Understanding Mitigation of Cybercrime Through Adherence to HIPAA Regulatory Requirements and Organizational Best Practices

THE BALDWIN REGULATORY
COMPLIANCE COLLABORATIVE

Table of Contents

BRP | THE BALDWIN REGULATORY COMPLIANCE COLLABORATIVE

INTRODUCTION

On February 5, 2016, Hollywood Presbyterian Medical Center was the victim of a vicious cyberattack. Infecting the hospital's entire network, the hospital's staff was forced to resort to pen and paper for recordkeeping for nearly a week while hospital security teams and administrative staff negotiated with their cyber attackers. The attackers deployed a strain of malware known as ransomware, seizing control of the hospital's computer systems and device controls. After five days of negotiations, the hospital negotiated the demanded ransom down from over a million dollars to $17,000 and paid the ransom (in bitcoin). The hospital system did not contact local or federal law enforcement officials until after thy had already paid the ransom, which was obviously not recoverable.

"Malware," or malicious software, is generally designed to gain access or to damage a computer without the knowledge of the owner, empowering the intrusive application to acquire as much data as possible prior to discovery. However, in the instance of ransomware, a specific strain within the broad category of malware, the cybercriminal specifically designs its applications to notify the recipient of infection upon the occurrence of infiltration. Having imbedded itself within the user's station, network, or cloud, the malware agent restricts access to files and technical operations, an international design aspect calculated to impair both operation and remediation attempts throughout the attack. Thereafter, the owner is delivered a cryptic digital message demanding the payment of a hefty "ransom" to be paid within a specified (and short) period, supposedly in exchange for a decryption key (which may or may not be delivered or even effective), else all infected files and systems are lost forever.

The prevalence and scope of ransomware exploded in 2021, as two-thirds of mid-sized organizations worldwide were targets and average ransom payouts saw a five-fold increase.[1] Average ransom payments reached $812,000 during 2021, compared with $170,000 the prior year.[2] The latest prediction is that global ransomware damage costs will soon reach $20 billion – which is 57X more than the resulting costs in 2015.[3]

While no single defensive strategy will defeat the ransomware phenomenon, a HIPAA-centric defensive strategy provides an employer plan sponsor with the means to identify, segregate, and potentially exterminate ransomware infiltration prior to the malware's proliferation with a user's network; thus, inhibiting the potential for unlawful and/or unauthorized exfiltration of user's data. In this way, while a single device may become corrupted, savvy device operators are able to reduce the potential for an attack to infect the user's entire network. Consequently, the target organization's net experience is the loss of a single device worth of data; a considerable improvement, considering the alternative of an entirely debilitated network. When paired with even the most minimal security procedures, the knowledge of a device operator to proactively identify the signs of an infiltration and to remove the infected device from the network can help to save an organization big bucks and substantial hardship.

