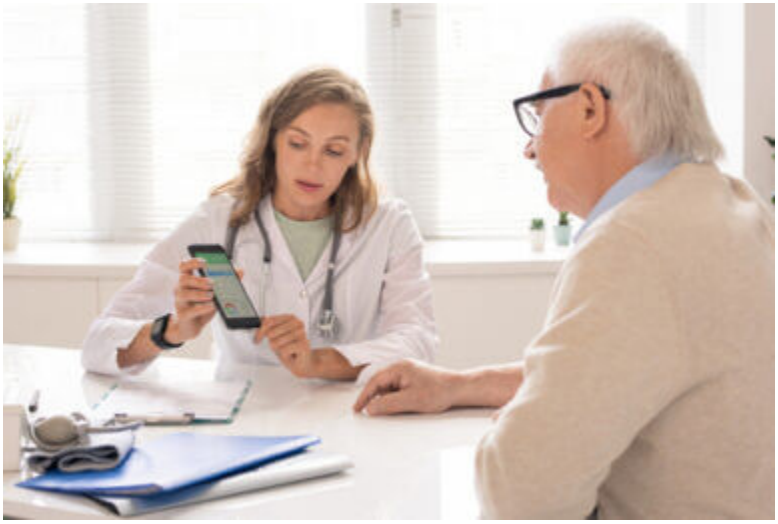
The Importance of Cyber Security in Healthcare



ARTICLE 03.17.22 DEAN DORTON

Modern medical advances have ushered in an era of greater precision in healthcare, leading to better patient outcomes and hope for a healthier future.

Still, as healthcare providers become increasingly reliant on digitization to deliver timely, modernized care, they have simultaneously become appealing targets for cyber criminals. And the stakes to protect the high-value data stored and shared — for patients and organizations alike — couldn't be higher.

Cyber attacks on healthcare systems and providers of all sizes have seen a sharp uptick since the beginning of the COVID-19 pandemic. Threats continue to grow as the number of connected devices across more networks increases. Combined with cloud services gaining in popularity, this creates a larger attack surface for bad actors constantly evolving the sophistication of their efforts. Everything from patient admissions information and payment records, to private **electronic health records** (EHRs), e-doctor visits, medical device wearables, and portable medical technologies can all be susceptible to compromise.

But a healthy cyber security posture can help defend against more than just an attack on a network, devices, or even an organization's reputation: It can aid in protecting the most vulnerable among us.

By understanding the challenges at hand and putting mitigation efforts in place, healthcare providers can work toward the all important triad of confidentiality, integrity, and availability of information. Meanwhile, they ensure access to vital patient data at the most crucial moments in the continuum of care.

Challenges of cyber security in healthcare

While few (if any) industries are exempt from cyber threats, healthcare is one of the most highly targeted industries today. In fact, hospitals in the U.S. currently account for 30% of all large data breaches, with over **one and a half million records** breached in February of 2020 alone. When the dust settled by the end of the year, the cost of all breaches to healthcare companies was **a staggering $6 trillion.**

What makes healthcare vulnerable

The obvious reason healthcare organizations are such an attractive target is the sheer amount of personal and sensitive information they must traffic and store. Data particularly appealing to cyber criminals include a patient's **protected health information** (PHI) like credit card and bank account numbers, and **personal identification information** (PII), such as social security numbers. It's an extremely lucrative enterprise: stolen health records may

sell for up to 10 times or more than stolen credit card numbers on the dark web.

The potential cost to patients if their privacy or sensitive information is stolen is only part of the equation.

For healthcare organizations, the cost to remedy breaches is **almost three times that of other industries**. The simple fact is that providers can't afford to go without critical care and other medical records at the ready. In cases of a ransomware attack, for instance, corporate suite decision makers are left with few options but to pay whatever is asked — or take other drastic measures. It's been reported that nearly half (48%) of U.S. hospitals have been forced to altogether disconnect their networks since March of 2021 due to ransomware attacks.

What's more, there can often be intellectual property information, proprietary medical research, and innovation ramifications affecting more than just an annual bottom line. The chaos of losing a competitive advantage in the marketplace can put the future of entire organizations in jeopardy.

How compliance impacts healthcare

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal requirement that establishes national standards to protect individuals' medical records and other identifiable personal information.

Two of the primary components are the Privacy Rule and Security Rule, which limit what information can be disclosed, how it can be used, and the guidelines that dictate how to handle critical protected health information. These regulations must be considered in virtually every process, from the care providers themselves, to the cloud service partners, to the cleaning crews hired.

