		
P58	Privacy	§164.520 (c)(3)	Provision of Notice - Electronic Notice	Does a covered entity that maintains a web site prominently post its notice? Does the covered entity implement policies and procedures, if any, to provide the notice electronically consistent with the standard? Determine whether the entity maintains a web site. If so, observe the web site to determine if the notice of privacy practices is prominently displayed and available. An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices. If the covered entity provides electronic notice (such as by linkage to a web page or e-mail), obtain and review the policies and procedures regarding the provision of the notice of privacy practices electronically and the process by which an individual can withdraw their request for receipt of electronic notice. If the covered entity provides the notice of privacy practices by e-mail or other electronic form, obtain and review the documentation of the agreement with the individual to receive the notice via e-mail or other electronic form. Inquire if covered entity has experienced failures when trying to provide the notice of	Upload the URL for the entity web site and the URL for the posting of the entity notice, if any. If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically. Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form.	Q: Can you provide clarity on the electronic request questions in privacy section - is that direct access to the EHR or does providing access to the portal suffice? A: If you review the protocol posted online and examine the document request, you will see that this question pertains to provision of the notice of privacy practices electronically. This question does not involve EHRs.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
				privacy practices by e-mail. If the covered entity has experienced e-mail transmission failures, obtain and review its attempts to provide a paper copy of the notice via alternative means (e.g., mail).		
P65	Privacy	§164.524 (a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)	Right to access	How does the covered entity enable the access rights of an individual? Inquire of management. Obtain and review policies and procedures in place for individuals to request and obtain access to PHI and to determine whether they comply with the mandated criteria. Determine whether policies and procedures adequately address circumstances in which an access request is made for PHI that is not maintained by the covered entity, per 164.524(d)(3). Obtain and review the notice of privacy practices. Identify whether an individual's right to access in a timely manner is correctly described in the notice. Obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied. • Verify that access was provided consistent with the policies and procedures • Verify that requests for access were fulfilled in the form and format requested by the individual if the covered entity can readily produce the PHI in the requested form and format, including electronic format • Determine whether response was made in a timely manner. (e.g., within 30 days of request receipt, unless extension provided consistent with 164.524(b)(2)(ii)) • Determine whether fee charged meets the reasonable cost based fee requirement of 164.524(c)(4) • If the entity denied access to certain PHI, determine whether it provided access to other PHI requested by the individual that was not excluded, per §164.524(d)(1) • For cases for which access was denied, assess whether the denials, and any reviews made pursuant to individual request, were consistent with the policies and procedures. Inquire of management whether the covered entity has used a standard template or form letter for requesting access to protected health information. If the covered entity has used a standard template or form letter for access, obtain and review the document and determine whether it includes the requirements.	Upload policies and procedures for individuals to request access to protected health information (PHI). Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year. (Remove PHI if possible) Upload all documentation related to the last five access requests for which the entity extended the time for response to the request.(Remove PHI if possible) Upload any standard template or form letter required by or used by the CE to document access requests.	Q: On P65 do you want acccess requests from individual only or include access requests from other entities authorized by the individual? A: The individual right to access includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Therefore requests by the individual to transmit a copy to a designated person should be included. However, requests for disclosures of PHI that are merely authorized by the individual are not considered an exercise of the access right and should not be included. Please see http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs Q; Regarding Access Requests, are you expecting copies of the DRS that we provided to the patient? We believe it should not be included. A: No, audited entities do not need to submit the the DRS provided to the individual in response to an access request. Q; P65 Right to Access- If the access request is from a personal representative on behalf of the patient, are we required to submit documentation proving the personal representative's authority? A: P65 requires all documentation related to the specified access requests. That would include documentation of personal representative status when such status is relevant to the handling of the request. Q; Could you please define "access request?" A: See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs and http://www.hhs.gov/hipaa/for-professionals/training/index.html Q: In regards to access request, this in regards to just those involved in a breech or all release of information for all including insurances and patients? A: The requests for information about compliance with the access requirements of the Privacy Rule are distinct and separate from the information requests regarding compliance with the Breach Notification Rule. Please review the relevant provisions of the HIPAA rules (see protocol for citations) to help you understand the distinction. Q; Is the right to access about giving the individual information