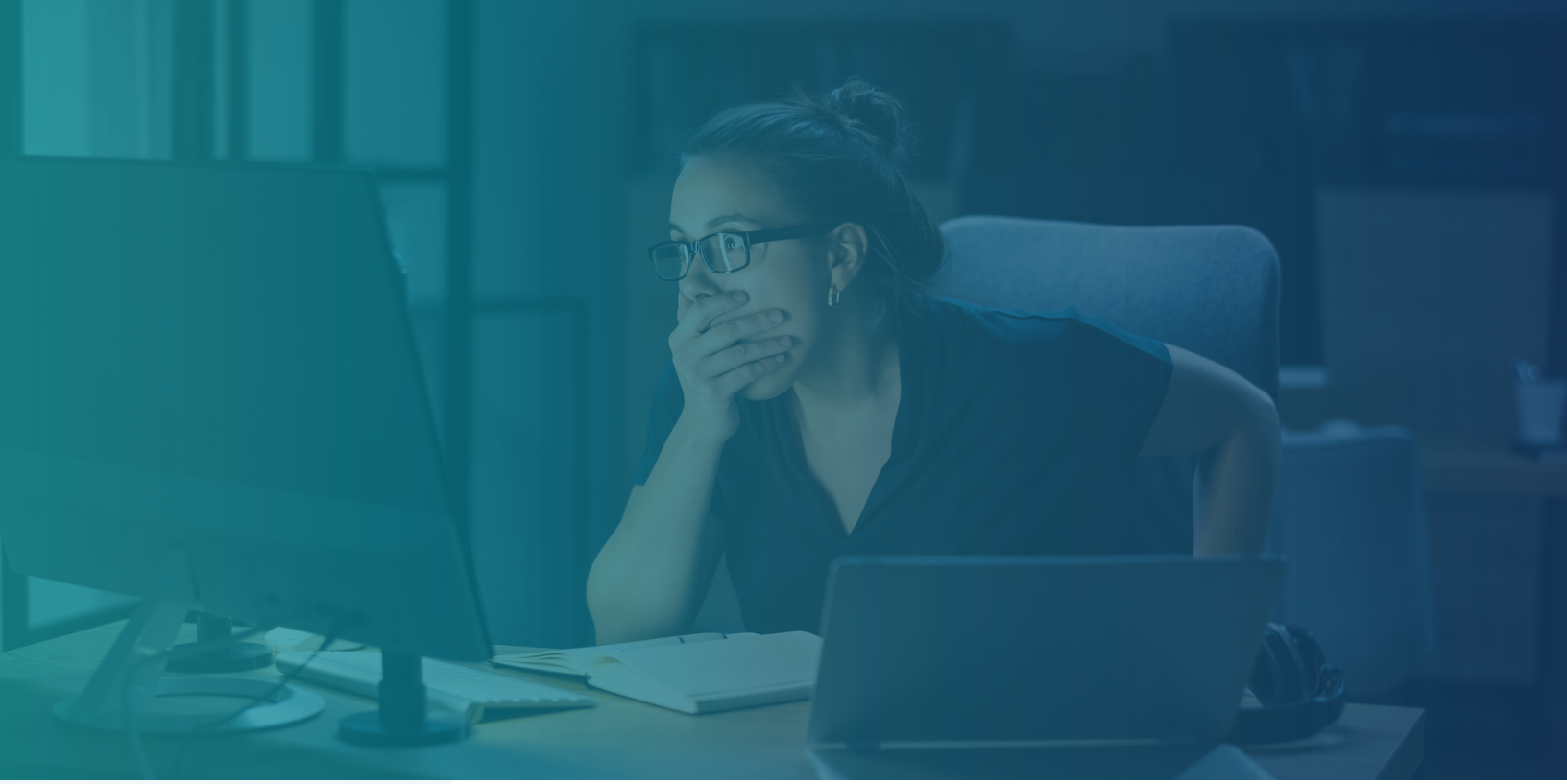
HIPAA-CENTRIC DEFENSIVE STRATEGIES INCREASE RANSOMWARE DEFENSIVE PREPAREDNESS

While no single defensive strategy will defeat the ransomware phenomenon, a HIPAA-centric defensive strategy provides an employer plan sponsor with the means to identify, segregate, and potentially exterminate a ransomware infiltration prior to the malware's proliferation within a user's network. In this way, while a single device may become corrupted, savvy device operators are able to reduce the potential for an attack to infect the user's entire network. Thus, the victim organization's net experience is the loss of a single device worth of data; a considerable improvement to the alternative of an entirely debilitated user network. When paired with even the most minimal security procedures, the knowledge of a device operator to proactively identify the signs of an infiltration and to remove the infected device from the network can help to save an organization substantial dollars and hardships.

Unless ransomware is detected and propagation halted by an entity's malicious software protection or other security measures, an entity would typically be alerted to the presence of ransomware only after the ransomware has encrypted the user's data and alerted the user to its presence to demand payment. However, in some cases, an entity's workforce may notice early indications of a ransomware attack that has evaded the entity's security measures. HIPAA's requirement that an entity's workforce receives appropriate security training, including training for detecting and reporting instances of malicious software, can thus assist entities in preparing their staff to detect and respond to ransomware. As identified by the United States Department of Health & Human Services' Office for Civil Rights (ORC), some of the user's identifiable indicators of a ransomware attack could include:

- A user's realization that a link that was clicked on, a file attachment opened, or a website visited that may have been malicious in nature;
- An increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- An inability to access certain files as the ransomware encrypts, deletes and re-names and/or re-locates data; and
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by Information Technology (IT) personnel via an intrusion detection or similar solution).

If an entity believes that a ransomware attack is underway, either because of indicators similar to those listed above or other methods of detection, the entity should immediately activate its security incident response plan (discussed below). This plan should always include measures to isolate infected computer systems in order to halt the propagation of the infiltration. Additionally, it is recommended that an entity infected with ransomware contact their local Federal Bureau of Investigation (FBI) or United States Secret Service field office. These Federal agencies work with Federal, state, local and international partners to pursue cyber criminals globally and assist victims of cybercrime.



Notwithstanding the foregoing, and even with adequate, reoccurring security training and advanced strategic planning, ransomware will occasionally make it past some users and on to their network. In those situations, the best response for an employer plan sponsor is to respond to the attack according to HIPAA best practices. The HIPAA best practices approach accomplishes two important objectives: first, the ransomware defense works to minimize the impact of an infiltration; and second, it is the best way to mitigate participant-based administrative liability arising from such an infiltration event.

Minimizing the impact of a ransomware attack is always the first priority of an infiltration victim. In this context, minimization means many different things. Obviously, minimization of the proliferation of the strain is first and foremost. However, minimization also refers to the mitigation of participant-based administrative liability arising from an infiltration event. Remember that HIPAA provides only administrative remedies; thus, a participant in an employee benefit plan that experiences a privacy breach event has the sole and exclusive remedy of filing an administrative complaint with OCR.

