FinThrive

# Preparedness Over Panic

## The checklist for choosing a cyber resilient RCM partner


In the past year, cyberattacks have surged, with **92% of organizations affected**.

# Healthcare's vulnerability to cyber threats is alarming, given the sensitive and confidential data managed by providers and vendors alike.

Unfortunately, with these incidents becoming more commonplace, our industry is now more acutely aware that a data breach can have catastrophic consequences, eroding patient trust and resulting in severe financial penalties for all involved.

In the past year, cyberattacks have surged, with 92% of organizations affected, up from 88% in 2023. Health systems and hospitals face heightened risks, making it less a question of 'if' they'll be targeted and more of 'when.' Adopting a prevention mindset is crucial, but fostering resilience is just as vital to ensure business continuity and financial stability, even amidst unexpected interruptions from these attacks.

Following a recent large-scale cyberattack, the American Hospital Association surveyed nearly 1,000 hospitals, many of which were negatively impacted.

**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**

# While cybersecurity education and awareness are crucial, has your company prioritized cyber resilience planning?

If you're just beginning or haven't found the right partner yet, it's crucial to understand that collaborating with the right tech vendor can give you a significant advantage, particularly if they recognize the critical importance it plays for both your patients and your financial performance.

When selecting a vendor partner, **contemplate these key points** to help guarantee you're making the right choice for your cyber resilience needs.

## 1 How does cyber risk management influence the vendor's policy universe?

**What You Should Hear**

We prioritize a security-first approach to our vendor policies. For example, we require the use of multi-factor authentication (MFA) instead of password-only authentication. MFA can prevent nearly 100% of automated attacks.

Additionally, we ensure patches are applied in a timely manner and require colleagues to complete regular security awareness trainings. Non-compliance could result in significant consequences for our colleagues, including terminations.

### MFA Best Practices

- 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

## 2 How does your vendor identify and manage the security risks associated with an RCM platform?

**What You Should Hear**

Regular risk and vulnerability assessments are a crucial part of our cyber resilience approach. To minimize risk, we classify data based on importance, encrypt data at-rest and in-motion and ensure that malware and ransomware protections are in place.

We also provide proactive 24/7/365 monitoring that's supported by an internal Security Operations Center (SOC) team, allowing us to address potential issues before escalation.

## 3 Does the RCM vendor utilize data centers certified against industry standards such as HITRUST, SOC2 and others?

**What You Should Hear**

As a company, we ensure strict compliance with industry-leading security standards and certifications, such as SOC, DirectTrust, NIST CSF and HITRUST.

## 4 Does your vendor have a documented cybersecurity program? Is that document available for review?

**What You Should Hear**

Yes, those documents are available for customers to review anytime. We encourage our customers to review our cybersecurity program documents so that you feel comfortable and knowledgeable about our policies, procedures, standards and guidelines. We want you to be confident in our commitment to not only meet industry standards and best practices, but to exceed them.

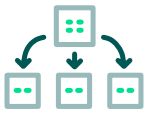
## 5 Have you determined which processes and capabilities are required for an effective cybersecurity program within your RCM? Is the vendor ensuring that its RCM security processes are an effective means to protect data?

**What You Should Hear**

Our security approach is not a one-size-fits-all approach, but rather one that's specific to RCM and the healthcare industry. We don't adopt a general corporate security program because it would put us at risk for overlooking industry-specific threats.

As a vendor, we gather intelligence from multiple sources directly related to healthcare, such as the Healthcare Information Sharing and Analysis Center (H-ISAC). We incorporate this threat intelligence into our threat detection systems.

## 6 How does the vendor organize and implement appropriate roles and responsibilities for its cybersecurity program? Do they have enough staff and resources?



**What You Should Hear**

As part of our commitment to safeguarding patient and provider data, we have an expansive technology team that includes hundreds of individuals. We have a specific group of colleagues that work on our cybersecurity team who partner with other security-focused colleagues in positions across the company, including DevOps, system architects, platform engineers, developers, IT and networking.

This allows us to reduce risk for our customers by ensuring multiple eyes are looking for threats and responding appropriately.

## 7 Does the vendor effectively build and manage a comprehensive Cyber Resilience program that includes contingency planning?

**What You Should Hear**

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 we are hacked, we have an active Disaster Recovery and Business Continuity plan in place. Plus, we conduct annual testing and receive certification by DirectTrust. These processes allow us to return to operations within 48 hours to minimize impact to your healthcare organization.

In addition, we also carry cyber insurance as a company, so if a cyberattack occurs, we're able to respond and recover in a timely manner for the benefit of our customers.

8

# Is the vendor able to meet payroll in the event of a cyber event such as ransomware?

**What You Should Hear**

To respond quickly and reduce impact for our customers, we also prioritize being able to pay our colleagues during our response to a ransomware event. We've seen that it can take weeks to months to recover from a cyberattack, and this can have a negative impact on everyone, including our staff, which can lead to attrition.

Fortunately, our company is strongly backed financially by private equity and investors that allow us to maintain payroll and meet the needs of our own colleagues so we can be best positioned to provide your organization with superior service, even following a cyberattack.

## The FinThrive Difference

By partnering with trusted experts like FinThrive, healthcare organizations can gain additional support and expertise, enabling them to navigate the complexities of data security and maintain cyber resilience.

To learn more on how to ensure financial stability and reduce operational risks, even during unplanned RCM interruptions, visit finthrive.com/cyber-resilience today!

FinThrive