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
						about who has seen the record? A: See http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html for more information about the the right to access. The individual right to access their protected health information is not the same as their right to request an accounting of disclosures of their information. Q: Regarding the right to access: what documentation is to be uploaded to respond to "all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year." A: There is no one required process for fulfilling access requests under HIPAA and therefore we are not able to specify all the possible documentation. Generally, entities should have a record of the requests they have received and filled in 2015. Do not submit copies of the PHI provided to the individual in response to the individual's request. Q: In a physician office, would access request apply to all requests for medical records by a patient? A: Generally, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, and the covered entity must permit individuals to request access to that information. Access requests include requests for medical records made by patients that fit this description. See the OCR access guidance http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Q: Is an "access request" the whole record set? What about a request for a single record or just certain payments or just a explaination(s) of benefits (EOB(s))? A: An access request may be for the entire designated record set but is not limited to that. An individual may request access to portions of the record, such as a medication list, a lab report or other information. See the OCR access guidance http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Q: Can you provide an example of what would be "evidence of fulfillment" with respect to right to access (P65). For example, if our access request form includes a section where a workforce member signs off that he or she has completed or responded to the access request and it is signed and dated...would that work? A: Yes, that is an example of "evidence of fulfillment." Other entities may have other types of documentation.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
S2	Security	§164.308 (a)(1)(ii)(A)	Security Management Process -- Risk Analysis	Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits? Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event. If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.	Upload policies and procedures regarding the entity's risk analysis process. Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification. Consistent with 164.316(b)(2)(ii)-(iii), upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated. Upload documentation of the current risk analysis and the most recently conducted prior risk analysis. Upload documentation of current risk analysis results.	Q; Can we submit documentation of an annual risk assessment performed by third party? A: Yes, a covered entity may use a business associate to conduct the risk analysis and the results may be submitted in response to S2 (1), Security Rule Risk Analysis. Q; If we recent conducted a risk analysis, but the report is in draft form - should we submit the draft, as well as the prior finalized risk analysis? A: Where entities are asked to provide documentation for a specified time period (e.g., current, previous calendar year, 6 years ago) they should submit documentation that reflects what is in place and in use during the time frame specified. Q: Can you please clarify the difference between S2 question 1 and 5? A: Question 1 is asking for the results of the risk analysis. Question 5 is asking for documentation that the risk analysis was conducted. Q: For the SR S2 Document request, is the request to upload documentation of CURRENT risk analysis results refering to 2015? A: Current means what is in place and in use as of the date of the notification letter you received--July 11, 2016. Q: Can you please be more specific about 6 previous years of risk assessments - that's a lot of documentation? I am only seeing request for 6 previous years of policies - can you repeat again where this request is? A: Question S2.3 and S3.2 both ask for documentation that the subject policies and procedures were in place and in effect 6 years prior to the date of the notification letter--i.e, July 11, 2010. The questions do not require documentation of what was in effect during the intervening years. Q: What would be an example of proof that the risk analysis was available to the workforce members? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Q: For SR audits, do all the Security Policies and documentation need to be submitted or is there a specific list that you can provide.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						A: Refer to the audit protocol for more information about the audit inquiry, which may help you determine what documentation to submit. Q: Do you truly want us to upload our current risk analysis to the portal? This would list vulnerabilities in our system (which we are working to resolve) and they would possibly become public knowledge under the FIOA? A: We believe that a risk analysis submitted by a CE for the audit to be covered by the following exemption from FOIA: Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged. Q: If the most current risk analysis is not that "current", do you recommend having one performed within the time frame allotted and submit this? If so, do you recommend having it done internally, or third party? A: No, do not create a new analysis. Current means as of July 11, 2016, not later. Q: Please explain what you are looking for in S2 Number 2. Are you looking for training records? