NETWORK DETECTION & RESPONSE:

The Role Frameworks and Privacy Regulations Play in Healthcare in Cybersecurity

EXECUTIVE SUMMARY

Healthcare's singular focus on saving lives has long meant cybersecurity was placed on the back burner. Given the choice between investing time and money to save a life versus patching insecure software, the choice has always been clear. Unfortunately, this has left the industry with a target on its back for cyberattacks. Cyberattacks cost the industry approximately $4 billion last year alone[1]. The proliferation of unprotected connected devices has created additional attack vectors that are increasing exponentially. The COVID-19 pandemic, which is driving the rapid adoption of new technologies such as telemedicine has only exacerbated the situation.

The Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, certifications like HITRUST, and security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and MITRE ATT&CK all play a role in helping healthcare organizations improve and enhance their cybersecurity efforts. But it can be difficult to understand how to apply each of these to any given organization because each organization is different. And with their history of low investments in cybersecurity, healthcare organizations have a lot of catching up to do.

This white paper explores how regulations, standards, and certifications work together to enable you to improve your organization's cybersecurity and meet your healthcare compliance mandates. It will also explain how network detection and response (NDR) provides the visibility you need to implement controls that improve your regulatory standards, while reducing risk and improving patient care and outcomes.

TABLE OF CONTENTS

HEALTHCARE FACES A BROAD RANGE OF CYBERSECURITY CHALLENGES

Healthcare is the industry most targeted by cybercriminals, with a third of all data breaches in the United States occurring in hospitals[2]. And the problem continues to grow. Between 2018 and 2019, the number of breached records increased by 37 percent to 41.3 million[3].

Among the major breaches that occurred in 2020, a Midwest healthcare organization was forced to notify just under 288,000 patients[4] from 19 of its affiliated hospitals that their data was compromised after a successful phishing attack. In another incident, a hacker obtained the credentials of an employee from a Texas-based healthcare-centric organization to access the insurer's systems and deploy malware. The attack breached the data of 274,837 patients from several providers and payers that use their system for billing and collections services. A California-based clinical genomic diagnostic vendor, suffered an email hack that compromised the data of 232,772 patients.

Ransomware is rapidly becoming one of the key cybersecurity challenges for the healthcare industry. A Check Point research report published in October of 2020 found that ransomware attempts jumped 50 percent in the previous three months compared to the first half of 2020, with healthcare organizations the hardest hit[5]. More recently, a joint advisory[6] was issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) that warned of cyber actors targeting the healthcare sector using TrickBot and BazarLoader malware, resulting in ransomware attacks, data theft, and disruption of services.

A proliferation of connected devices in the industry is exacerbating the situation. Healthcare organizations are in the vanguard of adopting IoT devices, such as blood glucose meters, blood pressure, monitors, and pulse oximeters, that allow providers to better understand and track patient health. A mid-sized hospital today has 20,000 medical devices, including about 10-15 devices per bed[7]. Many of these devices are inadequately secured, which means they can serve as entry points to the broader hospital network. For example, many IoT cameras in hospitals are inexpensive devices connected by WiFi to a service that stores the recorded footage. Not only is this insecure, if a Web camera's video feed is open to anyone on the network, that would be an instant HIPAA violation.

The COVID-19 pandemic has added further fuel to the fire by accelerating the adoption of remote care through telemedicine. Telehealth claim lines increased 4,347 percent nationally from 0.17 percent of medical claim lines in March 2019 to 7.52 percent in March of 2020. The increase was even greater in the Northeast, the region of the country where the pandemic hit hardest in March[8]. Any change in an IT environment can increase risk and when that change is rapid, risk has the potential to rise rapidly.

"This increased number of attacks makes it even more important for hospitals to heighten their ability to detect and respond to potential threats before any data is compromised," said Charles Alessi, MD, Chief Clinical Officer at HIMSS.

THE ROLE OF SECURITY FRAMEWORKS AND REGULATIONS IN IMPROVING CYBERSECURITY

Healthcare regulations and cybersecurity frameworks are designed to give consumers and patients peace of mind that their data will remain private and available only to providers. They also provide healthcare organizations with standards to follow to improve their overall security posture. But applying these standards and addressing regulations can get complex, because every organization is different and no single, standard approach works for all.

