Med Tech Solutions

HEALTHCARE IT SECURITY SERIES

Technical Risk Mitigation

Best practices in applying security standards

A risk-based approach to IT security focuses efforts on the technical controls that are most appropriate, based on the risks the organization is exposed to. This approach depends on existing standards to provide flexible, scalable, and cost-effective techniques that improve healthcare organizations' security posture over time.

TECHNICAL SECURITY CHALLENGES FOR HEALTHCARE PROVIDERS

The 2019 American Medical Collection Agency (AMCA) breach exemplifies many of the technical challenges that healthcare providers face today.

With a billing vendor of the major lab companies for the entire industry at fault, the breach affects nearly every provider's patient population, and monitoring for losses is insufficient. While that is just one event, healthcare data breaches cost the industry about $4 billion in 2019, and that number was expected to increase in 2020.[1] The ever-growing volume of valuable online personal health information (PHI) creates an increasingly attractive target for hackers.

13.6% **of breaches reported across all industries in Q1 2019 were specifically targeted against healthcare organizations.[2]**

67.6% **of healthcare organizations that were breached during this period cannot report how many records were lost or exposed.[2]**

14.7% **of all breaches involving medical records were exposed through the Internet.[2]**

Critical steps in addressing these attacks include improved network and data configurations, maintenance, and management by covered entities (CEs) and business associates (BAs). This requires that they take a risk-based approach to technical best practices for IT risk mitigation, data security, and regulatory compliance.

A risk-based approach to technical controls helps organizations be more efficient and cost-effective by identifying and focusing efforts on the controls that are most appropriate, based on the risks the organization is exposed to. This approach depends on existing standards to provide flexible, scalable techniques that improve healthcare organizations' security posture over time.

TOP 10 HEALTHCARE DATA BREACHES IN 2019[2]

1. **AMCA DATA BREACH**
   25M patients affected, investigation ongoing
2. **DOMINION NATIONAL**
   2.96M patients affected
3. **INMEDIATA HEALTH GROUP**
   1.5M patients affected
4. **UW MEDICINE**
   973,024 patients affected
5. **WOLVERINE SOLUTIONS GROUP**
   Estimated 600,000 patients affected
6. **OREGON DEPARTMENT OF HUMAN SERVICES**
   645,000 patients affected
7. **COLUMBIA SURGICAL SPECIALISTS OF SPOKANE**
   400,000 patients affected
8. **UCONN HEALTH**
   326,629 patients affected
9. **NAVICENT HEALTH**
   278,016 patients affected
10. **ZOLL SERVICES**
    277,319 patients affected

Standards to address technical risks

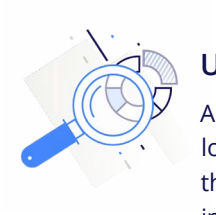
Healthcare organizations are required to protect personal health information in all forms, including electronic PHI. The HIPAA Security Rule (45 CFR 164.304) describes multiple standards that define the technology, as well as the policies and procedures for its use that protect electronic PHI and control access to it. These technical safeguards can be a wide range of security measures that allow organizations to reasonably and appropriately protect patients' PHI. If an organization has documented the risk-assessment process and appropriate investments and still suffers a breach, that documentation can help reduce subsequent fines.

Although no specific solutions are required, the standards indicate that organizations must know where their risk lies and add safeguards appropriately.

ACCESS CONTROLS STANDARD

The HIPAA Security Rule defines access as "the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource." There are four implementation specifications associated with this standard: **UNIQUE USER IDS**, **EMERGENCY ACCESS PROCESS**, **AUTOMATIC LOGOFF**, and **ENCRYPTION & DECRYPTION**.

Unique user IDs and emergency access are required, while automatic logoff and encryption are addressable. That means that while an organization may not be required to implement these, they must have a documented risk assessment detailing why they are not required.

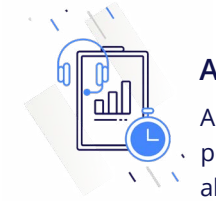


Unique user IDs

A unique name or number for each system user identifies and tracks their activity whenever they are logged into the system. This allows the organization to hold the user accountable for any functions they perform, and allows alerts to be set and audit reports to be run to account for how and where information was accessed. This does not change, even if the organization implements multifactor authentication (MFA). If a breach is discovered due to unique user IDs being bypassed, such as in an exam room used by multiple providers, the organization could be liable for willful neglect.

Emergency access procedure

A process must be defined for obtaining necessary PHI during an emergency. This specification normally occurs when the electronic health record (EHR) is unavailable, such as during severe weather events or other emergencies that prevent the workforce from being able to make it to the office. Access controls are still required under these emergency conditions. Whatever an organization defines that would require emergency access must be documented and in place, with staff trained in the process.



