MARCH 2024

Addressing a Critical Ransomware Recovery Gap

Solutions for ransomware recovery must include a focus on downtime data

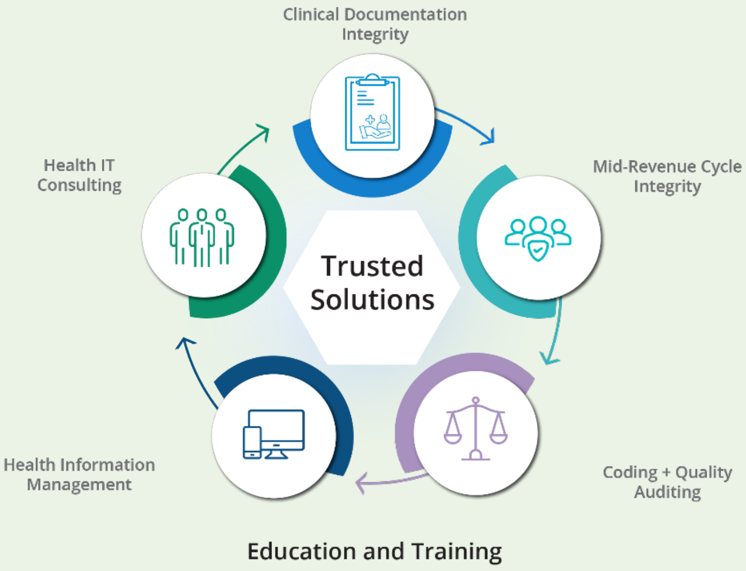
e4health

About e4health:

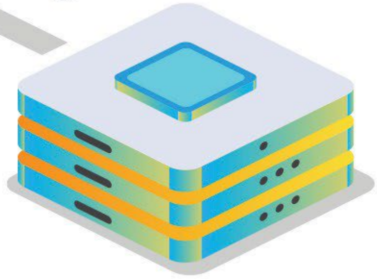
Serving more than 400 health systems and providers nationwide, e4health solves the most difficult challenges in the mid-revenue cycle with innovative and flexible healthcare solutions that deliver results, drive change, protect investments, and support long term value. Our services suite offers flexible end-to- end solutions that address revenue cycle management and data quality issues that health networks, hospitals, outpatient providers, and physician practices rely on to improve quality, overcome challenges, and drive better outcomes.

Utilizing strategic partnerships and proven methodologies, we combine leading-edge technology and best practices to elevate the business of healthcare and impel value and quality throughout healthcare organizations across the nation.

The e4health Services Suite


Clinical Documentation Integrity
Mid-Revenue Cycle Integrity
Coding + Quality Auditing
Health Information Management
Health IT Consulting
Trusted Solutions
Education and Training

Addressing a Critical Ransomware Recovery Gap



Solutions for ransomware recovery must include a focus on downtime data

By Albina Schweidler, MBA, RHIA and Kelly Cassidy-Vanek, MSTECH

Ransomware is a nightmare scenario that every healthcare organization dreads. The proliferation of well-publicized healthcare-targeted cyberattacks confirms that ransomware is a particularly serious threat to the industry. According to cybersecurity consultant, Mandiant, 20% of all ransomware victims are in the healthcare sector (*HIPAA Journal*, 2021). In 2020 alone, ransomware attacks cost healthcare organizations $21 billion (Leventhal, 2021). Recently, The CyberPeace Institute revealed that "295 cyberattacks are known to have been conducted on the healthcare sector between June 2, 2020, and December 3, 2021" (The CyberPeace Institute, 2021). Comprehensive cybersecurity strategies involve prevention, compliance, preparedness, and recovery. Beyond these, many health-sector security strategies overlook a critical gap by failing to address the timely handling and validation of patient data generated during ransomware downtime. Lack of attention to this gap may exacerbate the malware's effect on the quality of care and the bottom line.

What makes ransomware particularly dangerous?

Ransomware is a form of malware that invades computer systems and employs encryption to hold a victim's information for ransom. An organization's critical data is encrypted so that files, databases, or applications are inaccessible.

A ransom is then demanded by global cybercriminals who hold the keys to data decryption. Cybersecurity software provider McAfee notes, "Ransomware is often designed to spread across a network and target databases and file servers and can thus quickly paralyze an entire organization." For healthcare providers, the inability to access patient records, tests, and orders may result in life-and-death scenarios, critical data compliance breaches, and unrealized reimbursement.

Why is the health sector targeted?

As the ransomware threat continues to grow, the scourge has affected health networks, hospitals, nursing facilities, and pharmaceutical companies alike. In many cases, the healthcare organization is unaware that its systems have become infected by malware. It is often discovered only when data is no longer accessible and a demand for ransom payments is received.