HIPAA and HITECH, NIST CSF, and HITRUST provide guidelines that enable organizations to protect devices, networks, and sensitive patient health data and certify that appropriate actions were taken to keep the data secure and private. The MITRE ATT&CK knowledge base helps security analysts recognize the techniques used by attackers to better prepare for and respond to incidents.

HIPAA has a maximum penalty of $1,785,651 for the highest-level violations

HIPAA and HITECH—are regulations intended to guarantee that patients can access, and control access to, their personal data. The regulations also dictate how patient data and protected health information (PHI) should be kept private and secure. The fines for noncompliance in 2020 range from a minimum penalty of $119 for low level violations to a maximum penalty of $1,785,651 for the highest-level violations[9].

NIST CSF—this cybersecurity framework provides industry-standard guidelines that CISOs can employ to secure infrastructure across the organization. NIST offers a guide that helps organizations use its framework standards to implement HIPAA security requirements. The NIST CSF comprises voluntary recommendations and does not offer certification.

HITRUST—Developed in collaboration with data protection professionals, the HITRUST Cybersecurity Framework (CSF), rationalizes relevant regulations and standards into a single overarching security and privacy framework. While this standard can be certified, most of the HIPAA compliance standards will carry over to meet the requirements.

MITRE ATT&CK—is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. This knowledge base helps healthcare organizations understand how adversaries operate so they can plan how to better secure their networks and devices as well as detect and stop attacks.

HIPPA and HITECH

The 2000 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the HITECH Act of 2009 require U.S. hospitals to safeguard patient data.

HIPAA established individuals' rights to obtain a copy of their health records from a covered healthcare provider or health plan. The regulation also requires that healthcare organizations safeguard protected health information (PHI) through administrative policies and technical safeguards that include audit logging, backup, disaster recovery, and vulnerability scanning. As part of its mandate to protect patient data, the HIPAA Security Rule requires that healthcare organizations provide cybersecurity safeguards, such as secure messaging, for electronically held PHI found in electronic health records (EHRs) and medical devices. According to Jeff Costlow, CISO at ExtraHop, "HIPAA takes a very data centric-view and focuses on protecting healthcare patient records. It's all about providing specific actions you should take to secure patient data."

> "Compliant organizations have visibility to ensure that nothing out of the ordinary is taking place.
>
> **JEFF COSTLOW, CISO, EXTRAHOP**

HITECH was passed as part of the American Recovery and Reinvestment Act. The Act set aside funds for the creation of a nationwide network of electronic health records and initiated the Meaningful Use program. Because the Meaningful Use program incentivized healthcare providers to adopt technology as they provided healthcare, HITECH incorporates HIPAA Privacy and Security Rules to address concerns about the electronic storage and transmission of medical records.

Updates to HIPAA and HITECH often take one another's regulations into account. For example, HITECH raised fines for noncompliance with HIPAA to a maximum of $1.5 million per violation and required healthcare organizations to comply with Breach Notification rules that require organizations to notify individuals and in some cases the media of an unauthorized disclosure of PHI.

To comply with HIPAA and HITECH regulations, healthcare organizations must be able to confirm that they properly address specified administrative, physical, technical, and organizational regulations and procedures. Said Costlow, "Compliant organizations have visibility into what is connecting to their network, whether it's a PC, laptop, or one of the myriad medical devices on most healthcare networks today. They must know what devices are communicating with each other, where their most sensitive data is stored, who and what should access it, and how to best protect it. They can then monitor those devices and communications to ensure that nothing out of the ordinary is taking place."

HIPAA and HITECH provide no standard or implementation specification to enable Covered Entities or Business Associates to certify compliance. However, there are third parties who will conduct audits and attestations to assess companies and vendors to ensure they have the proper controls in place.

NIST

Organizations face potentially large fines for HIPAA and HITECH violations. Yet regulations can often use vague language, making compliance difficult. The NIST CSF and NIST security controls provide an objective approach that healthcare organizations can follow to meet regulatory requirements in a systematic manner.

