FinThrive™

Balancing Security and Agility

The key to effective healthcare cyber resilience

The healthcare sector is particularly vulnerable to cyber threats due to the sensitive nature of the data it handles. From patient records to financial information, the implications of a data breach can be devastating, not only compromising patient trust but also leading to significant monetary repercussions.

Following a recent large-scale cyberattack, the American Hospital Association surveyed nearly 1,000 hospitals, many of which suffered from the security breach.

74% Of hospitals reported a **direct impact to patient care**

94% Of hospitals reported a **negative impact to their financials**, with more than half reporting "significant or serious" impact

33% Of those that reported a financial impact from the cyberattack, more than 33% share the impact is **more than half of their revenue**

With cyberattacks on the rise, it is imperative healthcare organizations not only implement cybersecurity best practices but adopt strategies to remain cyber resilient, should an attack occur, to ensure business continuity and a stronger bottom line.

Understanding Cyber Prevention vs. Cyber Resilience Mindsets

Prevention mindset

This approach focuses on proactively identifying and stopping cyber threats before they can cause harm. It includes implementing robust security measures such as firewalls, antivirus software and regular vulnerability assessments. The core objective is to create a fortified perimeter that deters potential attackers altogether.

Benefits

Reduces the likelihood of successful attacks, protects sensitive data and maintains regulatory compliance.

Consequences

Overreliance on preventive measures can lead to complacency, with an insufficient focus on what happens if an attack bypasses defenses.

Resilience mindset

Conversely, a resilience mindset acknowledges that breaches can occur despite best efforts at prevention. It emphasizes the need to quickly respond, recover and adapt to cyber incidents. Key elements include incident response planning, business continuity management, regular backups and employee training. Resilience ensures an organization can maintain operational continuity and minimize financial impact post-attack.

Benefits

Enhances the ability to recover from incidents, maintain operations and protect reputation. It fosters a proactive culture ready to handle interruptions.

Consequences

May incur higher costs initially due to the need for sophisticated monitoring tools and regular training programs.

Shifting from prevention to resilience

Healthcare organizations traditionally emphasize preventive measures. However, a shift towards incorporating resilience is vital for a balanced cybersecurity strategy. Here's how to make this transition:

Develop comprehensive incident response plans

Draft detailed scenarios outlining potential cyber threats and corresponding responses. Include roles and responsibilities, communication protocols and escalation procedures.

Invest in continuous monitoring

Utilize security information and event management (SIEM) systems to detect unusual activities in real-time, enabling a swift response to incidents.

Conduct regular drills

Simulate cyberattacks to test and refine incident response plans. This practice identifies weaknesses and prepares the team for actual events.

Enhance employee awareness

Regular training programs ensure that staff recognize phishing attempts, social engineering attacks and other common threats, fostering a culture of vigilance.

Implement redundancy measures

Ensure critical data and systems are backed up and can be restored promptly. Consider cloud-based solutions for scalable backup and recovery.

Why both mindsets are vital for healthcare organizations

Integrating both prevention and resilience mindsets creates a robust cybersecurity framework. While preventive measures aim to block attacks, resilience ensures an organization can bounce back swiftly when breaches occur. This dual approach mitigates the risk of prolonged downtime, financial losses and reputational damage.

Cybersecurity Best Practices

The increasing frequency of cyberattacks on healthcare providers underscores the urgent need for robust cybersecurity measures. Here are some tactical strategies to consider at your organization to strengthen data security and reduce risk.

Implementing robust password policies and multi-factor authentication (MFA)

A strong defense against cyber threats begins with robust password policies and multi-factor authentication (MFA). Passwords are often the first line of defense, and weak or compromised passwords can provide easy access for cybercriminals. By implementing stringent password requirements and MFA, healthcare organizations can significantly enhance their security posture.

Robust password policies
Providers should enforce password policies that require complex passwords and regular updates. This includes:

- Using a combination of upper- and lower-case letters, numbers and special characters
- Avoiding easily guessable passwords such as “password123” or “admin”
- Mandating password changes every 60-90 days
- Implementing account lockout mechanisms after multiple failed login attempts

Studies show that more than **80%** of healthcare data breaches stem from inadequate password practices.

Multi-factor authentication (MFA)
Studies show that more than 80% of healthcare data breaches stem from inadequate password practices. To diminish the reliance on passwords for security, MFA requires users to present one or two additional verification factors.

According to Microsoft, utilizing MFA can prevent 99.9% of automated attacks. Consider these MFA best practices to make sure this enhanced access control is effective:

- Implement MFA across the entire healthcare organization
- Provide a range of authentication methods (i.e., Security questions, email, phone call, SMS/text message, etc.)
- Conduct regular assessments of MFA within the organization

Through MFA, greater control can be exerted by confining access to specific systems and resources solely to individuals possessing designated hardware authenticators.