Automatic logoff

Automatic logoff implements electronic procedures that terminate a session after a predetermined period of inactivity. This is a failsafe for when users forget to log off when leaving a workstation, but also includes network logoff, which can be different and must be addressed within each practice and workflow. Auto logoff is an effective way to prevent unauthorized users from accessing systems and PHI when left unattended, and most networks and healthcare applications include this option.

Encryption/decryption

Encryption/decryption, which implements a mechanism to encrypt and decrypt PHI, is one of the most misunderstood specifications. Encryption/decryption can be handled by the application, using database encryption or encoded fields, and can also be part of transport, providing encryption from end-to-end. It can also be addressed in storage systems. Even if the data cannot be encrypted in a reasonable way, organizations must determine if encryption is warranted. In today's IT environment, it is highly unlikely that risk-assessment mitigation would not indicate encryption as a valid control, but there are times when other controls and technologies are adequate. Organizations that feel strongly about not encrypting must be prepared to answer tough questions from an auditor, along with documenting all the other compensating controls that may minimize the need for encryption.

AUDIT CONTROL STANDARDS

There are no formal implementation specifications for audit controls, but organizations are required to have hardware, software, or processes that record and examine the activity in all of the systems that contain or use PHI. Most systems provide some level of audit capability, and despite the fact that audit controls can be one of the least-expensive safeguards, these are often not enabled or used. For many organizations, defining and using an audit process as part of an overall risk assessment can help compensate for other technical controls that may be too expensive.

> Despite the fact that audit controls can be one of the least-expensive safeguards, these are often not enabled or used.

INTEGRITY STANDARD

In IT and healthcare practices, integrity is defined as proving that data or information has not been altered or destroyed in an unauthorized manner, which can affect quality and patient safety.

Integrity is threatened by ransomware, but is also threatened by the broad attack vector of the Internet of Things (IoT), where billions of devices connect through the Internet to record vital statistics, health information, or even ongoing monitoring of a person's health. If data that warrants care intervention is removed or altered, this affects patients' health as well as their privacy. Similarly, there have been recent efforts to breach picture archiving and communication systems (PACS) and edit images to create chaos in patient treatment and cause additional expense and time.

Beyond hackers, integrity issues can easily occur by workforce or business associates who make accidental (or intentional) changes that can alter or destroy records. Data can also be altered or destroyed by media failures. Integrity controls should be assigned so that authentication is tied to PHI and integrity checks, including time stamps or checksums.

> Beyond hackers, integrity issues can easily occur by workforce or business associates who make accidental (or intentional) changes that can alter or destroy records.

PERSON OR ENTITY AUTHENTICATION STANDARD

While there are no formal implementation specifications, organizations are expected to implement procedures to verify a person or entity seeking access to PHI is the one claimed. This sounds simple, but the password remains the leading cause of denial-of-service attacks.

Users simply have too many passwords to recall, so they end up using ineffective passwords or reusing the same passwords. Passwords and personal identification numbers (PINs) are quickly being replaced with techniques such as smart cards, tokens, keys, and biometrics (fingerprints, facial patterns or iris patterns), which are assumed to be more secure, but are also more complex to implement. This leaves organizations to determine their risk tolerance as they decide how much they need to put in place to provide the appropriate level of authentication.

> The password remains the leading cause of denial-of-service attacks.

TRANSMISSION SECURITY STANDARD

This standard sets technical specifications that guard against unauthorized access to PHI that is being transmitted over a network, for instance, to a vendor or other covered entity. HHS most often refers to the National Institute of Science and Technology (NIST) for exacting methods and specifications to accomplish these connections. One of the implementation specifications includes integrity controls, which, in this instance, requires that organizations ensure the PHI is not improperly modified without detection; that is, using protocols to ensure that data sent is the same as data received.

This standard also revisits encryption, requiring it where appropriate. Organizations can't assume that connections are secured but can change the protocols used to force encryption from email server to email server via forced TLS. Browsers can be set to inform users when connections are secured and prevent it when it's not secured. When working with vendors or other covered entities, secure connections must be identified and protocols established. These must be well-documented, and organizations must also hold vendors accountable for change control if they're managing that connection.

> When working with vendors or other covered entities, secure connections must be identified and protocols established.

Steps to analyze and manage technical risk

An outside expert such as Med Tech Solutions (MTS) can provide a central resource to help organizations understand their risks and manage the administrative challenges related to compliance.

TECHNICAL RISK ASSESSMENT

The first critical step for any practice is an assessment of risk. Safeguards will still be required, but an assessment supports informed decisions to understand exactly what measures to implement. It's important to note that many technical safeguards can be cost-prohibitive, especially for smaller covered entities. But while cost may be considered when deciding on the implementation of a security measure, it can't be the only factor. If a technical measure is indicated, an appropriate safeguard must be put in place. It is up to the organization or its IT vendor to research appropriate options.