NIST provides a crosswalk that maps its security standards to the HIPAA standard and safeguards

NIST CSF is a voluntary framework that security teams can use to establish a comprehensive set of security standards across the organization. NIST provides high level recommendations for things security teams need to be able to do to improve their security and risk profiles.

As a voluntary framework of recommendations, NIST has no penalties for non-compliance. NIST provides a single set of guidelines that CISOs can turn to when dealing with fragmented cybersecurity regulations. NIST also provides a crosswalk that maps its security standards to the HIPAA standard and safeguards, which makes it possible to achieve compliance in both NIST standards and HIPAA regulations by following a single common framework.
Some of the key NIST recommendations include:

- **Identify**—You can't secure what you can't see. As the first step in keeping unauthorized devices out of your environment or in preventing authorized devices from sending PHI where they shouldn't, NIST suggests inventorying all devices in the healthcare environment and profiling relevant data about them.
- **Protect**—NIST encourages healthcare organizations to limit access to physical and logical assets to authorized users, processes, and devices and manage appropriate access permission. Additional suggested protective measures include using network segmentation to protect network integrity and protecting the confidentiality and integrity of data in transit.
- **Detect**—In order for healthcare IT and security teams to detect anomalous activity more easily, NIST urges organizations to develop a baseline of network operations and expected data flows. It also proposes reporting incidents in a consistent manner with well-established criteria so organizations can address regulations with time sensitive reporting requirements.
- **Recover**—NIST suggests that healthcare organizations ensure effective response and recovery by investigating notifications from detection systems and performing forensic investigations.

HITRUST

HITRUST is a private organization that has developed a set of cybersecurity prescriptive controls called the Common Security Framework (CSF) that can help a healthcare organization ensure it has proper HIPAA controls in place. "HITRUST comes in and evaluates your processes and procedures and if they meet certain standards tells others that you are compliant with the regulations," explained Costlow.

The HITRUST CSF is broken out into 19 different "domains" that are aligned with common IT process areas, including information protection, network protection, incident management, endpoint protection, and others. These 19 domains are further broken into 135 Security Controls and 14 Privacy Controls that map back to multiple domains. Controls are then broken down into control requirements.

HITRUST helps healthcare organizations ensure they have proper HIPAA controls in place

To achieve HITRUST certification, organizations must achieve a passing score in each of the 19 HITRUST domains. Each control requirement is scored and evaluated against five different maturity levels based on the degree to which the control is implemented. The certification process looks at whether the organization has:

- Policies in place to address the requirements of the controls
- Formally documented procedures for non-automated controls
- Implemented all the elements of the control requirements
- Continuous monitoring in place to measure and manage controls

The score for each maturity level is based on the degree of implementation and the weighting of that maturity level.

MITRE ATT&CK Framework & Medical Device Incident Response Playbook

Compliance is not the same as security. Concentration on HIPAA and penalties often steer healthcare organizations to focus on data protection and not on overall operational security and resilience. Yet no matter how many HIPAA/HITECH/HITRUST compliance certifications an organization has, a determined attacker can always find a way in. New attack methods are constantly being developed, and since healthcare is a high-profile target, profit-driven attackers are investing in ways to attack healthcare organizations specifically. To prepare, hospitals need to prioritize overall security.

The MITRE ATT&CK framework[10] complements healthcare organizations' cybersecurity efforts by providing a knowledge base of real-world tactics that adversaries use to attack computer networks, including medical devices and telehealth infrastructures. MITRE ATT&CK was started in 2013 to catalogue observed tactics, techniques, and procedures (TTPs) used by advanced persistent threats (APTs) and other types of attack. Organizations of all types and sizes use the framework to identify gaps in security coverage, with notable adherents including the U.S. Department of Health and Human Services (HHS) and the National Health Information Sharing and Analysis Center (NH-ISAC). Said Costlow, "The MITRE ATT&CK framework lets you see how attackers operate so you can put in place controls that systematically stop specific attacks.