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Training records are not responsive to the request. Q: Would the absence of a HIPAA security risk analysis be viewed as a "significant threat" to PHI potentially triggering an enforcement action? A: Please include in the comment field a rationale for why a risk analysis will not be submitted Q: For clarification on Security audit, you listed 164.308 at beginning of slides and then 164.316 in the sample audit -- are you asking for only one area A: 164.316 is the provision that requires covered entities and business associates to implement reasonable and appropriate policies and prcodures to implement the required safeguards (e.g. for 164.308, risk analysis and risk management); to maintain documentation of them for 6 years; and to review that documentation periodically and update as needed.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						Q: Our security policies have an effective date as well as a historical record of annual revisions. I assume that will suffice for the six year requirement of what "was" in place? A: Yes Q: Since the questions seem similar in nature, we discerned that the S2 questions were about the documentation of policy/procedures, and S3 is about the "what you actually did" ... is this correct? A: The subject of S2 is risk analysis--the conduct of an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. The subject of S3 is the risk management plan implemented to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. Documentation of the entity's policies and procedures is required as well as documentation showing that the activities required by the policies and procedures have been conducted. Q: If the current risk analysis is 2015, the most recenlty conducted prior risk analysis is 2014? A: Current means what is in place and in use as of the date of the notification letter you received--July 11, 2016. The most recently conducted prior risk analysis would be the one conducted prior to the current one. Q: To validate S2.2, would a simple organization chart of the security organization suffice? Maybe include committee minutes? A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Another example could be committee meeting minutes documenting the efforts the entity has in place to ensure appropriate personnel have appropriate access to the documentation required to implement the procedures of the security rule to which the documentation pertains. To the extent that an organizational chart could assist in the identification of individuals or groups identified in the supporting documentation, such organizational information should also be submitted.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
S3	Security	§164.308 (a)(1)(ii)(B)	Security Management Process -- Risk Management	Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.	Upload policies and procedures related to the risk management process. Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification. Consistent with 164.316(b)(2)(ii)-(iii), upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated. Upload documentation demonstrating the efforts used to manage risks from the previous calendar year. Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment. (Upload documentation demonstrating that current and ongoing risks reviewed and updated.)	Q: Some of the documentation around risk analysis and management seems to apply to several of the different layers of request. Should we upload to each individual question? A: The questions each ask for different documentation; of existing policies and procedures, or evidence that an analysis was conducted or risks addressed, or the results of those actions. Q: What constitutes appropriate documentation for questions that relate to security measures/recommendations being given to and reviewed by appropriate personnel? A: Management approval of plans and/or projects to implement security measures to remediate or mitigate identified risks. Such approvals could take the form of management signatures on risk management plans or other indicators of approval for implementation and/or documentation showing approval and funding of specific projects to implement security measures. Q: Could you provide an example of documentation that would demonstrate people had access to what they needed? This is in the Security section. A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access. Q: Risk assessments are a daily ongoing process and the technical controls implemented are vast. How much evidence is enough or not enough? We want to make sure we strike the right balance. A: The amount of evidence required to show compliance with the risk analysis implementation specification is whatever amount is necessary to show that an accurate and thorugh assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of all of the ePHI the entity creates, receives, maintains or transmits has been conducted. Q: The security request to provide documentation the the proper people had access to the information is confusing. Can you please clarify what is being request? Are you looking to see that employees of a CE have access to policies? Or are you asking if the authorized individuals in management are reviewing security risk assessments

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Questions / Answers
						A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access.

