How Secure is Your Health IT?

7 Steps to Protect Against Vulnerabilities

PARAGON CONSULTING PARTNERS

PCPIMAGING.COM

Contents

Top Health IT Security Concerns

Security has always been a top-of-mind concern for healthcare organizations because of the critical and confidential nature of the information they generate and house. Recently security has become a hotter topic than ever among healthcare IT professionals, largely due to the recent surge in ransomware attacks worldwide, but also because of the growing volume of data and the increasing complexity associated with the web of systems and devices generating and accessing it.

Emerging Vulnerabilities

For instance, consider the paradox associated with the rapid emergence and adoption of Wifi or Bluetooth enabled medical equipment, mobile devices, and IoT applications within the healthcare realm. For example, equipment such as drug infusion pumps and defibrillators equipped for remote monitoring and control can improve and simplify patient care for clinicians,

however if an intruder were to gain control of these life sustaining systems there could be very serious ramifications. Similarly, while mobile and IoT applications that provide 'anytime, anywhere' information capture and viewing capabilities are invaluable for closing the information gap, most have weak and inconsistent security controls and as such can expose health networks to vulnerabilities – in fact, nearly half of US firms using such devices are reported to have experienced a security breach as a result.

Unfortunately, hackers recognize the value of the information contained within patient health records, making healthcare the largest target for ransomware attacks compared to any other industry. Not only are covered entities subject to financial penalties under the Health Insurance Portability and Accountability Act (HIPAA) for breach of protected health data, but even worse - such records can be rendered inaccessible by attackers, who can withhold potentially life or death information from care providers until a ransom is paid. The result is significant fiscal and clinical implications for providers and patients.

There are many methods available for resourceful attackers to wreak havoc on an unsuspecting healthcare organization. In addition to the popularized ransomware attacks, other potential breaches could include brute force attacks, where attackers attempt to decipher valid user credentials in order to gain access to the system – either to access protected data, or to install malware.

Additionally, Distributed Denial of Service (DDoS) attacks take a different brute-force approach, inundating systems with repeated requests that overwhelm servers and prevent legitimate traffic from making it through – effectively rendering the system unusable.

As well, it's important to remember that breaches are not always technical in nature - the human element must not be ignored. Human error has long been a leading contributor to security breaches as a result of poor user management such as weak passwords or infamous sticky notes containing credentials for all to see.
Even with proper controls in place to mitigate these obvious risks, clever social engineering can also be leveraged by attackers to gain access to critical systems.

This is by no means an exhaustive list, rather it is merely a few examples of the potential threats that exist. To mitigate these and other vulnerabilities requires a multi-faceted approach, beginning first and foremost with implementing effective policies and procedures for controlling system access by internal and external stakeholders, and extending to more sophisticated technical security controls. In the sections that follow we outline 7 tangible solutions that can be implemented to protect against vulnerabilities and improve your healthcare IT security.

7 Steps to Protect Against Vulnerabilities

1. Two-Factor Authentication

The most common authentication method in most healthcare organizations today remains the tried and true username/password combination. However, even with strong password policies in place (character limits, alphanumeric requirements, and automatic expiry) they're still not quite good enough to thwart a tenacious attacker. Two-factor authentication ensures an additional protection layer is in place, often in the form of a physical or biometric control, such as swipe cards, security tokens, finger print scanners, or facial recognition. While all offer an additional degree of security, and another hurdle for an attacker, the latter two offer the strongest protection while minimizing risk of forgetting or misplacing security devices.

2. Security Monitoring & Alerts

Most healthcare IT systems in use today have some form of proactive monitoring that notifies IT staff of potential issues, such as performance degradation, storage capacity, or unanticipated outages. Similarly, security monitoring systems can identify usage patterns and alert security personnel when exceptions arise. For example, multiple failed login attempts for one or more users (Brute Force attacks), or repeated and aggressive requests (Distributed Denial of Service attacks – DDoS) that could bring a system to its knees. By quickly identifying potential security risks steps can be taken to resolve the issue before the system is compromised.

3. Encryption at Rest

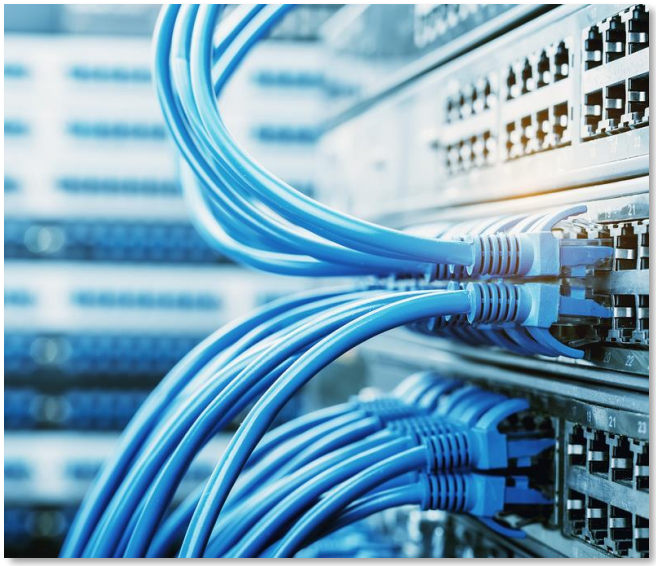
A top of mind concern for IT departments is secure encryption of data when it's in transit – especially if it will be leaving the secure network to an outside location, such as a teleradiology network, referring physician's office, or even a patient portal. While this protects the movement of data, too often when the data is sitting idle in storage it is unencrypted, and therefore unprotected should an access breach occur. Encrypting data at rest provides an additional layer of security that would prevent a would-be intruder from deciphering or distributing the data in any meaningful way, even if they were to gain access.

