WHITEPAPER

Attivo NETWORKS®

MEETING HIPAA REQUIREMENTS WITH ATTIVO NETWORKS THREATDEFEND® PLATFORM

EXECUTIVE SUMMARY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) laid out a broad range of rules for Healthcare providers in the United States that fundamentally changed how these organizations were required to handle patient information. The HIPAA requirements set standards for protecting patient records without laying out specific technological or process solutions. One of the goals of these requirements was to allow enough flexibility for organizations to meet the privacy and security mandates using the tools that best fit their environment. In this paper we will look at how attack prevention, detection, and adversary intelligence collection based on cyber deception and data concealment technologies can help an organization meet these requirements effectively, and efficiently, specifically in the context of Information Security.

CHALLENGES

The HIPAA regulations are complex and meeting their requirements has proven to be a challenge for many organizations, as they have been updated several times since their introduction. As a result, different healthcare organizations have been subjected to various requirements at different times depending on their scale. The fact that the requirements present standards and expectations without specifying which technologies to use does add some flexibility, and organizations can take advantage of this to adapt their defenses to meet their needs.

The Health and Human Services website[1] sums the security requirements up as follows:

> "The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI[2].
>
> Specifically, covered entities must:
>
> 1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
> 2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
> 3. Protect against reasonably anticipated, impermissible uses or disclosures; and
> 4. Ensure compliance by their workforce "

Anticipating attacks and potential new threats, as noted in points 2 and 3, can be a challenge for many conventional defensive technologies. The regulations go into greater depth about what they consider appropriate safeguards, but they expressly allow for flexibility as shown in the same reference:

> “HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore, the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.
>
> Therefore, when a covered entity is deciding which security measures to use, the rule does not dictate those measures, but requires the covered entity to consider:
>
> - Its size, complexity, and capabilities,
> - Its technical, hardware, and software infrastructure,
> - The costs of security measures, and
> - The likelihood and possible impact of potential risks to e-PHI.
>
> Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.”

Many organizations have opted to take the most obvious approach to meeting the HIPAA requirements and securing their IT infrastructure: perimeter defenses, endpoint defenses, intrusion detection, data loss prevention, and logging, all from established security vendors. This “check all the boxes” approach technically satisfies the requirements, letting health care organizations pass any required audits. For smaller organizations that lack the resources to manage their own security, a broad range of Managed Security Service Providers (MSSP) can fill their needs.

However, the “check all the boxes” approach is not always enough. Sophisticated attackers have shown repeatedly that they can slip through perimeter defenses and avoid conventional detection techniques once inside. While e-PHI is the obvious target for attackers, healthcare environments have felt the effect of ransomware attacks, medical IoT devices have been leveraged for attacks, and idle systems have been leveraged for cryptomining, to name just a few potential targets in this space.

With the sensitivity of the information involved and the potential damage to patient privacy, organizational reputation, and financial risks imposed by HIPAA, healthcare organizations need to implement best-of-breed solutions to support a full defense in depth posture.

THE ROLE OF DECEPTION AND DERAILMENT

Attackers have shown repeatedly they can bypass perimeter security and evade conventional defenses within the enterprise. While "dwell time" – the time between an attacker's initial compromise and their discovery by the defender – hhas been growing consistently shorter, the median dwell time in the Americas is still approximately 24 days[3]. This is down from 60 days in 2019[3], and is likely attributed in part to the increase in ransomware attacks in recent years. However, this still gives time for an attacker to exfiltrate information or damage the target environment. This leaves organizations in need of a solution that can deliver a scalable defense that is highly accurate in detecting in-network threats that have bypassed perimeter defenses. Technologies designed to proactively reveal threats are also invaluable for detecting early and mitigating the energy required to remediate infections.

> Regardless of the attack vector or motive, deception technology offers capabilities that other layers of a Defense in Depth model can't provide. Assuming attackers can, and will, penetrate the perimeter...