The penalties for failing to be HIPPA-compliant vary depending on the severity of the violation, but can be broken down into four tiers:

- Tier 1: A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA rules. **Minimum fine of $100 per violation up to $50,000.**
- Tier 2: A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. **Minimum fine of $1,000 per violation up to $50,000.**
- Tier 3: A violation suffered as a direct result of "willful neglect" of HIPAA rules, in cases where an attempt has been made to correct the violation. **Minimum fine of $10,000 per violation up to $50,000.**
- Tier 4: A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation. **Minimum fine of $50,000 per violation.**

Who cyber security helps protect

Everyone who comes into contact with any part of the continuum of healthcare has a vested interest in the strongest, most robust cyber security to help protect against attacks and keep information protected.

Each group presents a different perspective that must be considered. Within each of these groups come certain expectations of the care needed, delivered, and responsibilities to be communicated as well.

- **Patients:** From their personal health and wellness to personal finances, this group has perhaps the biggest stake in healthcare cyber security. Cyber attackers can make incredible amounts of money by way of leaked data, or by leveraging personal and health information to access private accounts, as well as by ordering expensive medications for resale through legitimate cardholders.
  With the proliferation of telehealth, e-visits, and e-pay systems, healthcare providers can help protect patients by educating them on the most effective ways to securely communicate with their providers.

- **Healthcare providers:** All healthcare providers, from clinicians to billing departments to executives in the C-suite, have a role to play in enhanced cyber security. They are the eyes and ears of the organization, able to identify irregularities on the front lines. It's crucial they are trained in HIPAA standards and understand established security policies.

More healthcare organizations now have a chief information security officer (CISO) in place to make executive decisions about the cyber security program. CISOs typically work on strategy, and ideally on the same level as other C-suite executives, such as the chief financial officer, chief information officer, and so on.

- **Vendors:** Many healthcare organizations rely on hundreds or even thousands of vendors to operate successfully. These can include everything from payroll to HVAC specialists, to every other service necessary for daily operations.

Much like supply chain attacks in other industries, cyber criminals can use smaller, unsuspecting vendors as a stepping stone to access credentials to larger organizations for greater paydays.

The most common healthcare cyber threats

As the technology we rely on to deliver cutting-edge care continues to advance, so too do the complexities and stealth of cyber attacks.

The most common purpose of an attack, as we've noted, is accessing sensitive information to either sell or for personal use. The methods of these attacks, however, can be as varied as the attackers, including destruction of data and industrial espionage.

In the context of healthcare cyber security, here are a few threats causing the greatest damage to bottom lines — and reputations.

Ransomware

When a machine or a device is infected by ransomware, the files and other data are typically encrypted, access is denied, and ransom is demanded. Patient care services are particularly vulnerable to this type of attack due to their high dependence on technology combined with the critical nature of their daily operations. In fact, ransomware attacks on the sector occurred at a rate of four incidents per week in the first half of 2021.

Health records are a low-risk, high-reward target for cybercriminals because each record can fetch a high value on the underground market. Unfortunately, ransom payment doesn't always result in the return of the stolen information.

Phishing

Many significant security incidents are caused by a variety of phishing attacks. The effectiveness can be attributed to criminals targeting the weakest link in the cyber security chain: people. Unwitting users may click on a malicious link or open a malicious attachment and infect their computer systems with malware that ultimately divulges information or enables access to it.

Cloud Storage Threats

Many healthcare providers have been switching to cloud-based storage solutions for greater convenience, and an "always on" connectivity. Unfortunately, not all cloud-based solutions are HIPPA compliant, making them easy targets for intruders. Threats include improper access management, data breach, data leak, loss of sensitive data, and misconfiguration of cloud storage. What's more, some organizations don't properly encrypt the data — or implement restrictions — before transmitting.

Be sure to utilize a private cloud or an on-premise data center to regularly secure and encrypt data.

Internal Threats

In our high-level primer on cyber security, we share research indicating that 90% of cyber claims stem from some type of human error or behavior. As more healthcare professionals access sensitive patient information on more devices — some that are still unsecured — the likelihood of an attack increases. While some internal threats can be malicious,

most are the result of negligence or unwitting compromise.

10 healthcare cyber security best practices

Across every healthcare organization — from major hospital systems to private clinics — cyber criminals are continually probing weaknesses to find entry points. Their attacks are increasing at significant rates, improving in how they're delivered and the damage they can produce.