4. Whitelisting

Whitelisting, sometimes referred to as Application Control, involves limiting the applications, users, systems, and devices that can connect to your network to those explicitly listed on the 'whitelist'. Not on the list? You are denied access. There are a number of ways to manage whitelisting, including domain names, file and folder attributes, digital signatures, cryptographic attributes, physical or IP addresses, and more. While maintaining a whitelist may seem cumbersome, it is an effective method for protecting against vulnerabilities that can be introduced by external users and devices that are not under the control of your IT department and therefore not subject to the same security scrutiny as your own internal systems.

5. Maintain a Secure Backup of your Data

In the event a security breach occurs, ensuring a reliable backup copy of your data is available, and a well-tested recovery plan is in place, can minimize the impact and allow operations to continue with minimal, if any, interruption in care delivery. To be effective for protection against attacks that are targeted at data availability or consistency is important to ensure that backups are geographically separated and cordoned off from production systems and networks to ensure they are not directly connected to compromised systems.



6. Blockchain

A forward-looking option, Blockchain is a new innovation that is not yet widely adopted within the healthcare industry yet offers significant promise for delivering a highly secure and reliable method for exchanging information. With Blockchain no one entity has complete ownership or control of the data, rather it is securely distributed across a system of participating entities who collectively store, track, and validate information and transactions. Any update or change in data is recorded in an immutable ledger, and in order for a piece of data to be deemed 'true' consensus is required across the Blockchain. This technology enables unencumbered access to patient health records while virtually eliminating the possibility for data to be maliciously deleted, altered, or otherwise tampered with.

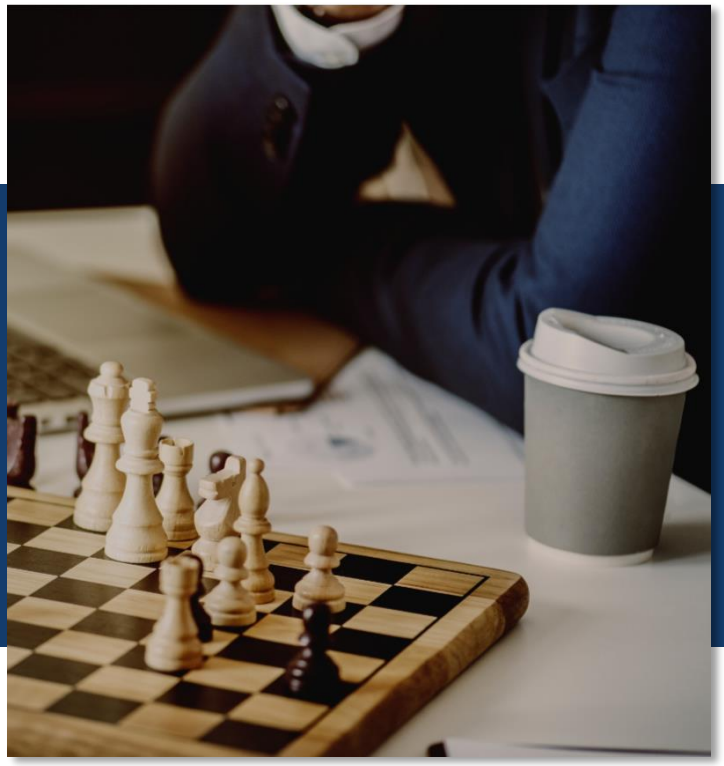
7. Look to the Experts

Another common issue within many healthcare organizations is the lack of true security expertise within the IT team. Due to budget constraints, many IT personnel are called upon to be 'jacks of all trades', mastering storage, server and workstation hardware, virtualization, and software management, and more – all in addition to setting up and managing network and software security management. Each of these are considered a professional discipline in themselves and require continuous education and practical experience to execute well. In order to ensure your data and systems are well protected it is necessary to engage a security expert. This can take the form of a full-time employee, if budget allows, or engagement with an expert resource such as an experienced consultant who can help define and execute security controls and processes, as well as educate your team on best practices for ongoing operations.

Define & Execute a Tailored Strategy

Finally, it's important to keep in mind that while security is a ubiquitous requirement across the healthcare industry, like many other facets of healthcare IT, it does not offer a once-size-fits-all solution. Selecting and implementing security controls that will work best for your organization requires a thoughtful analysis of your current operations and policies, including clinical workflow and technical dataflow – both within and outside your organization – to identify critical integration points and potential vulnerabilities and inform a complete, tailored security strategy to protect your business and patients, without compromising the efficiency or efficacy of your care delivery services.

We can help you craft and execute comprehensive security strategies to protect your data and your patients. For more information contact pcpimaging.com.



About PCP Imaging

We are a team of passionate healthcare professionals with more than 100 years of collective clinical, technical, and business leadership experience within the healthcare IT and imaging fields. Each partner contributes a unique set of skills that together guide collaborative efforts to unify and improve healthcare delivery alongside our care provider and vendor partners.

Offering a wide variety advisory, consultative, and professional services for healthcare organizations and industry vendors our experts can bring relevant experience to your unique situation to augment your team, accelerate success, and increase your return on investment.

Contact Us

PCPIMAGING.COM

PARAGON CONSULTING PARTNERS

500 Capitol Mall, Suite 2350
Sacramento, CA 95814
916.382.8934
info@pcpimaging.com
pcpimaging.com