Regularly updating and patching all software

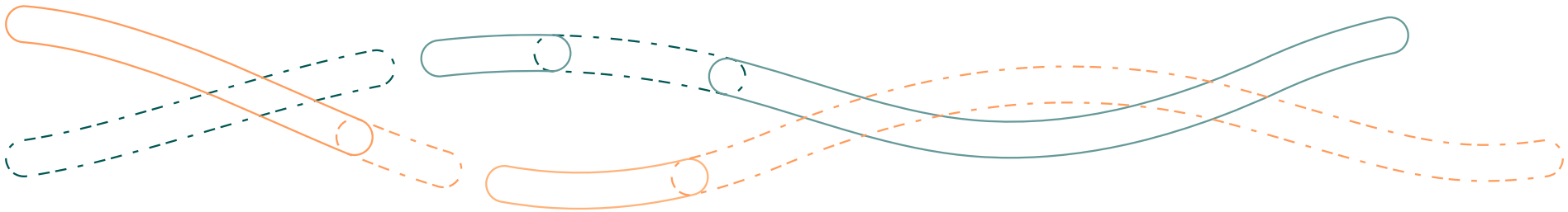
Software vulnerabilities are a common entry point for cyberattacks. Regularly updating and patching software ensures known vulnerabilities are addressed, reducing the risk of exploitation by cybercriminals.

Importance of software updates
Outdated software can contain vulnerabilities that hackers can exploit. Regular updates and patches are crucial in:

- Fixing security flaws that could be exploited by attackers
- Enhancing the functionality and performance of the software
- Ensuring compatibility with other systems and technologies

Implementing a patch management strategy
Healthcare organizations should develop a comprehensive patch management strategy that includes:

- Regularly scanning for software updates and patches
- Prioritizing critical patches that address significant security vulnerabilities
- Testing patches in a controlled environment before deployment
- Monitoring systems for any issues post-deployment



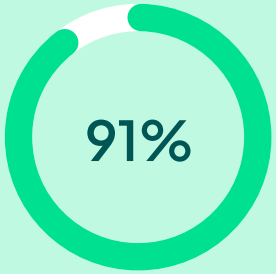
Conducting comprehensive cybersecurity training for staff

Human error is one of the leading causes of cybersecurity incidents. Educating staff about cybersecurity best practices and potential threats can significantly reduce the risk of breaches.

Across the healthcare industry, the frequency of cybersecurity training varies. According to a survey published in 2023, nearly 28% of healthcare organizations engaged in cybersecurity awareness training sporadically, while only 18% of providers said they received training annually.

When conducting staff training programs, it's imperative to cover the following topics:

- Recognizing phishing emails and social engineering attacks
- Safeguarding sensitive patient information
- Proper use of company devices and networks
- Responding to potential cybersecurity incidents



Of cyberattacks originate from phishing attempts.

Continuous education and awareness
Cybersecurity training should not be a one-time event. Continuous education and awareness programs can help keep staff updated on the latest threats and best practices. Regular training sessions, simulated phishing attacks and informational newsletters can reinforce the importance of cybersecurity. Alarmingly, 91% of cyberattacks originate from phishing attempts, underscoring the critical importance of equipping your team to detect phishing indicators and respond securely.

"Having a strong security awareness program can help mitigate ransomware attacks that often originate through phishing and social engineering," said Greg Surla, Senior Vice President and Chief Information Security Officer at FinThrive, during the *HealthLeaders* podcast. "Ensuring that employees and colleagues are aware of these types of attacks is important.

Furthermore, Surla emphasized the importance of buy-in from the top.

"When top-level executives emphasize security awareness, it trickles down to everyone else, reducing the risk of phishing."

Utilizing secure communication platforms

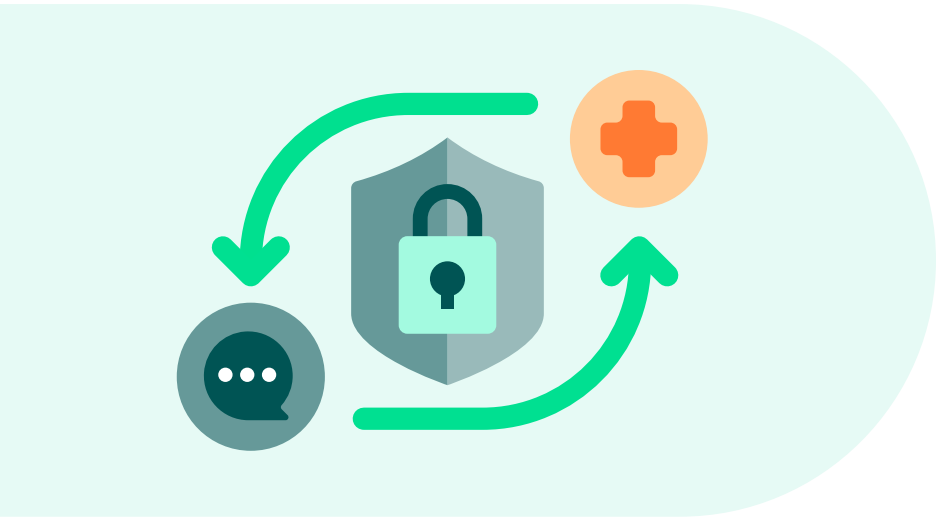
Secure communication is vital in protecting patient information during exchanges. Healthcare organizations must ensure that all communication platforms are encrypted and compliant with industry standards.