The CyberPeace Institute pointed out in their report "Playing with Lives: Cyberattacks on Healthcare are Attacks on People," that the health industry is a low-risk and high-reward target. "Healthcare organizations, especially hospitals and medical service providers, have suffered from a rapid and disjointed digitalization of their infrastructure. The COVID-19 pandemic has only accelerated these processes" (The CyberPeace Institute, 2021). The growth in telehealth, internet-connected medical devices, and patient wellness apps, has created many benefits. However, the increase in the number of devices and endpoints connected to a healthcare network exposes vulnerabilities that cybercriminals regularly attempt to exploit. Further, it is estimated that 83% of medical imaging devices are running on unsupported operating systems (The CyberPeace Institute, 2021).

A focus on attack prevention

As a known target of cybercriminals, protection from attack is clearly the first focus. Healthcare IT and security teams face the daunting task of building and maintaining a hedge of protection to guard against cyber threats. The HIPAA Security Rule requires covered entities to assess data security controls by conducting a risk assessment and implement a risk management program to address any identified vulnerabilities. HIPAA-covered entities must also implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (*HIPAA Journal*, 2022). In-house teams may be assisted by or rely on consulting services, resources, and tools, to analyze systems, pinpoint vulnerabilities, overcome protection shortcomings and undertake dark web monitoring tasks.

A focus on incident preparedness

Even with rigid HIPAA rules compliance, dark web monitoring, and security best practices, no system is immune from attack. The FBI does not recommend paying ransom to cybercriminals. Paying a ransom does not guarantee that the organization will get the decryption key or code needed to regain access to computer systems or files being held hostage. However, preparedness may help to overcome an attack. The National Institute of Standards and Technology (NIST) recommends being prepared by

- Developing and implementing an incident recovery plan with defined roles and strategies for decision making.
- Carefully planning, implementing, and testing a data backup and restoration strategy.
- Isolating backups so ransomware can't readily spread to them.
- Maintaining an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

(NIST Releases Tips and Tactics for Dealing With Ransomware, 2021)

Still many health organizations find that a ransomware attack is untenable to continuing operations and pay the ransom. To mitigate losses, many in the health sector opt for cyber liability insurance coverage to help prepare for and respond to cyberattacks. Depending on the policy, coverage may include ransom fees demanded by hackers, crisis management and investigation costs, hiring negotiators to handle hackers, costs associated with shoring up computer system.

Minding the gap: Downtime date

Clearly, HIPAA compliance standards, ransomware prevention strategies, and preparedness to address security breaches are critical. Facing a recovery effort, however, can drive disruptions far deeper than simply regaining system access. A gap in dealing with a ransomware attack exists and is often overlooked: **Ransomware attacks create system downtime, however, the demand for health services continues.**

Before the unimaginable happens, a plan must be developed to determine how health organization data generated during cyberattack downtime is collected, coded, and validated.

> “Many healthcare organizations have a myopic view of ransomware attacks. Their plan doesn’t encompass proper handling of downtime documentation including paper records, test results, and orders.”
> — Shawn Van Doren
> RN, BSN, CCS

In many cases ransomware downtime results in a return to paper charting for medical records. Manual charting accuracy directly affects documentation integrity related to patient care, physician orders, billing, and payments. Then, when the system is restored, the organization faces the task of synchronizing mounds of paper documentation generated while EHR and other systems were blocked. A monumental backlog of health information updates must be addressed to ensure that the EHR and patient health records are the “source of truth” for doctors, patients, insurers, and facilities.

Filling the downtime disruption gap

Through their experience in assisting healthcare organizations victimized by cyberattacks, Intellis has developed a preparedness checklist and a project management road map to facilitate the timely validation and synchronization of back-logged historical documentation compiled during ransomware breach downtime.

Preparedness Checklist: A planned response to addressing documentation generated during security breach downtime.

As part of a cybersecurity plan, Shawn Van Doren, RN, BSN, CCS said, “Many healthcare organizations have a myopic view of ransomware attacks. Their plan doesn’t encompass proper handling of downtime documentation including paper records, test results, and orders.” He recommends:

1 Ensuring that CTOs and HIT leaders have a comprehensive understanding of their systems’ capabilities and vulnerabilities.

Understanding system architecture and knowing in advance what systems can and cannot do is vital to the timely and efficient handling of a data backlog caused by malware downtime.

2 Establishing the roles and responsibilities of leaders, departments, and stakeholders before a cyber incident occurs. Clear expectations and task descriptions provide a foundation for successful execution of response procedures and recovery accountability.

3 Identifying data points involved in validating and synchronizing historic and current documentation into the EHR. The EHR acts as the source of truth for patient care data, patient care communication, and business functions. The complexity of the data sets must be understood before embarking on creating downtime paper processes that incorporate the entire workflow.

4 Mapping the projected workflow with a deep understanding of current electronic processes. The data management strategy must be designed in a way that is easily deployable. It must provide a downtime paper solution for documentation and maintain continuity for ancillary testing, results reporting, medication ordering, care team communication, and other specified intricacies involved with capturing care delivery, billing, and downstream system activities.

5 Preparing staff with refresher education for manual charting to achieve quality paper records and documentation continuity. Hands-on exercises for paper documentation and manual clinical processes are essential to simulate real-time mission-critical patient care delivery documentation processes.