While there's no way to prevent every attack, here are 10 tips to begin instilling a culture of cyber security that can help mitigate cyber attack frequency or effectiveness.

1. Educate the entire healthcare staff

Despite best efforts and top technology, human error is still the primary culprit for healthcare data breaches. With consistent annual training, organizations can help limit the chance that employees will click on malicious links, overlook an inconsistency, or accidentally violate HIPAA policies.

Some areas of training to help workers better anticipate and prepare for cybersecurity threats include:

- Using real-world cyber attacks (like phishing examples) to help spot scams
- Creating awareness of suspicious external *and* internal activity
- Understanding existing and new policies, including who to alert in the event of a threat

2. Restrict access to sensitive information

Adopt a zero-trust mentality, providing access to only those who require sensitive patient information to perform their roles as the standard. Implementing technology such as two-factor authentication and complex password requirements can also help limit unauthorized access, and empower those with access to be more mindful in accessing data.

3. Email security

For so many across the healthcare industry, email is the primary means for communication.

As we grow more dependent on mobile devices, it's important to be aware of the sensitive information that gets created, received, sent, and transacted within email systems. Managing mailbox storage capacities is one way to prevent sensitive data from sitting in inboxes, unnoticed and unaccounted for.

4. Plan for breaches while aiming to prevent them

Overcoming the perception that "it can't happen to us" is one of the toughest challenges. So for starters, assume a data breach has already occurred, and understand that simple compliance does not ensure data security.

This mindset is key in preparing employees with not only what to look for, but how to create a comprehensive response strategy and recovery plan. Outline how your organization will attempt to recover lost information, and detail notifications to those affected. It's also a positive way to demonstrate publicly that any potential data loss will be handled responsibly and appropriately.

5. Protecting data in transit and at rest

Encrypting data in its "at rest" state while untouched in a server can keep it protected during a breach. It's also necessary to encrypt data while in transit, especially when being sent to or shared with someone outside of the primary network.

6. Secure all physical assets

Not only must private files and sensitive information be secured — the very devices themselves that exist in the EHR system must also be protected. Smartphones, laptops, tablets, medical equipment, and wearable devices can all be threats when not managed properly no matter how well controls and file permissions are installed. It's possible that physical exploitation of a device left behind or stolen could defeat any technical controls.

Ensure strict personal device regulations, and policies that frequently account for devices. Be sure to also securely and properly dispose of/destroy devices no longer in use. One single weak link — even if no longer in use — can put an entire system at risk.

7. Address legacy systems

Legacy systems are those systems no longer supported by the manufacturer. They may include applications, operating systems, and even the hardware itself. These legacy systems may still be in use due to cost of upgrading or because an upgrade may not be available. Other issues can stem from lack of awareness or indifference to the need. It's important to update these legacy issues as you're able.

8. Keep software updated

Cybercriminals can take advantage of holes in outdated software. Updates often include security updates that keep the attackers guessing. Utilize two-factor authorization, and strongly encourage frequent strong password updates.

9. Assess all associated vendors

Properly vetting the vendors that will be introduced into your EHR system — regardless of size or function — is mission critical. While the valuable and sensitive patient information you're charged with protecting should be housed in ways not available to every user, it can be a challenge to check and safeguard every potential access point.

10. Perform regular risk assessments and/or audits

No facility or system is exactly the same. So checking and testing your healthcare organization's cyber security posture that calls attention to gaps surrounding vital data should garner your full attention to help devise the roadmap to recovery.

Pursuing cyber security assessments and audits can prove your commitment to preserving all sensitive patient information to key stakeholders and the public alike. Perform these regularly to not only keep pace with an evolving technological landscape, but to separate your organization from the rest as well.

Cyber security: as vital as the care delivered

The trust that patients have with their healthcare providers exists on many levels, from care they need, to where they're best treated, to what treatment will produce the most favorable outcome.

But with the relatively recent digitization of the industry, the trust that sensitive personal information is protected has become a major concern — for patients and organizations alike. A strong healthcare cyber security strategy can help any provider maintain a trustworthy reputation, avoid financial issues and other penalties, and improve the adoption of technologies and efficiencies.

Give your healthcare organization a first step in the right direction to mitigating risks, safeguarding your valuable data, and protecting your reputation. Connect with Dean Dorton for a cyber security risk assessment today.

And for more insights and analysis be sure to subscribe to our blog.