Secure communication tools
Investing in secure communication tools can help protect sensitive information. These tools should include:

- End-to-end encryption so only intended recipients can access the information
- Secure messaging and email platforms tailored for healthcare providers
- Compliance with regulations such as HIPAA to ensure patient privacy and data security

Tips for secure communication
To maintain secure communication, healthcare organizations should:

- Limit the use of personal devices for work-related communication
- Regularly review and update communication policies
- Educate staff about the importance of using secure communication channels



Increase Cyber Resiliency by Partnering with the Right Healthcare RCM Vendor

Collaborating with RCM technology vendors can provide healthcare organizations with the expertise and resources needed to enhance their security measures and reduce any impact of a potential attack. With many options available, what should providers look for in the right vendor?

Industry-leading security certifications

When it comes to prioritizing security, vendors often turn to reputable security performance evaluation firms to confirm they uphold current and robust security practices.

Common certifications and standards worth considering include:

HITRUST
Health Information Trust Alliance (HITRUST) certification provides independent assurance that an organization has appropriate security and data protection controls in place based on risk and compliance requirements.

SOC 2 Type 2
A SOC 2 Type 2 certification is based on standards developed by the AICPA to report on controls at a service organization relevant to security, availability, processing integrity, confidentiality and/or privacy over a period of time.

DirectTrust
Governed by the Electronic Health Network Accreditation Commission, a DirectTrust accreditation ensures accredited organizations meet rigorous standards for data security and privacy, comply with regulatory requirements, demonstrate a commitment to high-quality healthcare data exchange practices and when appropriate support interoperability.

Proactive monitoring

It's imperative that a vendor's dedicated security and compliance program offers comprehensive 24/7/365 monitoring supported by an internal Security Operations Center (SOC) team. By addressing potential issues before they escalate, the vendor can maintain the highest standards of security and compliance within the healthcare industry.

Contingency planning

The reality is that no healthcare organization or vendor is 100% safe and cyberattacks continue to be a looming threat for everyone. Should an attack occur, and the vendor is hacked, what processes are in place to ensure continuity?

Vendors should have active Disaster Recovery and Business Continuity plans in place and annual testing conducted and certification by EHNAC. Ideally, a vendor could return to normal operations in 48 hours to minimize impact to any healthcare.

The FinThrive Difference

At FinThrive, we take a 360-degree view of our environment, conducting risk assessments and identifying any areas that may have more exposure than others. With a foundation of a dedicated 40-person security team, security is a top-priority – not a box to be checked.

While maintaining strict compliance with NIST CSF, HITRUST, SOC and other industry best practices, FinThrive offers comprehensive solutions designed to support healthcare providers during unplanned RCM interruptions.

Standby Eligibility

Standby Eligibility provides a resilient backup for eligibility verification processes so healthcare providers can maintain accurate eligibility checks even during unplanned downtime.

- **Preconfigured backup:** Standby Eligibility is implemented alongside existing applications to provide a rapid switchover for uninterrupted eligibility activities.
- **Enhanced patient experience:** Provides clear insights into expected reimbursements, enabling cleaner claims submissions, improved financial counseling and a reduction of unnecessary, duplicative efforts.
- **Up-to-date coverage data:** Improves efficiency and accuracy with automation and the latest coverage information, displayed in a user-friendly format.
- **Quick recovery:** Patient eligibility status and coverage can be accessed within hours to a few days, depending on customer readiness and regular maintenance.

Standby Claims

Standby Claims is a comprehensive solution for billing workflows and clearinghouse services. By implementing Standby Claims, healthcare providers are enabled to get their claims management processes quickly restored during system failures or other interruptions.

- **Preconfigured backup:** Standby Claims is set up alongside existing applications to provide a rapid switchover in case of system failures, such as cyberattacks.
- **Full-version Claims Manager:** Access to a full-version of Claims Manager for claims scrubbing and clearinghouse functions helps confirm accurate and efficient claims submission to payers.
- **EHR/PAS integration:** Seamless integration with Electronic Health Records (EHR) and Patient Administration Systems (PAS) for tracking and reporting.
- **Quick fail-over:** Quick switch to production mode provides a backup alternative for editing and submitting claims. Billing operations can be restored within hours to a few days, depending on customer readiness and regular maintenance.

Partnering with trusted experts like FinThrive can provide additional support and expertise, helping healthcare providers navigate the complexities of data security and maintain cyber resilience. With FinThrive's solutions, you can ensure financial stability and reduce operational risks, even during unplanned RCM interruptions.

Learn more about how FinThrive's solutions can help your healthcare organization improve its cyber preparedness.

FinThrive