Upon receipt and evaluation of a HIPAA-based privacy complaint, the first thing OCR will assess is whether, and to what extent, the employer plan sponsor has performed its HIPAA defense and response obligations, ranging from risk assessments, development of appropriate policies and procedures, and conducting associate and officer trainings, and breach notifications to participants, the media, and the Secretary of Health and Human Services (HHS). Having performed these essential operations, the employer plan sponsor reduces, and in some situations, entirely disposes of the participant liability potential, via satisfaction of its HIPAA-related (and required) tasks. In this way, the HIPAA best practices approach guarantees an employer plan sponsor will not face unnecessary participant liability associated with remedying an already frustrating infiltration event.

HIPAA-CENTRIC DEFENSIVE STRATEGIES LAY THE FOUNDATIONS FOR SUCCESSFUL DETERRENCE AND RESPONSE TO RANSOMWARE ATTACKS

Embedded within HIPAA Rules are a set of specific security guidelines to inform and direct e-PHI protections for covered entities, including plan sponsors, healthcare providers, and healthcare clearinghouses. Referred to implementation specifications, the sum set of forty-two (42) specifications provides an employer with a roadmap to both compliance and security assuredness. Of the set of implementation specifications, each is identified as either of an "addressable" or a "required" specification. The former refers to specifications the covered entity must consider for enterprise implementation, while the latter refers to mandatory specifications that must be implemented by each covered entity. Implementation specifications are divided into three categories of safeguards, referred to as HIPAA's technical; physical; and administrative safeguards or firewalls. (See following Charts Numbered 1-3 for complete list of implementation specifications.)

CHART NUMBER 1:
Administrative Safeguards

Standards	Sections	Implementation Specifications (R)=Required; (A)=Addressable	
Assigned Security Responsibility	CFR § 164.308(a)(2)		(R)
Business Associate Contracts & Other Arrangements	CFR § 164.308(b)(1)	Written Contract or Other Arrangement	(R)
Contingency Plan	CFR § 164.308(a)(7)	Applications & Data Criticality Analysis	(A)
		Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operations Plan	(R)
		Testing & Revision Procedures	(A)
Evaluation	CFR § 164.308(a)(8)		(R)
Information Access Management	CFR § 164.308(a)(4)	Access Authorization	(A)
		Access Establishment & Modification of Access	(A)
		Isolate Healthcare Clearinghouse Functions	(R)
Security Awareness & Training	CFR § 164.308(a)(5)	Log-in Monitoring	(A)
		Password Management	(A)
		Protection from Malicious Software	(A)
		Security Reminders	(A)
Security Incident Procedures	CFR § 164.308(a)(6)	Response & Reporting	(R)
Security Management Process	CFR § 164.308(a)(1)	Information System Activity Review	(R)
		Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
Workforce Security	CFR § 164.308(a)(3)	Authorization and/or Supervision	(A)
		Termination Procedures	(A)
		Workforce Clearance Procedure	(A)

CHART NUMBER 2:

Physical Safeguards

Standards	Code Section(s)	Implementation Specifications (R)=Required; (A)=Addressable	
Device & Media Controls	CFR §164.310(d)(1)	Disposal of e-PHI	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup & Storage	(A)
Facility Access Controls	CFR § 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control & Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Security	CFR § 164.310(c)		(R)
Workstation Use	CFR § 164.310(b)		(R)

CHART NUMBER 3:

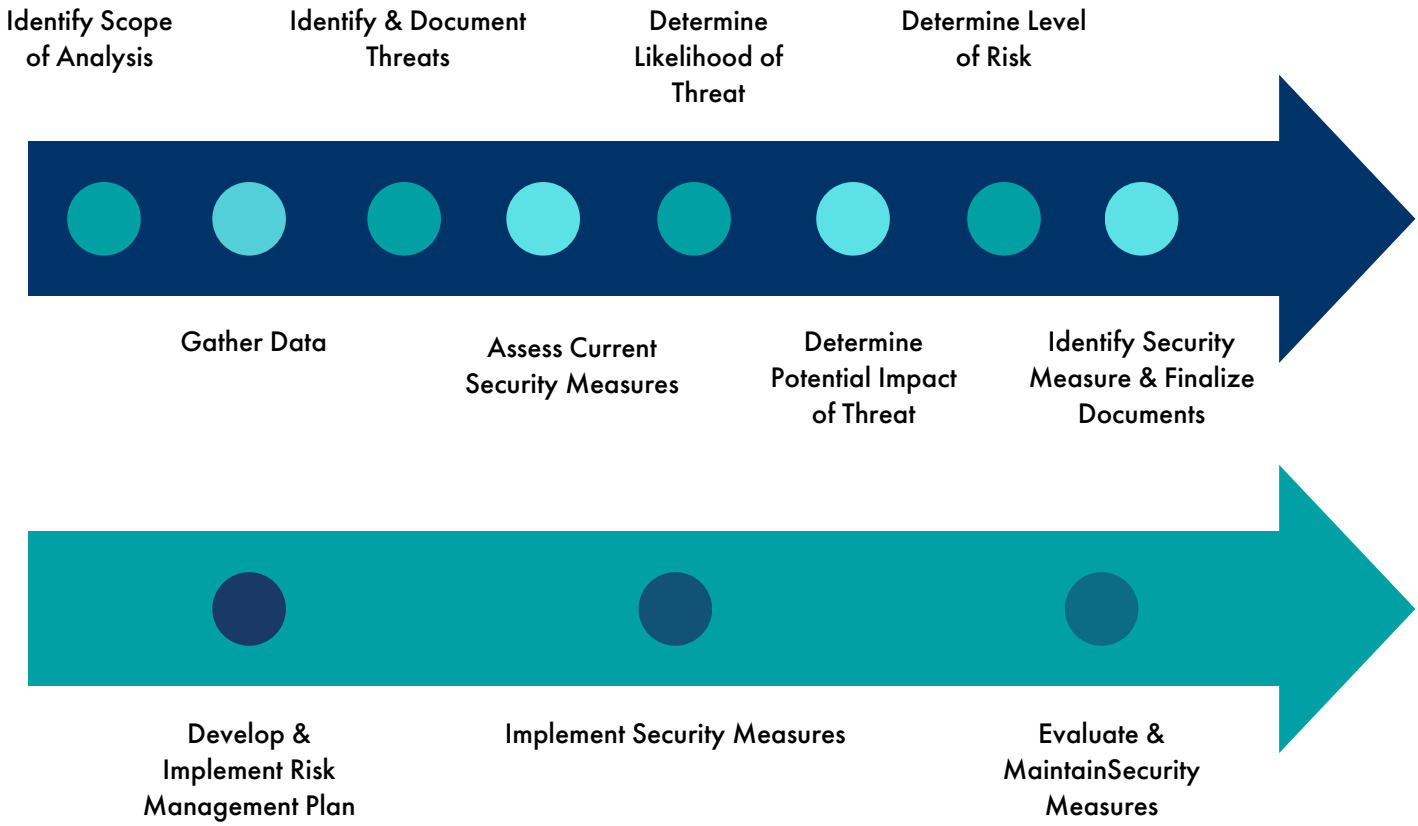
Technical Safeguards

Standards	Sections	Implementation Specifications (R)=Required; (A)=Addressable	
Access Controls	CFR § 164.312(a)(1)	Automatic Logoff	(R)
		Encryption & Decryption	(A)
		Emergency Access Procedure	(R)
		Unique User Identification	(R)
Audit Controls	CFR § 164.312(b)		(R)
Integrity	CFR § 164.312(c)(1)	Mechanism to Authenticate e-PHI	(A)
Person or Entity Authentication	CFR § 164.312(d)		(R)
Transmission Security	CFR § 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Performance of the implementation specifications is actually a two-part process. In part one, the covered entity performs a risk analysis of each specification (either required or addressable), making a determination of appropriateness for the particular entity. This is referred to as the “risk analysis” or the “observations phase.” In part two, the covered entity actually performs the exercise of installing each individual implementation specification according to HIPAA best practices and the individual resources and utilities of the covered entity as an enterprise. This phase is referred to as “risk management” or the “actions phase.”

When performing risk analysis and risk management, it is important to keep in mind two distinct constructs that pervade all implementation specifications: first, the concept of neutrality; and second, the concept of scalability. Neutrality relates to the technology utilized for the satisfaction of the implementation specifications and stands for the proposition that the Agency (in this case, OCR) is of a neutral stance with respect to the various types of implementation technologies. Thus, OCR does not recommend or otherwise suggest the utilization of a particular technology solution for implementation of the specifications. Instead, OCR leaves the choice of technology up to the covered entity, so long as the implemented technology solution can satisfy the related specification(s).

Next, considering the concept of scalability, OCR recognizes that covered entities come in all shapes and sizes. The solutions that are reasonable for one covered entity may be totally impracticable for another entity. Take for example the contrasting of a single-source employer plan covering 50 individuals versus a multiple employer welfare arrangement (MEWA) covering 5,000 individuals within two plans consisting of three coverage tiers, across a spectrum of states, localities, industries, or other subdivisions (e.g., corporate and manufacturing). Obviously, the risk management plan for the single-source plan is going to require a very different risk analysis than the one developed for the MEWA. Thus, OCR has adopted the HIPAA scalability standard to help with the individual management of the implementation specifications by each responsible covered entity.
The specific steps of the risk analysis and risk management processes are relatively straight-forward. Analysis consists of eight steps:



The steps of risk analysis and management are important to understand, because while these activities are required as part of an overall HIPAA compliance process, they also frame a covered entity's response to a breach incident and the associated response notifications. Thus, performance of the risk analysis and management steps as a matter of routine installation of HIPAA compliance measures is a fantastic pre-breach practice for a covered entity's performance of the required post-breach analysis that must be performed after an attack, also referred to as part of the security incident response plan.

