Avoiding Compliance Surprises – Healthcare Guide

A proactive guide for IT and security teams in the healthcare sector to stay ahead of compliance obligations, manage risk, and ensure the integrity of protected health information (PHI).

Healthcare organizations are popular targets for today's opportunistic cybercriminals, and medical security professionals are constantly updating security tactics to stay ahead. To protect life-saving systems and infrastructure, as well as sensitive patient data, it's essential to understand the kinds of threats that are out there, as well as the offensive *and* defensive measures that can prevent them.

Table of Contents

Section 1: The Evolving Healthcare Compliance and Threat Landscape

Healthcare has always been a highly guarded industry, and it's got the compliance landscape to prove it. Throughout the world, there has been an increasing focus on data privacy and patient protection over the past decade and a half, with updates to major healthcare frameworks like HIPAA being made as recently as this year.

With mounting scrutiny from regulatory bodies like the US Department of Health and Human Services (HHS) and its Office for Civil Rights (OCR), it is more imperative than ever that healthcare providers and medical facilities ensure their processes are above board where compliance is concerned. When you look at the threats to the healthcare landscape, you'll see why.

A recent House Energy and Commerce Committee Subcommittee on Oversight hearing was held to address the issue of threats to the healthcare industry. When asked why healthcare has become a particular target for attackers, as opposed to lucrative industries like finance, Mr. Garcia, one of the interviewed cybersecurity expert panelists, stated:

> *"[Healthcare] is a widely distributed, multifaceted ecosystem that has a lot of touch points, a lot of vulnerabilities. Secondly, there is less money to spend against cyber threats [than in industries like finance]. And thirdly, it's easy money. When you have a ransomware attack, if you are a hacker and you ransom a hospital, you are forcing the decision on the hospital: should I pay the ransom and continue to treat patients or should I not and run the risk of not treating patients and… going out of business."*

In the face of these large, external currents, rising threats to electronic health records (EHRs) and connected medical devices make compliance even trickier – and crucial. This means that internal policies that were once suitable for securing protected health information (PHI) may fall short in the face of these new dangers, leaving organizations not only vulnerable, but non-compliant. Healthcare groups are being forced to reassess their security strategies and compliance commitments as a result.

Pro Tip: Know the Consequences of Paying the Ransom

You hear it all the time: never pay the ransom. This may go without saying in some industries, but it can be especially difficult in the healthcare sector when human lives are on the line. Whether or not your organization decides to pay up is a personal choice, but every medical facility should understand the consequences either way.

Paying the ransom in a ransomware attack sends the signal that you are willing to do anything to retrieve stolen data, and that a similar tactic would work again. While being willing to sacrifice to protect patient privacy is admirable, noble, and even beneficial PR in front of customers, it can also backfire. A 2024 report notes that over 75% of healthcare organizations admitted to paying out over $500,000 in ransom demands as the result of cyberattacks. Unfortunately, 80% of companies that paid the ransom were hit again with another ransomware attack, and even after paying, over one in three were not given working decryption keys to recover their data.

Section 2: Key Healthcare Compliance Frameworks and Standards

Currently, some of the major US healthcare compliance requirements on the books include:

- **The HIPAA Security Rule** | This protects the electronic PHI (ePHI) of individuals and outlines standards for appropriate physical, technical, and administrative safeguards. This is similar to the HIPAA Privacy Rule (what most think of generally as "HIPAA"), which protects PHI in all its forms. By contrast, the HIPAA Security Rule protects ePHI, specifically.
- **The Omnibus Law** | Signed into effect in 2023, the Omnibus Spending Bill allows the Federal Drug Administration (FDA) to enforce cybersecurity requirements for medical devices.
- **The HITECH Act** | The HITECH Act incentivized the adoption of electronic health records (EHR), expanded HIPAA requirements to apply to Business Associates of Covered Entities, and strengthened the privacy and security provisions of HIPAA while introducing tougher penalties.
- **21st Century Cures Act** | The 21st Century Cures Act, established in 2016, makes the sharing of electronic health records standard practice, with a few notable exceptions. In cases like preventing harm, securing people and systems, and ensuring patient privacy, it is permitted to "information block" and deny the free exchange of EHRs.
- **NIST Cybersecurity Framework (CSF)** | While the NIST CSF is not mandatory for any but US government agencies, it can help healthcare organizations comply with HIPAA and other healthcare cybersecurity standards. OCR research revealed that 86% of Covered Entities under HIPAA (and 83% of Business Associates) did not meet expectations for a Risk Assessment. Complying with NIST can improve those figures. NIST has also issued additional healthcare-specific guidance in an effort to "help the industry maintain the confidentiality, integrity and availability of electronic protected health information."
- NIST SP 800-213 | NIST Special Publication 800-213 establishes guidance for federal entities when deploying IoT devices, including medical IoT devices, within their systems.

And internationally, the list includes:

- Canada's PIPEDA (The Personal Information Protection and Electronic Documents Act)
- The UK's Data Protection Act 2018 and
- Australia's Privacy Act 1988
- The United Arab Emirates' Health Data Law 2019
- Abu Dhabi's Healthcare Information and Cyber Security Standard (ADHICS)
- Singapore's Cyber & Data Security Guidelines for Healthcare Providers
- Korea's PIPA (Personal Informati on Protection Act)

With more always on the way.

Section 3: Common Pitfalls That Jeopardize Compliance in Healthcare

With so many varied requirements, it is easy to see how organizations can inadvertently make compliance errors. However, fines and penalties are levied regardless of intent, and reputational damage almost always follows. Here are some common ways in which healthcare organizations can fail to meet compliance standards:

- **Vulnerable medical devices and misconfigured IoT endpoints**
  Healthcare IT News reports that among healthcare organizations, "Endpoint misconfigurations emerged as a significant risk, with 35% of systems unable to quarantine malicious files, increasing susceptibility to ransomware encryption." In addition, recent research reveals that 63% of vulnerabilities found in CISA's Known Exploited Vulnerabilities (KEV) Catalogue "can be found on healthcare networks" and that nearly a quarter (23%) of medical devices are operating with at least one known exploited vulnerability.

63% of vulnerabilities found in CISA's Known Exploited Vulnerabilities (KEV) Catalogue "can be found on healthcare networks" and that nearly a quarter (23%) of medical devices are operating with at least one known exploited vulnerability.

- **Lack of centralized log management across EHR systems**
  Collecting log data and storing it in a central location gives security teams visibility over security incidents, compliance violations, and other impactful events that occur within an organization's network. Neglecting to put a centralized log management system in place for EHR records could leave many important electronic health files in the lurch, out of the line of sight of SOCs, and vulnerable to outside attack.
- **Inadequate access control and user provisioning**
  In 2024, OCR research revealed that 25% of healthcare breaches were "due to individuals without proper authorization accessing sensitive healthcare information or these data being disclosed to individuals without proper protocols." Speaking of the EMEA region specifically, the 2024 Verizon Data Breach Investigations Report noted that "virtually half of the breaches (49%) in EMEA are initiated internally, suggesting high incidences of privilege misuse…" Unfortunately, many healthcare compliance breaches are caused by friendly fire, and often by employees accessing data that they don't know they shouldn't be accessing. Without the proper security protocols in place, there is nothing to stop them.
- **Failure to detect or respond to insider threats**
  Research reveals that eight healthcare industry data breaches, impacting a total of 98,936 patients, were due to possible insider threats. Detecting these subtle, malicious behavioral patterns can be like finding a needle in a digital haystack.