This is where deception technology comes into play. Most attackers operate with the assumptions "I have time" and "what I see is what I get." The currently reported median dwell times speak to their first assumption. In many documented cases, they do have time. Even after an organization identifies and remediates the compromise, attackers routinely leave multiple routes in place to let them return. In relation to the second assumption, attackers typically expect the resources they see on the network to be what they appear to be. Why wouldn't they? Commercial availability of solutions to deploy and manage convincing decoys that include customized data and application deceptions did not exist until a few years ago. Historically, an attacker felt safe making these assumptions.

Deception technology changes not only the paradigm, but also the asymmetry of an attack. By placing highly attractive decoys into the environment, the attacker can no longer assume that what they see is what they get. Using a deception network to obfuscate the attack surface alters the economics of their attack and when combined with enticing lures, can dramatically increase the odds of an attacker making a mistake which will reveal their presence.

With a traditional "low and slow" attack strategy, an adversary could limit their exposure and extend their dwell time, while operating on the assumption that everything they were seeing was real and that they could freely explore without being detected. With decoys and lures spread through the environment, attackers must now thread through a virtual minefield where even a slight misstep gives the defenders a high-fidelity alert. The complexity of an attack can also be increased when decoys are deployed in nontraditional areas, which threat actors are now targeting based on their increased complexity to secure. These could be IOT, medical IOT, infrastructure, telecommunications, industrial control or point-of-sales systems, to name a few, all of which can be found in healthcare environments.

With deception, concealment and derailment techniques in place, the adage "an attacker only needs to be right once to get in while the defenders need to be right every time" is turned on its head. The attacker must be right every time, or they will alert the defenders. They no longer have time and what they see is not guaranteed to be what they get.

THE ROLE OF ATTIVO NETWORKS IN HIPAA COMPLIANCE

One key point of the HIPAA regulations is: "Identify and protect against reasonably anticipated threats to the security or integrity of the information." This is especially challenging in a dynamically changing threat environment where attackers are constantly finding, and employing, new techniques that go beyond "reasonably anticipated." This is where the Attivo Networks® ThreatDefend® platform provides an invaluable tool for defense and detection.

The Attivo Networks® ThreatDefend® platform is a unique solution that prevents identity privilege escalation and detects attacker lateral movement. The ThreatDefend platform's concealment and misdirection technology derail attackers as they can longer find or access the data, files, AD objects and credentials they seek. With a focus on the needs of the healthcare environment, the portfolio offers the full range of deception, with decoy servers, credentials, data, and application deceptions that scale to accommodate both on premise and in the cloud needs. Additionally, the ThreatDefend platform is easy to manage with machine self-learning for automated deployment and an intuitive user interface that presents high fidelity alerts, correlated attack analysis, along with native integrations for incident response, so threat responders can quickly identify and remediate an attack.

> Native integrations with many highly respected 3rd party security solutions let an organization automate their response, automatically isolating infected hosts, initiating reporting, and streamlining their incident response.

To be most effective, decoys need to be both realistic and cover the entire environment. Deception for hosts and services need to seamlessly blend into the environment and appear as real hosts delivering authentic services. For maximum effect and authenticity, the deception can't stop with just host and service decoys. By adding authentic credentials, resources, and even decoy documents, the Attivo Networks® ThreatDefend® platform provides complete deception that makes it extremely difficult for an attacker to tell what is real and what is a trap.

With a range of decoys to simulate an entire production environment, Attivo provides highly authentic deception that projects servers, medical IoT devices, endpoint, IoT, Active Directory, infrastructure, and telecommunications devices that appear identical to production assets. The platform deploys more than just decoys to trap the attackers during reconnaissance, but also includes credentials, shares, applications, and decoy documents that entice an in-network attacker to take the bait. This redirects them into the deception environment where they can be monitored and contained. Collectively, these deceptions make an attacker's job dramatically harder, consume more of their time, and often serve as a deterrent as an attacker is driven to seek easier targets. Any misstep on the attacker's part reveals their presence to the defender whether they are a live Advanced Persistent Threat (APT) or an automated attack tool. In fact, the ThreatDefend® solution offers a highly effective defense against not only known threats such as ransomware, malware, and bitcoin mining attacks, but also the targeted and unknown attacks that, by design, don't have available detection signatures. Deception will also not create "alert fatigue" as each alert is created after engaging with a threat actor. Any attack that even lightly touches a decoy asset or attempts to use deception credentials, or bait, is immediately reported and the attack derailed.

