7 Steps to Help Prevent Ransomware Attacks against Healthcare Delivery Organizations

CENSINET®

WHITE PAPER **NOVEMBER 2021**

Ransomware is a threat to business operations and patient safety. Make sure you're ready to defend against it.

Healthcare Delivery Organizations (HDOs) are highly-valued ransomware targets. They have valuable health information and need to continuously ensure that technology and information are available to provide essential patient care. Ransomware attackers are sophisticated and opportunistic, understanding that HDOs are lucrative targets because of organizational resource constraints in the patient care setting and across the operational plane.

With the ongoing transition into digital health, HDOs increasingly rely on third-party providers to help deliver care and capabilities. Safeguarding patient data confidentiality, integrity, and availability is critical for ensuring patient safety and quality-based outcomes. Expanding and incorporating remote work exacerbate vulnerability, so organizations must stem these frequent, complex, and virulent attacks.

Recent ransomware attacks on HDOs significantly reduced or cut off access to patient records, impacting continuity of care delivery and creating potential patient safety issues. This form of cyberattack exposes protected health information, resulting in substantial financial costs to regain control of operations and patient data integrity. In the recent landmark study, The Impact of Ransomware on Healthcare During COVID-19 and Beyond, IT and biomed staff at HDOs are now less confident in their ability to sufficiently protect their organizations and their patients.

There is no silver bullet to stop the existential threat ransomware poses to healthcare records, IT systems, and medical devices. However, there are proven methods and systems for HDOs to mitigate cybersecurity risk and reduce the likelihood of ransomware attacks. The following are seven critical areas of focus to help protect against ransomware.

Ransomware attackers are sophisticated and opportunistic, understanding that HDOs are prime targets because of organizational resource constraints in the patient care setting and across the operational plane.

67%
of all HDOs experienced **one ransomware attack***

33%
experienced **two or more ransomware attacks***

STEP 1. Always maintain visibility

With a distributed workforce and reliance on third-party vendors, HDOs need visibility into their operations along with an understanding of the associated risks. These insights must address your ability to quickly pinpoint who has access to what and identify where your most sensitive data resides. Understanding the landscape of your applications and services becomes critical in truly understanding the risk to the availability of the applications and services and the possible implications on patient safety and care. This visibility also allows you to establish additional controls that are necessary to maintain continuous operations.

STEP 2. Be vigilant in your backup strategy and execution

When responding to a ransomware attack that impacts patient care or hospital operations, you need a backup strategy that enables rapid, effective recovery while offering additional protection afforded by modern continuity and backup solutions. While that may still be the older 3-2-1 strategy or a more modern take such as 3-2-2, you should choose and implement a system that delivers continuity as well as local and extended retention (e.g., cloud backup solutions). An immutable copy of your data must always be available.

STEP 3. Expedite and automate patching

When new vulnerabilities are discovered in clinical applications, business applications, medical devices, and other patient care and delivery systems, you must prioritize the delivery of patches when they become available. These updates must be validated and tested to ensure the affected assets' continued operational functionality and performance. Automate distribution of patches where possible during regular maintenance times. As soon as vulnerabilities are identified, automate updates and distribute patches to third-party applications known to be impacted, such as internet browsers. Develop metrics to monitor patch status and have a process in place for weekly status reviews.

Ransomware attacks have serious impact on patient care and is leading to increased patient deaths. Ransomware is normally discussed in terms of **economic** (ransom and lost revenue) and **operational** (clinical changes) impact, but now we have the third piece: **mortality.**

NEARLY **1 OUT OF 4** of the survey participants reported an **increase in mortality rates***

STEP 4. Regularly review and restrict access to critical assets to include third party vendors

Performing regular reviews (upon access request, when workforce members terminate, or when they change roles in the organization) of access is especially important with critical assets. Restrict access to assets that can impact business or compromise patient care. Management and patching of security vulnerabilities in these assets can often be limited. Medical devices, security cameras, badge readers, environmental sensors, and building management systems are frequently legacy devices and systems that remain in use but can no longer be patched.

When life-sustaining medical devices are involved in patient treatment, it's imperative to segment these systems only to authorized, privileged users and connection points within the organization. This approach includes restricting access to them from general access networks. Most importantly, a clear understanding of the risk of these devices and services is necessary for any HDO to verifiably assess their own risk. All HDOs should be assessing these life-sustaining devices and mission-critical systems frequently and consistently.

STEP 5. Secure the human – vigilance, delivered through security awareness training

This type of education is paramount for all workforce members. Everyone's at risk, including C-suite members, clinical employees, administrative personnel, and more. As a result, all staff and contract help must be provided with core cybersecurity awareness training consistently reinforced with timely threat information. Responsible behavior can prevent cybercrime, especially ransomware, in its many sophisticated forms.

STEP 6. Implement systems to manage vendors and risk

Primitive tools, such as spreadsheets and text documents, are no match for organizations to gauge and manage their risk posture against the threats described above. Using them, ironically, elevates HDO vulnerability to ransomware and other forms of cyberattacks. New platforms, such as Censinet RiskOps, are purpose-built for the unique demands of healthcare and cover third-party and vendor risks and help protect medical devices, supply chain, IRB, and more. Censinet also has the largest collaborative risk network for healthcare, ensuring faster risk protection and delivering more comprehensive risk exposure coverage.

STEP 7. Take part in threat and information sharing

No healthcare provider is an island. When it comes to cybersecurity, it's incumbent upon you to communicate with trusted personnel at other HDOs. And reciprocity matters. Join and contribute to trusted threat intelligence organizations to be proactive about known or existing threats and vulnerabilities that can potentially impact your organization. Take part in providing advance notice to others about attack details and other relevant information. Help your peer HDOs prevent confirmed threats. Information sharing can provide higher levels of confidence in the reported intelligence and increase the resiliency of all HDOs.

NEXT STEPS

None of these efforts are set-it-and-forget-it. And since Risk Never Sleeps, it will take a continuous effort and a vigilant organization to keep cyberattacks at bay. Now you can address ransomware and keep it from negatively impacting your ability to deliver care to your patients while ensuring optimal business operations.

SEE YOUR FUTURE IN ACTION.

Visit censinet.com/prevent-ransomware and we'll show you how.

* Report sponsored by Censinet and independently conducted by Ponemon Institute LLC. See full report at Impact of Ransomware on Healthcare During COVID-19 and Beyond