The MITRE ATT&CK Framework for Enterprise comprises nearly 300 attack TTPs, organized into 14 technique categories: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, and Impact.

Since healthcare organizations need to be especially worried about ransomware attacks, the Impact category of the MITRE ATT&CK Framework is likely to be particularly interesting to healthcare security professionals. Ransomware doesn't exist in a vacuum and often uses automated tactics from the Lateral Movement, Persistence, and Defense Evasion categories to ensure its success. For healthcare organizations with limited resources to dedicate to threat detection and incident response, focusing on ransomware and other common attacks leveraged against healthcare is one way to achieve the greatest risk reduction for your investment.

MITRE ATT&CK framework provides controls to systematically stop specific attacks

In addition to their ATT&CK Framework, MITRE has published a medical device security playbook in cooperation with the FDA, covering a range of security concerns around medical devices, including:

- Medical device procurement and asset inventory
- Medical device incident response, containment, eradication, and recovery
- Incident communications planning
- Medical device forensic investigation in the wake of an incident
- And many more relevant topics and guidelines

The MITRE Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook[11] is an invaluable tool for any healthcare organization looking to improve their cybersecurity, and a great complement to the MITRE ATT&CK Framework for teams particularly focusing on incident detection and investigation.

NETWORK DETECTION & RESPONSE: ENHANCE COMPLIANCE WITH REGULATION & FRAMEWORKS

Network detection and response (NDR) helps organizations comply with HIPAA/ HITECH regulations by simplifying the implementation of NIST and HITRUST recommendations and enabling rapid detection and investigation of MITRE ATT&CK TTPs being used against the organization. NDR delivers these capabilities by providing complete visibility into every device, user, application, and communication on the hybrid network. It detects threats other solutions miss, improves investigation, and accelerates response times as well as enhances network and application performance.

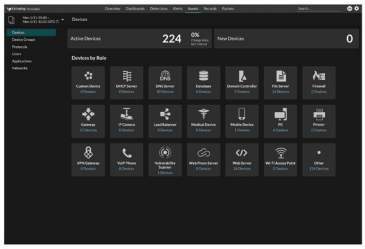
NDR not only complements the SIEM and EDR solutions that many security operations centers (SOCs) have in place, but enhances their overall efficacy. Where activity logs (SIEM) can be tampered with or deleted by an attacker to cover their tracks, observed network behavior is immune to tampering. Where endpoint (EDR) solutions require an agent that may be unsupported by certain devices, especially IoT, NDR can observe any traffic that crosses the network, and can identify and monitor which endpoints are not being, or cannot be, tracked.

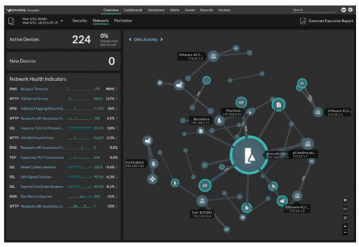
The network is considered the source of truth. It is passive, meaning attackers can't know they are being watched, and extremely hard to evade. Using network data, organizations can monitor and examine data in flight for real-time analysis of both north-south and east-west traffic. NDR employs protocol parsing and packet-level investigation to detect and investigate adversary behaviors and attack TTPs.

Extrahop Reveal(x):
Improving Security for Healthcare Organizations

The ExtraHop Reveal(x) network detection and response (NDR) solution has been independently assessed to meet HIPAA[12] compliance requirements and enables healthcare organizations to meet HIPAA/HITECH and HITRUST requirements. Additionally Reveal(x) incorporates MITRE ATT&CK TTPs within the solution for faster investigation and response to incidents.

Reveal(x) enables organizations to decrypt TLS 1.3 traffic to provide the complete visibility needed to see all traffic and encrypted payloads and ensure the legitimacy of the data received by the network. When a healthcare organization adopts Reveal(x), ExtraHop maintains the privacy of its data by not actively processing data in patient records—it simply serves as a caretaker for this data.