REQUIRED ADMINISTRATIVE TASKS FORM THE FOUNDATION OF A SUCCESSFUL CYBERCRIME DEFENSE

The HIPAA Privacy and Security Rules require covered entities and business associates to perform certain administrative tasks to ensure compliance with their regulatory obligations. While very much beleaguered by plan sponsors, the performance of these administrative tasks actually forms a relatively robust information security incident management plan.Generally, the administrative tasks include:

- The entity must have a Privacy Officer; [4]
- The entity must have a Security Officer; [5]
- The covered entity must have written policies and procedures in place; [6]
- The covered entity must conduct workforce training and management; [7]
- The covered entity have and apply an appropriate sanctions policy; [8]
- The covered entity must have and apply an appropriate harm mitigation policy; [9]
- The covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards; [10]
- The covered entity must have and apply procedures for individuals to complain about its compliance with its privacy policies and procedures under the Privacy Rule;
- The covered entity must not retaliate against a person for exercising rights provided in the Privacy Rule, for assisting in an investigation, or for opposing an act or practice violated the Privacy Rule; [11]
- The covered entity must maintain required documentation; and, [12]
- The covered entity must provide a notice of its privacy practices. [13]

[14]

While the above-referenced tasks can be time-consuming and costly to implement, they are essential requirements of any HIPAA compliance action plan. For example the task of implementing policies and procedures to assist an entity in responding to and recovering from a ransomware attack. Policies and procedures should consider the required inclusion of certain procedures outlining the requirement and process for performing routine data back-ups. Remember that ransomware denies access to data, so maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack. To that end, policies and procedures should require test restorations be conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Also, OCR notes that ransomware variants have been known to remove or otherwise disrupt online backups, so entities must consider maintaining backups offline and unavailable from their networks.

While implementing a data backup plan is a Security Rule requirement for HIPAA covered entities and business associates as part of maintaining an overall contingency plan, there are additional activities that must be included as part of an entity's contingency plan which include: disaster recovery planning, emergency operations planning, analyzing the criticality of applications and data to ensure all necessary applications and data are accounted for, and periodic testing of contingency plans to ensure organizational readiness to execute such plans and provide confidence they will be effective.

Training and readiness for employees is also essential to any ransomware defensive strategy, and the HIPAA Administrative Simplification Rule requires this training as an aspect of overall administrative preparedness. The HIPAA Rules neither offer a course outline for training, nor do they standardize any curriculum for such education. Instead, relying on the concepts of scalability and neutrality, the Rules merely require that an organization conduct HIPAA training on the policies and procedures it has implemented in observation of compliance with the rules. Thus, while it is common sense that an organization should conduct training of its pertinent employees with respect to the identification and response to certain security incidents, the task is made mandatory by the HIPAA Administrative Simplification Rules.

During the course of responding to a ransomware attack, an entity may find it necessary to activate its security incident procedures, as defined in its written policies and procedures. Once activated, an entity will be able to continue its business operations while continuing to respond to and recover from a ransomware attack. Security incident procedures, including procedures for responding to and reporting security incidents, are also required by HIPAA.[15] An entity's security incident procedures should prepare it to respond to various types of security incidents, including ransomware attacks. As outlined by OCR, robust security incident procedures for responding to a ransomware attack should include processes to:

- Detect and conduct an initial analysis of the ransomware;
- Contain the impact and propagation of the ransomware;
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual, or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

RESPONDING TO THE CYBERCRIME EVENT

Once a network is infiltrated with a ransomware agent, the plan sponsor has specific, timely duties related to the plan's status as a HIPAA covered entity. This is the point where the performance of HIPAA best practices forms the substantive operations by which the infiltration is identified, segregated, and eradicated. Remember, a covered entity's emergency response plan is triggered by the actual ransom notification, or in some cases by failing network operations, as the ransomware agent begins propagating itself throughout the victim's network. As noted by OCR, the presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. An entity's security incident response activities should begin with an initial analysis to determine:

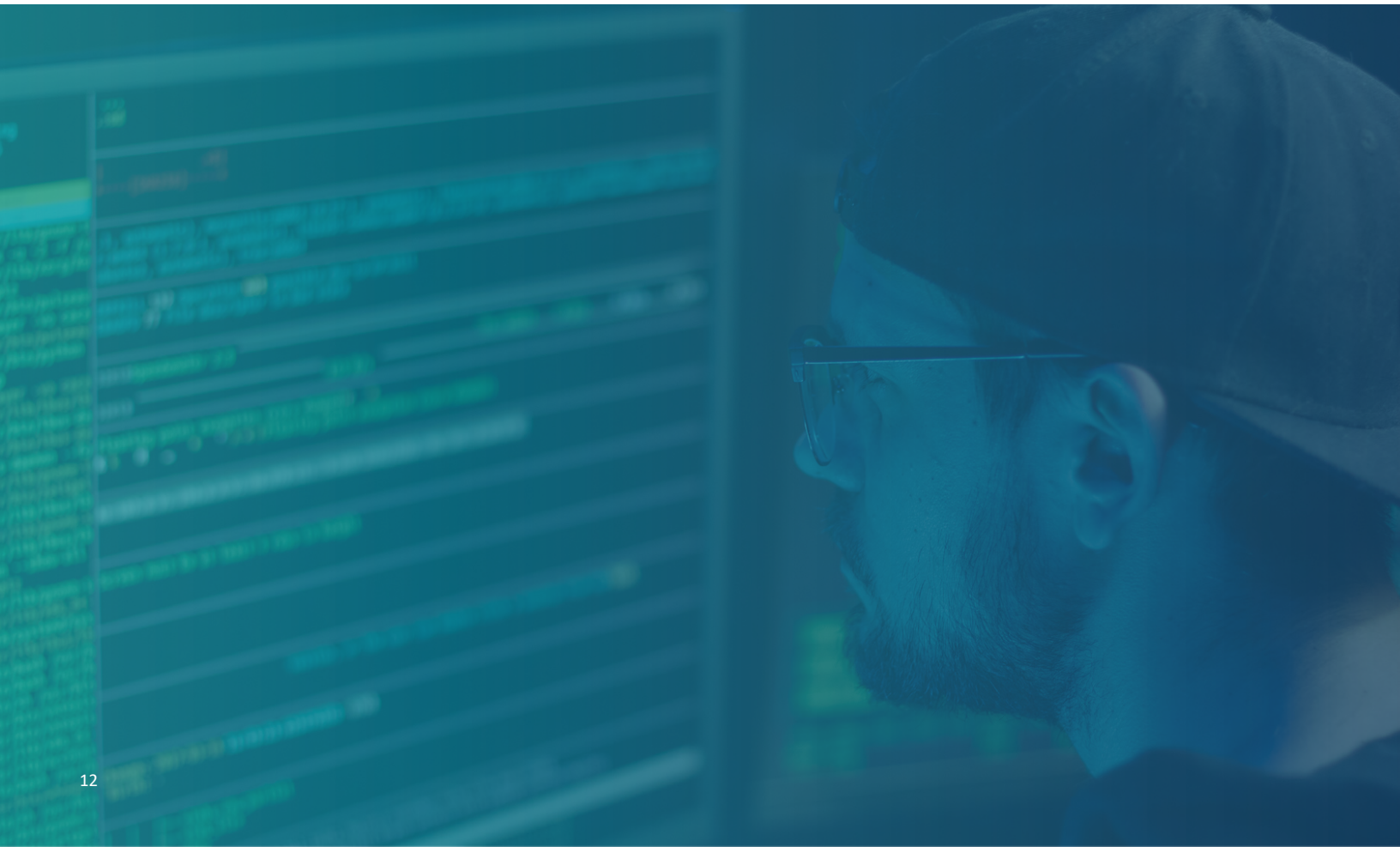
- The scope of the incident to identify what networks, systems, or applications are affected;
- The origination of the incident (who/what/where/when);
- Whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and
- How the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).

These initial steps outlined by OCR should assist the entity in prioritizing subsequent incident response activities and serve as a foundation for conducting a deeper analysis of the incident and its impact. Subsequent security incident response activities should include steps to:

- Contain the impact and propagation of the ransomware;
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual, or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

Having performed its security incident response activities, any post-breach analysis must involve assessing whether there was a breach of PHI as a result of the security incident. OCR notes that the presence of ransomware (or any malware) is a security incident under HIPAA that may also result in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack. When the covered entity or business associate identifies an impermissible disclosure of PHI in violation of the Privacy Rule, the organization will have to not only analyze the methodologies of infection and eradication, but also assess the propriety of activating the participant, organizational, media, and Secretarial notification procedures defined by the Rules (noting that the Breach Notification Rule defines these steps).

It is important to note that the determination of whether the presence of ransomware is a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." When e-PHI is encrypted as the result of a ransomware attack, the covered entity must assume a breach has occurred because the e-PHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" prohibited by the HIPAA Privacy Rule. However, if the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," (based on the factors set forth in the Breach Notification Rule), a breach of PHI is not presumed to have occurred and the covered entity or business associate will not have to activate its notice procedures.



ESTABLISHING A LOW PROBABILITY PHI WAS COMPROMISED

To make the notification determination, the covered entity or business associate must first perform a risk analysis to establish whether there is a low probability that the PHI contained on the hard drives and/or backup drives was compromised. The analysis takes the form of the risk analysis discussed above; however, OCR requires the covered entity or business associate to conduct an analysis of at least four essential factors in this type of post-incident risk assessment:

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

To the extent additional risk factors are relevant to the inquiry, the covered entity or business associate may need to work through additional analytic steps, as appropriate. As for the four essential factors, OCR's recent Factsheet regarding ransomware and HIPAA explains the analysis at length, but the key points are summarized herein.

First, remember that any breach analysis, and where needed, the accompanying breach notifications, are based on an analysis of the prevailing facts and circumstances; thus, there is no 100 percent right answer when making breach determinations. In each instance, the plan sponsor, working in concert with the plan's Privacy and Security Officers and other designated individuals, will need to work through a consistent and methodological approach to the analysis of the event, response and eradication, member notifications, and post-incident recovery activities.