Native integrations with many highly respected 3rd party security solutions let an organization automate their response, automatically isolating infected hosts, initiating reporting, and streamlining their incident response. This reduces the operational burden on information security teams, making them more effective and efficient. As a result, the organization achieves a more comprehensive security program that includes prevention and in-network threat detection, all without requiring additional personnel.

> The attacker must be right every time, or they will alert the defenders. They no longer have time and what they see is not guaranteed to be what they get.

MEETING SPECIFIC HIPAA REQUIREMENTS

The complete HIPAA documentation runs hundreds of pages and covers a range of requirements. Below, we have highlighted specific sections of the HIPAA regulations focused on Information Security that are addressed with Attivo Networks® deception technology. These regulations are specific to section 164 – Security and Privacy – of the HIPAA requirements[6], and key highlights are included here.

For complete coverage of HIPAA regulations, reference the Health and Human Services website at: https://www.hhs.gov/hipaa/

HIPAA REQUIREMENT SECTION	DESCRIPTION	ATTIVO SOLUTION
SECURITY STANDARDS		
§ 164.306 (a) 1, 2, 3	(a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	The ThreatDefend platform uses deception technology to provide defenses that adapt automatically to a changing threat landscape. Even as attackers alter their approach, deception shifts the balance in favor of the defender, protecting their data against evolving threats.
§ 164.306 (b) 1, 2	(b) Flexibility of approach. (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The covered entity's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.	The ThreatDefend platform scales effectively, efficiently, and economically to provide security across a range of organizations without placing additional strain on IT or Information Security resources. The platform allows a range of installation options, including physical appliance, virtual machine, Cloud, or hybrid installation. The ThreatDirect® solution allows an organization to seamlessly project assets into remote locations without requiring additional infrastructure or overhead.

HIPAA REQUIREMENT SECTION	DESCRIPTION	ATTIVO SOLUTION
ADMINISTRATIVE SAFEGUARDS		
§164.308 (a) (1) (ii) (A), (B), (D)	(a) A covered entity must, in accordance with § 164.306: (1) (ii) Implementation specifications: (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). (D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	The ThreatDefend platform can provide valuable insights during risk assessments and penetration tests, helping assure an organization's security. The ThreatPath® solution provides attack path visibility and can identify misconfigurations and credential vulnerabilities that may lead to lateral movement and compromise. The Endpoint Detection Net (EDN) suite tracks the activities on the endpoint systems. If it deems the activity malicious, it raises an alert which feeds forward into the enteprise's Security Operations Center for remediation.
§164.308 (a) (3)(ii) (A)(B)	(3)(ii) Implementation specifications: (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. (B) Workforce Clearance Procedure (Addressable). Implement procedures to ensure appropriate PHI access.	The ThreatPath solution offers a unique capability to detect exposures of key accounts and credentials across the IT infrastructure. The ThreatPath solution can alert if credentials of an authorized workforce member with access to ePHI are exposed in the network.
§164.308 (a) (5) (ii) (B)(C)(D)	(5) (ii) Implementation specifications. Implement: (B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software. (C) Procedures and monitoring of log-in attempts (D) Procedures for password management	The ThreatDefend platform detects malicious attacker activities and provides deep forensic data for investigation. The EDN Suite's anti-ransomware function helps to defend against malicious software in two ways: • Blocking ransomware attacks on endpoints • Hiding the files, folders, and mapped network drives. Additionally, the BOTsink® server offers a sandbox environment for malware analysis and study the attacker's malicious intent. The ADAssessor solution offers real time detections for brute force attacks, these are achieved by monitoring the log-in attempts. The EDN Suite's ThreatStrike® solution safeguards passwords by preventing unauthorized access to the various password stores. It can also deploy deceptive credentials and accounts that look real.