TECHNICAL RISK ASSESSMENT BEGINS WITH RESEARCH
How is our local network deployed?
Have we scanned the network to see how it is managed and what the network rules are set to?
Do we have adequate access controls and are they defined?
Are we proactively looking for vulnerabilities within our environment?
Are we collecting logs or event-management alerts and reporting on these?
Are we sure we have anti-virus and malware protections installed and activated?
Is our EHR installed in our environment?
If so, do we understand the ownership issues related to technical risk?
If our EHR is hosted elsewhere, how are we protecting the workstations or terminals that interact with it?
What responsibilities does our vendor or the host take on?
Can they prove they're doing what they say they are?

TRANSFER RISK TO THE CLOUD

There are many reasons why organizations don't properly protect their network: limited staff, limited security expertise, complex and extensive data architectures, dynamic data environment, managing multiple security apps, and difficulty monitoring staff are some of the most common. Moving data and applications to the cloud is one way to transfer risk to a vendor for most of the core protections of data and applications. Today, almost every covered entity uses cloud services, from single applications to everything of value. While this can be an effective approach—for cost as well as risk reasons—organizations must understand what they're getting into and ensure that contracts include adherence to standards. When using a cloud host, covered entities must also understand where their data resides and how it can be used. Many cloud providers are spread across multiple data centers across the U.S., and sometimes across the globe, for instance, which can make it difficult to track where PHI is located at all times.

Moving data and applications to the cloud is one way to transfer risk to a vendor for most of the core protections of data and applications.

THIRD-PARTY ASSESSMENT OF VENDOR CONTROLS

As noted by the AMCA breach, when a business associate is breached, it can affect everyone. Third-party assessment of vendor controls can help organizations ensure that vendors meet the expectations required of covered entities to protect PHI. The covered entity should have a list of questions for a vendor to answer before a contract is signed and to maintain contractual obligation, and the covered entity must have a signed business associate agreement (BAA) before releasing access to PHI. At the same time, business associates must understand what it means when they sign the BAA, as some may sign to get a contract without completely understanding their requirements. Many perform none of the security or compliance work a covered entity does, even though by signing the BAA they agree that they do indeed have policies in place, that they train their staff, and perform risk assessments regularly. It's the rare business associate that can provide audit evidence that they adhere to HIPAA, HITECH, and privacy rules, just as covered entities are required to. If they are not adhering to a framework or testing by an independent third party, they could be adding an entirely new level of risk to an organization.

It's the rare business associate that can provide audit evidence that they adhere to HIPAA, HITECH, and privacy rules, just as covered entities are required to.

MTS ITCARE SERVICES

- The fastest and safest public, private, and hybrid cloud environments, purpose-built for healthcare organizations, with comprehensive services that include installation, deployment, and maintenance.
- A team of security and compliance experts to assess, implement, and maintain secure and compliant environments.
- Turnkey apps and systems to configure, deploy, maintain, and optimize system and operational workflow.
- 24/7 helpdesk to keep devices, infrastructure, and applications running at their best, with support plans that are tailored to meet existing and future needs.

MTS MANAGED SECURITY SERVICES

- Network configuration scanning
- Security meeting facilitation & management
- Vulnerability assessment
- White hat pen testing
- Phishing simulation
- Web content filtering
- Multi-factor authentication
- Single sign-on network & app access

EXPERT ASSISTANCE FOR TECHNICAL CHALLENGES

Med Tech Solutions' security and compliance experts assess, implement, and help you maintain compliant environments that meet healthcare regulations. We also provide secure IT environments for healthcare providers, payers, and other sponsors of care. MTS has achieved certification from HITRUST by demonstrating repeatable risk-management processes, continually improving security on behalf of clients, and meeting stringent requirements that helps clients set high standards in protecting patient and business data. This helps ensure that MTS-hosted environments are secure and that covered entities are confident in its adherence to the control framework and HITRUST certification. Third-party independent testing is done regularly, which is far more detailed and granular than the SOC 2 report or the SSAE 18 control reviews.

1 https://securityboulevard.com/2020/01/u-s-healthcare-data-breach-cost-4-billion-in-2019-2020-wont-be-any-better/

2 Security Magazine, Data Breach Trends in 2019 – May 8, 2019

To discuss our hosting or security and compliance services,
contact us at info@medtechsolutions.com

Med Tech Solutions

medtechsolutions.com | 877.687.1222

Med Tech Solutions (MTS) creates technology systems that work the way healthcare practices work. Our Practice-Centered Care services use dedicated IT Care Teams to ensure that technology systems support essential clinical workflows. Provider organizations and networks get a secure, reliable IT infrastructure, optimized clinical and business applications, and full end-user support so they can focus on patient care. MTS was founded in 2006 and is headquartered in Valencia, California. The company has been recognized as an Inc. 5000 Fastest-Growing Company and a Channel Futures MSP 501 provider, and has achieved HITRUST Common Security Framework (CSF) certification for its cloud platform. Learn more at medtechsolutions.com.