The plan sponsor should work through the analysis sequentially, starting with point one: **"the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification."** For this step the plan sponsor should consider all the potentially breached PHI/e-PHI as breached. Then, consider which documents or applications contain the accessed PHI/e-PHI. Part and parcel of this consideration, remember to look past the obvious, as health information has a way of showing up in many human resources information and documents. Also, for this inquiry, the plan sponsor may have to consider documents and things outside the traditional reach of HIPAA, such as return to work certifications, drug testing results, and physician reports because the misuse of this traditionally HIPAA-exempt information may implicate HIPAA, or other state confidentiality laws. As for re-identification, the plan sponsor should determine if the information breached was readily identifiable or if it was encrypted, either electronically or via the utilization of unique identifiers, such as masked social security numbers or other random identifiers. Then, based on the analysis of this information, the covered entity or business associated should make its point one determination, in terms of how likely it is that if the breached information were viewed, would the acquiring entity be able to piece together an accurate picture of whom that PHI/e-PHI is actually about or to whom it belongs.

Moving on to point two, the covered entity or business associate should make an analysis of **"the unauthorized person who used the PHI or to whom the disclosure was made."** Unlike cases of misplaced mobile media or non-password protected and lost laptops, ransomware attacks are unique in that determinations of the actual identity of the attacker are quite easy; this is because the attacker will generally identify himself or herself after infiltration, when the actual ransom demand is made to the organization. However, remember that identifying the attacker means more than a name and address or telephone number in Croatia – identifying an attacker means performing an analysis of the particular skillset of the infiltrator. Here, it is important to consider not only the specific identify of the breaching individual(s) or entity(ies), but also the skills and competencies exhibited by the attacker. A proficient attack likely means a more proficient attacker, so it is important to consider worst case and best case examples of how the identity of the attacker will influence the outcome of the risk analysis and larger investigation.

Point three, **"…whether then PHI was actually acquired or viewed,"** is perhaps the least complex step of the post-breach analytic process, yet the most consequential, because the outcome of step three largely determines whether, and to what extent, the covered entity or business associate will have to perform required breach notifications. Here, the covered entity or business associate is charged with assessing whether the PHI was actually acquired (exfiltrated) or viewed (largely, infiltrated). Unfortunately, in the case of ransomware, oftentimes the plan sponsor will not know whether the e-PHI has actually been acquired by the attacker (that is, exfiltrated), or if the attacker has merely locked the victim's hard drive. Where the victim is unsure, the determination must be made that the worst-case scenario is reality and that the e-PHI was actually acquired. Later, it may be determined that the information was merely locked on an otherwise secure hard drive, but until such time as that determination can unequivocally be made, the entity must assume that an exfiltration event has in fact, occurred.

The fourth and final step of the minimum required post-incident risk analysis involves **"…the extent to which the risk to the PHI has been mitigated."** Here, the covered entity or business associate should consider the impact of the ransomware on the integrity of the PHI. Frequently, in the case of a ransomware attack, after encrypting the data it was seeking, the strain deletes the original data and leaves only the data in encrypted form. An entity may be able to show mitigation of the impact of a ransomware attack affecting the integrity of PHI through the implementation of robust contingency plans including disaster recovery and data backup plans. Conducting frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack and ensuring the integrity of PHI affected by ransomware. OCR cautions plan sponsors to conduct periodic test restorations to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. However, integrity assurance is only one aspect of the analysis when considering to what extent the risk to PHI has been mitigated. Additional aspects, including whether the PHI was exfiltrated, should also be considered when determining the extent to which the risk to PHI has been mitigated.

Robust security incident response activities will assist the covered entity or business associate with the performance of the post-incident risk analysis detailed herein. For example, OCR suggests the evidence drawn from the investigation may help to:

- Understand the exact type and variant of malware discovered;
- Analyze the algorithmic steps undertaken by the malware, so that the victim organization can understand the steps the malware is programmed to perform;
- Discover communications, including exfiltration attempts between the malware and attackers' command and control servers;
- Analyze whether the malware propagated to other systems, potentially affecting additional sources of e-PHI; and,
- Analyze whether the malware may attempt to exfiltrate data, or whether or not the malware deposits hidden malicious software or exploits vulnerabilities to provide future unauthorized access.

Upon performance of the foregoing post-breach risk analysis, ultimately the covered entity or business associate will have to make the factual determination of whether there is a low probability that the PHI involved in the attack was compromised. To the extent the entity determines there is a low probability, the entity may not have to perform individual, organizational, or media notification of the breach. However, to the extent the entity cannot establish that there is a low probability the suspect PHI was compromised, the entity will need to activate its breach notification procedures under HIPAA. This may involve individual notices to affected plan participants, enterprise-wide notification, media notifications, and even notice to the Secretary of HHS. Also, in many instances, covered entities and business associates may also accrue state-level notification obligations in the event of a breach of confidential information. Finally, the covered entity or business associate may have to (or should) notify local law enforcement, the FBI, and other law enforcement agencies regarding the breach. These obligations are outlined with detail within the regulations and various sub-regulatory guidance underlying HIPAA's Breach Notification Rule.