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
BNR12	Breach	§164.404 (b)	Timeliness of Notification	§164.404(b) Timeliness of Notifications Were individuals notified of breaches within the required time period? Inquire of management. [Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach.]--*Not included in current audit* Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).	Upload documentation of five breach incidents for the previous calendar affecting fewer than 500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.	Q; Under BNR13 Content Notification, you ask for an upload of a written notice sent to affected individuals. If we do not have a breach incident affecting over 500 individuals, should we identify this as not applicable or provide you with a letter from a notice of breach under 500? A: If the entity has not reported a breach involving 500 or more individuals in the specified time period, the entity should search for and provide the evidence from breaches in previous time periods until the requested number of events is reached. If the entity has reported in total fewer than 5 breaches involving 500 or more individuals, the entity may attest to it using the comment field. Q; If we do not have the number of incidents requested and have to go back, do we need to provide the ones that are within the time frame requested in addtion to the ones in the previous time frame not requested? A: Yes. If you do not have documentation of the full number of events in the specified time interval, search back and include additional events in previous time intervals until you are able to compile the specified number. If you have not experienced the total number of requested events, be sure to attest to that in your submission. Q: BNR12: Can we enter this information into an Excel spreadsheet? Or do you need the documentation for each data element? A: A spreadsheet would be helpful, but all the specific documentation requests must be met--which likely will require additional documentation. Q: we had a incident in December but once the audit was concluded we reported in January 2016. can we count that for 2015? A: You may reach your own determination of what to include in documentation "for the previous calendar year" (i.e., 2015).

Element #	Audit Type	Section	Key Activity	Audit Inquiry	Document Request List	Question / Answers
BNR13	Breach	§164.404 (c)(1)	Content of Notification	§164.404(c)(1) Content of Notification Evaluate if the specifications at §164.404(c) are met. Inquire of management whether the covered entity has used a standard template or form letter for notification to individuals for all breaches or for specific types of breaches. If the covered entity has used a standard template or form letter for breach notification, obtain and review the document. Evaluate whether it includes this section's required elements. Obtain and review a list of breaches, if any, in the specified period and documentation of written notices sent to affected individuals for each breach. Select notifications sent to individuals to be reviewed and verify that the notices include the elements required by §164.404(c). [Does the covered entity have policies and procedures for providing individuals with notifications that meet the content requirements of §164.404(c)? Inquire of management; obtain and review policies and procedures.] Not included in current audit	Upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year. Upload a copy of a single written notice sent to affected individuals for each breach incident. If the entity used a standard template or form letter, upload the document.	Q: In BNR 12 and 13, can you provide an example or elaborate on appropriate "sampling methodologies"? A: You may ignore the phrase "using sampling methodologies." This phrase will be deleted from the document submission pages. Q; For BNR #3 are you requesting all breach letters sent in the previous year or just one letter sent as an example? A: BNR13.3 asks for a single copy of the notification sent to individuals for each event. So if you have experienced three breaches, provide one letter for each breach. Q: We had five HIPAA incidents (assumed breaches) in 2015. However, if we determined after an analysis that notification was not required for all breaches in 2015, would you like us to provide a notification from 2014? A: We are asking for documentation for breaches for which notification was provided. If you did not have a sufficient number for 2015 to meet the request, please add incidents from previous years until you reach 5 total. Q: BNR13 -3 copy of single written notice-is this for 500< only? A: BNR13.3 asks for a single copy of the notification sent to individuals for each breach event, regardless of size. So if you have experienced one breach under 500 and two over 500, these count as three breach events, and you would provide one letter for each. Q: we are small pharmacy and only sent out one breach notification to a patient ...should we just upload that one ? A: If you only have a total of one breach notification, attest to that in the comment box and provide the required documentation for that one notification. Q: Breach definition: would that include all the unpermitted/unintended releases that were not reported? How about cases that were only reported to States? A: The subject of this section is breach notification. Please provide information regarding breaches for which you determined notification was required by the HIPAA Breach Notification Rule. State law reporting is not the subject of this audit. Q: We are an entity with one tax ID, and many sites. One of our sites was identified for the audit, and we report the HIPAA breaches as an entity. We have only had one breach for that particular site that was identified. Do I just enter that one breach? SHould I use all sites as response for the breach examples? A: Use your best judgement. In general, notifications were sent to the location of interest. If the address was to a headquarters, reply based on the entire entity.