Reveal(x) helps healthcare organizations make better use of the NIST framework and achieve HITRUST certification by:

- **Identifying all devices.** ExtraHop Reveal(x) provides a complete real-time asset inventory of all managed and unmanaged device, including connected medical and IoT. This includes device make and model for the majority of devices.
- **Understanding the behavior of the hybrid network.** Machine learning is employed to create a behavioral profile of each device and understand its intended and baseline behavior. It can then identify when that device deviates from established norms within the context of the network to prioritize the alerts that really matter.
- **Protecting PHI.** By monitoring network behavior with automated understanding of what is most important, Reveal(x) will alert when unusual behavior is occurring on your most sensitive assets to ensure data confidentiality, integrity, and availability.
- **Detecting threats other tools miss.** Attacks like server-side scripting or DNS need the full context of the attack and the only way to detect these attacks is by line rate decryption of the payload to ensure the integrity of the data.
- **Providing analysts with data-rich investigation workflows.** Reveal(x) provides intuitive data that enables even inexperienced cybersecurity teams to understand the full scale of an attack quickly so they can perform necessary reporting within mandated timeframes.
- **Investigating faster.** Reveal(x) automatically provides all of the detection details to show offenders and victims in the context of the entire network to uncover lateral movement and privilege escalation activity.

ExtraHop Reveal(x) provides MITRE ATT&CK framework details within the investigation workflow, without an analyst needing to look elsewhere to understand the attack and the employed techniques, such as lateral movement, command and control, and data exfiltration. Reveal(x) detects behavioral signals that can indicate various types of attacks on the network and medical devices. In the case of ransomware, it will look for file extensions associated with that type of attack and provide alerts on what really matters.

Conclusion

Healthcare organizations are challenged to provide the highest possible level of patient care while protecting the sensitive data of their patients and partners. The task is rendered more difficult by the fact that healthcare is the number one targeted industry. And the issue is only growing worse. Ransomware and other attacks are skyrocketing. Poorly secured connected medical and IoT devices are proliferating. And healthcare cybersecurity must keep up with the surging use of telemedicine in the wake of the COVID-19 pandemic and the increased adoption of the cloud. It's time for healthcare organizations to improve cybersecurity by monitoring network data to provide the oversight needed to stop attacks before they breach the network.

NDR addresses the additional challenges of adhering to HIPAA and HITECH regulations, implementing NIST and HITRUST cybersecurity controls, and addressing vulnerabilities described in the MITRE ATT&CK framework, enabling healthcare organizations to increase regulatory compliance.

ExtraHop Reveal(x) helps healthcare organizations to improve both their security posture and compliance. It provides complete visibility and monitoring for both north-south and east-west traffic to detect and investigate threats faster. By enabling organizations to quickly understand the full impact of incidents, investigate, and respond Reveal(x) safeguards patient data, improves patient safety, and increases patient satisfaction.

Sources

[1] *https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech*
[2] *https://www.endpointprotector.com/blog/study-reveals-hospitals-vulnerability-to-data-breaches/*
[3] *https://www.hipaajournal.com/2019-healthcare-data-breach-report/*
[4] *https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far*
[5] *https://www.usatoday.com/story/tech/2020/10/06/ransomware-hits-health-care-organizations-hardest-says-check-point/3626931001/*
[6] *https://www.extrahop.com/company/blog/2020/security-alert-ransomware-warning-for-hospitals/*
[7] *https://www.forescout.com/company/blog/how-hospitals-are-dealing-with-the-cybersecurity-challenge-of-covid-19/*
[8] *https://www.usnews.com/news/healthiest-communities/articles/2020-06-02/covid-19-and-the-transformation-of-telehealth*
[9] *https://hipaasecuritysuite.com/hipaa-violation-fines-and-penalties-what-are-they-in-2020/*
[10] *https://assets.extrahop.com/whitepapers/Reveal%28x%29%20MITRE%20ATT&CK%20white%20paper.pdf*
[11] *https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and*
[12] *https://www.extrahop.com/company/press-releases/2020/new-compliance-for-hipaa/*

ABOUT EXTRAHOP

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. **Get Started at www.extrahop.com/freetrial**

ExtraHop

info@extrahop.com
www.extrahop.com