Pro Tip: Any Industry Could be Handling Healthcare Data

More and more often, even non-healthcare-related entities find themselves handling electronic health data, from fitness apps that track your heart rate to pop-psychology sites that ask you questions about your mental health. While not a healthcare organization, the Olympic Games and related affiliates are trusted with athlete health information, and now even the workers themselves are not exempt. As privacy and security culture make their way into the mainstream, the need for non-healthcare-related entities to still comply with PHI privacy laws will only increase – as will the opportunity for error.

Section 4: Five Key Security Controls to Maintain Compliance

Asset Discovery and Inventory

It's a tired phrase, but still true as ever; you can't defend what you can't see. The same goes for compliance, as it's unlikely that unaccounted for assets can be adequately put within the realm of compliant policies, and shadow-IT is a ticking time bomb when it comes to hidden attacks. To begin your healthcare organization's journey of maintaining (or attaining) a fully compliant stance, asset discovery needs to include:

- **All network devices.** Start with basics like computers, workstations, printers, scanners, BYODs, mobile devices, and iPads.
- **EHR systems.** Leave no stone unturned when it comes to tracking where all electronic health records are kept, how they are stored, and the systems for transferring them, saving them, accessing them, and more. These are "jackpot" articles for attackers, who love to exfiltrate data-rich health paperwork and sell it on the dark web.
- **Medical and IoT devices.** These include things like heart monitors, infusion pumps, patient monitors, and IoT devices used to monitor patient vitals remotely. These are critical bearers of sensitive patient information, in structured and unstructured formats, and their accessibility should be strictly monitored and limited to a "principle of least privilege" basis.

Secure Configuration Management

Configuration management can be overwhelming in an industry like healthcare, where widespread medical groups can have thousands of configurations to manage. When done manually, the task is a nightmare. A security configuration management solution can automate that time-consuming, error-ridden process and help large healthcare systems reduce errors when deploying and configuring innovative new technologies.

Vulnerability Management

Security misconfigurations are just one of the many vulnerabilities troubling healthcare, especially when it comes to medical devices and legacy systems. As noted in The HIPAA Journal, "medical device hardware can remain functional for 10 to 30 years; however, the life cycles of the medical device software are much shorter. Once software reaches end of life and security updates stop being provided, vulnerabilities will no longer be fixed."

Legacy medical devices are defined as those that cannot withstand modern cyberattacks. The list includes intracardiac defibrillators, pacemakers, mobile cardiac telemetry devices, and more, mentioned above. In the Subcommittee on O&I hearing, it was established that "healthcare is a widely distributed, multifaceted ecosystem that has a lot of touch points, a lot of vulnerabilities," and that there are "easily 10,000,000 [medical] devices that exist" - each a potential carrier of these vulnerabilities.

To stay ahead, patch management programs need to be put in place, as well as vulnerability management systems that automatically prioritize vulnerabilities based on patient impact.

Log Collection and File Integrity Monitoring

Logs are the lifeblood of incident detection. The ability to not only collect them but *decipher* them is the key to catching criminals in the act. However, a healthcare organization uses about 45-76 security tools on average, and the number of logs and alerts those can generate can be hard to manage. An all-in-one tool like an extended detection and response (XDR) platform is necessary to un-silo telemetries and view all logs at-a-glance, plus additional behavioral-driven threats.

Additionally, HIPAA requires file integrity monitoring (FIM) to be in place so medical groups can further detect early signs of compromise. Compromise at the file level, such as encryption, can be one of the first indicators of an ongoing attack. File integrity monitoring notifies teams of unauthorized changes and verifies that files are untouched, helping to prove compliance and pass HIPAA audits.

Audit-Ready Reporting and Alerting

No one knows better than the medical industry that sometimes, despite your best efforts, things fall apart. When breaches do occur, the best you can do is have a well-documented audit trail and follow applicable breach reporting policies. The HIPAA Breach Notification Rule, for instance, states that in the event of a breach affecting unsecured protected health information, covered entities must notify the individuals affected, the Secretary of the Federal Trade Commission (FTC), and in some cases, the media.