INFORMATION SECURITY BEST PRACTICES FOR PLAN SPONSORS

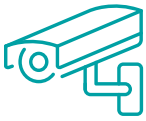
Throughout many of the publications and much of the enforcement data released by OCR and HHS, a common theme arises with respect to HIPAA compliance assuredness: covered entities and business associates repeatedly fail to perform even the most basic HIPAA security assuredness tasks. Including such activities as appointing Privacy and Security Officers, conducting training, development of policies and procedures, performance risk analyses, and properly contracting with third party vendors and service providers, HIPAA's administrative tasks have required implementations for years, yet, time and again, plan sponsors are audited only to find out that they have failed to perform the HIPAA basics, much less its more advanced security requirements. While these tasks are burdensome, in their performance lies the key to responding to a surviving a ransomware event.

In addition to the administrative tasks outlined above, plan sponsors and covered entities are reminded to keep the information security basics in mind, which generally include such items as:

- Use complex passwords ("Aa#.lo%++]59") that are changed according to regular intervals;
- Promptly terminate access for unauthorized users;
- Develop and maintain an actionable sanctions policy for employees that fail to adhere to HIPAA's requirements;
- Develop and maintain a workable mobile device policy that assures data is not accessible by unauthorized users;
- Conduct training on regular intervals for newly hired and continuing workers;
- Deliver security reminders to workforce members on regular intervals, reinforcing the basics and reminding users to be careful with email and on-line applications;
- Establish a "security culture" by encouraging and recognizing good computer habits;
- Install, maintain, and regularly update firewalls and virus protection applications;
- Limit access – both physical access to sensitive areas and information and network access to essential personnel;
- Report information security issues appropriately and promptly, and always consider reporting to law enforcement, where indicated;
- Perform and maintain backups of data according to regular intervals and keep backups segregated and offline; and,
- Prepare and plan for the unexpected.

Considered in context, the following key takeaways will help to ensure an organization has secured adequate initial defenses to the threat of cybercrime. While these actions may not totally circumvent the many opportunities existing for cybercriminals to exploit organizational weaknesses, many of these activities represent the best bets for an entity seeking to mitigate its exposure related liabilities and mitigate the consequences of same (see following Chart 4).

Chart Number 4:
BEST PRACTICES FOR CYBERSECURITY



Establish a Security Culture

Plan for the Unexpected

Protect Mobile Devices

Control Access to PHI

Maintain Good Computer Habits

Use Strong Passwords & Update Often

Use a Firewall

Limit Network Access

Install & Maintain Anti-Virus Software

Control Physical Access

CONCLUSION

Law enforcement and regulatory agencies readily admit the ransomware problem will be impossible to eradicate because no single response, in and of itself, will defeat the ransomware threat. Nevertheless, steadfast utilization of a diligent approach to the performance of best practices and the regulatory requirements espoused under the law of HIPAA will help to mitigate this threat. Through regular and comprehensive training, diligent development and practice of HIPAA policies and procedures, and steadfast adherence to the post-incident and post-exposure guidelines, plan sponsors have a toolbox brimming with experience and practical resources. So then, the issue and prevailing problem becomes one of utilization, rather than one of availability of responsive resources. Thinking back to the statistics offered in this article, the question each plan sponsor should be asking is "When will it happen to me and how will I respond?" For additional resources, enforcement data, and sample documents for covered entities and business associates visit https://www.hhs.gov/hipaa/index.html or https://www.hhs.gov/ocr/index.html.

1 See: https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/
2 See: Id.
3 See: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
4 45 C.F.R. § 164.530(a).
5 45 C.F.R. § 164.308(a)(2).
6 45 C.F.R. § 164.530(i).
7 45 C.F.R. §§160.103 and 164.530(b).
8 45 C.F.R. § 164.530(e).
9 45 C.F.R. § 164.530(f).
10 45 C.F.R. § 164.530(c).
11 45 C.F.R. §§ 164.530(d) and 164.520(b)(1)(vi).
12 45 C.F.R. § 164.530(g).
13 45 C.F.R. § 164.530(j).
14 45 C.F.R. §§ 164.520(a) and (b).
15 See 45 C.F.R. 164.308(a)(6).

BRP | THE BALDWIN REGULATORY COMPLIANCE COLLABORATIVE

The Baldwin Regulatory Compliance Collaborative (the "BRCC") is a partnership of compliance professionals offering client support and compliance solutions for the benefit of the Baldwin Risk Partners organization. The BRCC team includes: Jason Sheffield, BRP National Director of Compliance; Richard Asensio, Burnham Benefits Insurance Services; Nicole L. Fender, the Capital Group; Bill Freeman, AHT Insurance; Stephanie Hall, RBA/TBA; Caitlin Hillenbrand, AHT Insurance; Paul Van Brunt, Baldwin Krystyn Sherman Partners (BKS); and Natashia Wright, Insgroup.