HIPAA REQUIREMENT SECTION	DESCRIPTION	ATTIVO SOLUTION
ADMINISTRATIVE SAFEGUARDS (CONT.)		
§164.308 (6) (i), (ii)	(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. (ii) Implementation specification: Response and Reporting (Required).	The Attivo ThreatDefend platform automated incident response with integrations that provide automatic threat intelligence sharing, blocking, and threat hunting. The Attivo Networks ThreatOps® supports playbooks through integrations to increase the efficiency of the incident response process.
TECHNICAL SAFEGUARDS		
§164.312 (b) (e) (1)	(b) Audit Controls - Procedures and mechanisms for monitoring system activity (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	The EDN suite tracks the activities on the endpoint systems, and if deemed malicious, raises an alert that feeds into the enterprise's Security Operations Center for remediation. The EDN Suite's ThreatStrike solution deploys deceptive credentials, accounts and files designed to look authentic, detect and misdirect an attacker looking for ways to compromise critical data such as ePHI. The ThreatPath solution monitors active lateral paths in the infrastructure, and its policies can flag an unauthorized transmission of ePHI data.
ORGANIZATIONAL REQUIREMENTS		
§164.314 (b) (2) (iv)	(iv) Report to the group health plan any security incident of which it becomes aware.	The ThreatDefend platform includes extensive reporting of any suspicious activity that takes place within the deception environment. Integration with 3rd party applications, including SIEM and ticketing tools, delivers easy and complete reporting of security incidents for accelerated response.

SUMMARY

Complying with the HIPAA regulations can be complex, and conventional defenses may not be enough to assure that e-PHI information remains secure. Health records are not the only potential target for an attacker. Healthcare organizations also face other threats, such as ransomware and other malware that can affect patient privacy and even safety.

Regardless of the attack vector or motive, the Attivo Networks ThreatDefend platform offers capabilities that other layers of a Defense in Depth model can't provide. Assuming attackers can, and will, penetrate the perimeter, visibility of exposures, early alerting, and placing defenses inside the environment that are expressly designed to trip up and trap an attacker turns the tables on the attacker and shifts the odds in the defender's favor.

By delivering insight into credential and attack path vulnerabilities and Active Directory domain, user, and device-level exposures, healthcare organizations are better prepared to increase their security posture. Concealment technology denies and derails attackers since they can no longer see or access critical data, files, AD objects, and credentials to move forward with their attack. Additionally, the solution's decoys obfuscate the attack surface, collect forensic data, automatically analyze attack data, and automate incident response through its 30 native integrations.

Whether a large, multi-state health plan, or a small organization, the Attivo Networks solution delivers a highly efficient, effective, and accurate prevention and detection solution that provides the tools to stay a step ahead of modern cyber-attackers.

1] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
2] e-PHI is the HHS designation for "electronic protected healthcare information"
3] https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
4] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&
5] https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf pg. 24
6] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com

APPENDIX

Resources

The United States Department of Health and Human Services maintains the complete HIPAA requirements and provides several useful resources that can help an organization meet these regulations.

Relevant regulations

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

Privacy Rules Summary

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Combined regulation text

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/

HIPAA Administrative Simplification

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

Full requirements

https://www.hhs.gov/hipaa/for-professionals/security/

Key Dates in HIPAA History

- August 1996 – HIPAA Signed into Law by President Bill Clinton.
- April 2003 – Effective Date of the HIPAA Privacy Rule.
- April 2005 – Effective Date of the HIPAA Security Rule.
- March 2006 – Effective Date of the HIPAA Breach Enforcement Rule.
- September 2009 – Effective date of HITECH and the Breach Notification Rule.
- March 2013 – Effective Date of the Final Omnibus Rule.

Potential Penalties

HIPAA includes severe financial penalties for healthcare providers that fail to meet a range of security requirements, ranging from hundreds to tens of thousands of dollars depending on the nature of the violation and the organization's culpability. The following table is presented for example purposes, and organizations should refer to the HIPAA regulations for clarification.

HIPAA TIER	DESCRIPTION	FINANCIAL PENALTY
Tier 1	Unaware: Covered entity or individual did not know - and by exercising reasonable diligence would not have known - the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
Tier 2	Reasonable cause: The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.
Tier 3	Willful neglect but corrected within required period: The HIPAA violation was due to willful neglect, but the violation was corrected within the required period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.
Tier 4	Willful neglect and uncorrected within period. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.

HIPAA regulations may also impose criminal penalties.

HIPAA TIER	POTENTIAL JAIL SENTENCE
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years