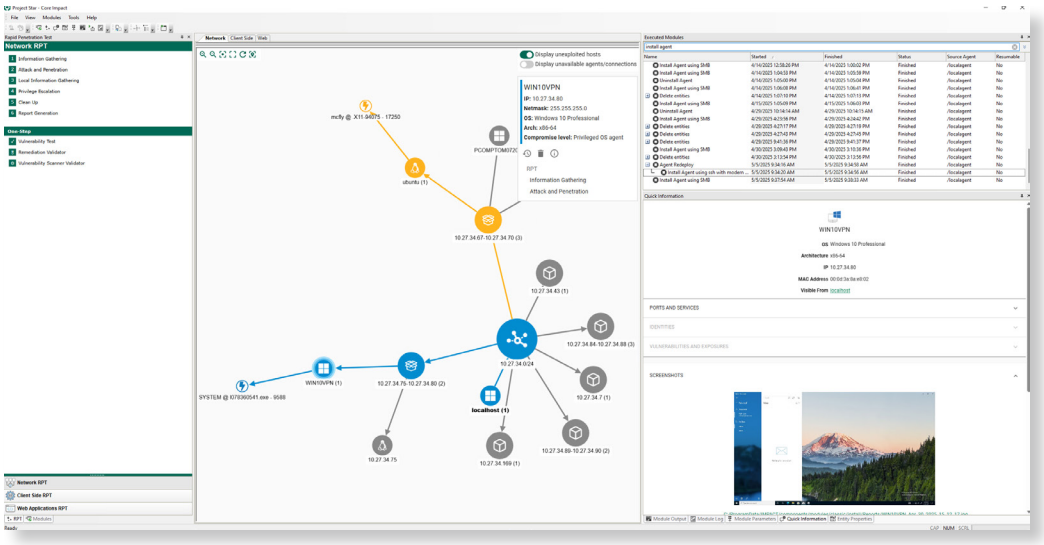
As for the audit, being audit-ready means having logs in place that reflect user activity at the time of the compromise; who accessed ePHI, what the action was, timestamps, the involved systems, and more. Putting a plan in place to automate your system and audit reporting now can set the stage so when accidents do occur, you won't have to scramble to prove compliance.

Section 5: How Fortra Can Help

Fortra's cybersecurity solutions for healthcare support healthcare compliance and cybersecurity with multiple layers of protection, including offensive and defensive security tactics.

Offensive Security Tools

Fortra offers offensive security tools to empower your penetration testers and red teamers to do thorough analysis and attack simulation. Core Impact penetration testing software, for example, provides a host of certified exploits, a centralized toolset, and an automated walk-through that even inexperienced practitioners can follow to test for ransomware inroads and exploitable vulnerabilities. Red team tools Cobalt Strike and OST give red teamers the ability to conduct advanced adversary simulation using the latest in evasive tactics. These simulations will highlight areas of weakness in the organization's software, hardware or physical infrastructure so that blue teams can shore up weaknesses before attackers can exploit them. Core Impact, Cobalt Strike, and OST are interoperable tools, allowing session passing and tunneling capabilities, among others, to create more advanced, streamlined engagements.



Monitoring, VM and other Defensive solutions

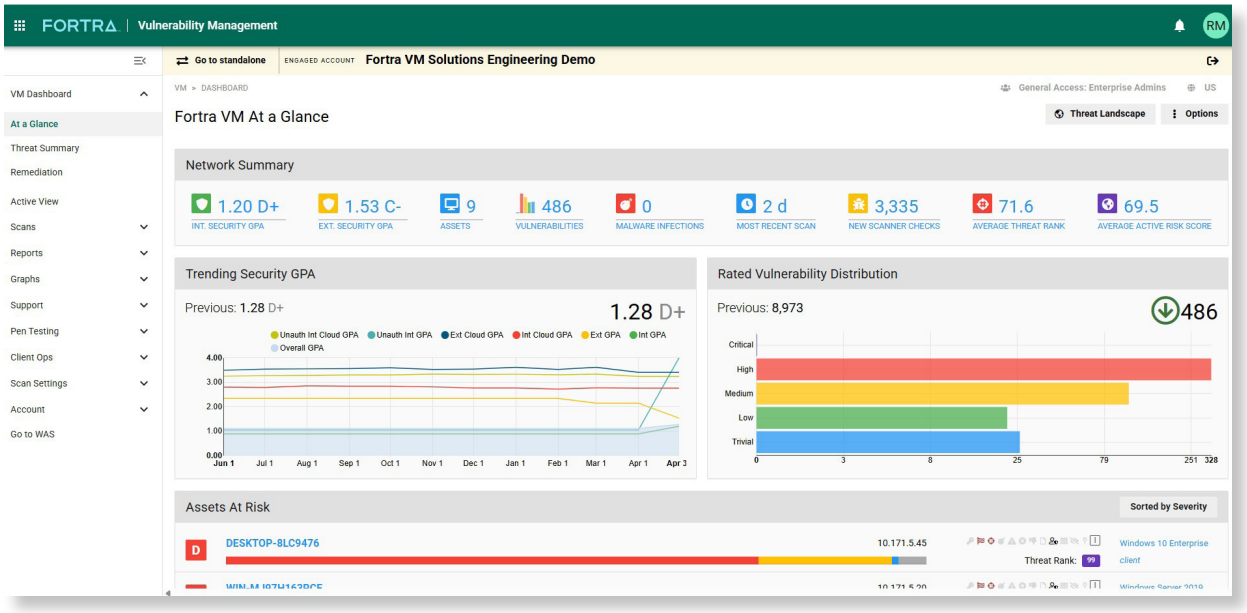
Fortra helps healthcare organizations detect unauthorized changes and enforce security configurations that align with HIPAA, HITECH, and other compliance frameworks. Heathcare providers must introduce new IT changes into their networks to serve patients best. The right change management software can help keep security risks to a minimum while organizations make necessary adjustments to the technicalities of patient care.

Tools like Fortra's Tripwire Enterprise and Fortra's Digital Guardian support visibility into sensitive data usage and potential misuse, helping maintain audit trails and prevent data leakage. With Tripwire Enterprise, check the configuration and integrity of not only your files, but your servers, endpoints, operating systems, medical IoT devices, and more. Know who changed what (and when) as you keep a clean audit trail of all changes made to in-network systems.

Leveraging Digital Guardian, you can locate sensitive information across your healthcare system's disparate assets and get full visibility into all hardware, software, data movement, data storage, and data creation within your environment.

Fortra Vulnerability Management assesses your healthcare organization's security posture, providing analysis and prioritization of your highest risk weaknesses, so you can address them swiftly. On demand scanning and reports show the impact of remediation instantly and help your security find and fix vulnerabilities in your infrastructure before attackers do.

Where email is concerned, Fortra's email security and anti-phishing tools go above and beyond searching for signature-based malware threats alone; its Integrated Cloud Email Security (ICES) solution spots hard-to-catch ploys like social engineering scams and Business Email Compromise (BEC) attacks.



Fortra solutions offer reporting features that make it easier to demonstrate continuous compliance during audits. Show hospital executives and auditors alike the "big picture" as technical security metrics are displayed in terms of business objectives. Plus, get all stakeholders on the same page – security teams, medical managers and staff, and top healthcare leaders – with reports and dashboards accessible from any device, at anytime, anywhere.

Conclusion

Fortra's wide-ranging security portfolio helps overwhelmed healthcare security professionals protect their PHI and ePHI and stay ahead of today's aggressive industry-targeted threats.

By allowing Fortra to do what it does best: provide the right suite of solutions to make compliance as streamlined as possible, healthcare providers can be free to do what *they* do best: innovate the technology systems that save human lives.

FORTRA™

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

(fta-gd-0425-r1-gm)