6 Creating standardization for downtime forms. Regular drills employing standardized forms promotes familiarity with procedures ensuring the continuity of documentation, patient care, and business practices.

7 Executing ransomware response scenario exercises. These exercises are designed to assess the preparedness of the organization if mission-critical applications are impacted. Post-exercise assessments help to determine the gaps and lags in patient care delivery, identify documentation vulnerabilities, and assist in fine-tuning downtime paper processes.

8 Considering whether an in-house response or contracted HIT experts can best meet facility needs. Once a cybersecurity incident occurs and system access is regained, electronic processes commence. However, an organization is faced with mountain of paper documentation and manual activities that need to be incorporated into the EHR. While provisions for backlog processing may be in place, the enormity of the task coupled with time-sensitivity, may necessitate partnering with experienced cyber incident downtime experts. Specialists in restoring data through clinical data abstraction, scanning, and other technology help to ensure documentation integrity while meeting time requirements.

9 Planning for timely records scanning for remote access. The need to scan paper records for immediate access by healthcare

providers across an organization is likely depending on the duration and severity of the security breach. A trusted and experienced HIT partner can alleviate the burden on staff and implement a scanning strategy with accuracy and timeliness.

10 Developing realistic timelines is a key step to a robust cyber incident response plan. Planning and training to respond to documentation disruptions caused by malware, helps to create the foundation for developing realistic timelines for documentation validation, EHR updates, and restored business function execution. Timelines must take into consideration documentation volume, paper charting accuracy and quality, and system capabilities.

Backlog Road Map: Preparation for implementing the documentation backlog plan

Considering the in-depth thought rigor involved with preparing for a ransomware attack, the e4health team developed a simple road map to guide an organization's preparation. The 3-step approach reflects e4health's experience in resolving downtime data challenges for clients.

Case Example: A client turned to the Intellis team for documentation expertise and recovery following a malware incident. The team was tasked with resolving more than 35,000 diagnostic tests, capture them in the EHR system, and meet the CMS billing deadline for reimbursement. Unfortunately, the client did not have a downtime documentation plan in place and manual charting proved substandard.

Van Doren said, "Being prepared is crucial. Having procedures in place and knowing the right questions to ask on day one helps to ensure timely document resolution. When patient safety and revenue cycle concerns are at the forefront, there is no time to waste." The Intellis' IQ team of RNs and EHR specialists quickly addressed all sub-standard charting and confidentially resolved all tests (X-rays, MRIs, CT scans) and met the client's deadline.

Although each organization faces unique challenges, the Intellis recovery road map addresses the three critical areas to prepare for the downtime documentation gap resulting from a cyberattack.

Assembling an A-Team: Before a cyber incident occurs, a downtime data response team should be assembled and armed with clearly defined perspectives of their roles and responsibilities. Representation is needed for each department and system that may be impacted by a breach. Examples include security, IT, human resources, and finance including billing, compliance, and EHR system experts. Each team member's understanding and preparedness contributes to the quick resolution of downtime documentation. The team response keeps patient safety at the forefront, establishing a workflow that enables entered orders and completed exams to match tests results. The team's plan allows for validated documentation to proceed to the billing system without rejection and alleviates concerns due to constraints for timely billing.

Ensuring Paper Charting Proficiency: Paper charting proficiency is not usually a priority for day-to-day health systems operations. However, it is critical for an appropriate response to resolving downtime data as the result of a cyberattack. A commitment to staff training and readiness is necessary to execute paper charting should the EHR system be unavailable. This includes ensuring a staff-wide understanding the basics needed for proper documentation for patient safety, coding, and billing (e.g.: legibility of handwritten information, clearly written signatures, and exact dates and times of exams, tests, and procedures).

Creating Realistic Timelines: Employing untenable arbitrary timelines adds undue stress and unrealistic expectations to an already difficult situation. Real-world consideration must be given to documentation volume, staff charting proficiency, leadership team dynamics, and the effectiveness of advanced preparation. Capricious decision-making, rushing processes, and over-taxing staff are actions that convert to a lack of attention to detail. These actions precipitate system and human errors. Preparation and appropriate timelines help to ensure that all information from paper charting enters the EHR accurately for patient safety and billing purposes.

The End Game

It is frightening to think that nothing can be done to prevent cybercriminals from targeting healthcare and attempting to exploit systems. The return on investment for cybercriminals ensures that ransomware and other forms of malware will continue in the future, and online extortion is bound to evolve. Being prepared for continued operations during downtime due to an attack is as important as preemptively assessing what organization-wide cybersecurity measures are in place. Like overall cybersecurity strategies, planning and preparedness for the resolution of downtime documentation requires a targeted approach. Using the preparedness checklist and following the downtime documentation road map helps to positions healthcare organizations for the timely and accurate resolution of backlogged data.

References

HIPAA Journal. (2021, December 20). New Data Reveals Extent of Ransomware Attacks on the Healthcare Sector. Retrieved from HIPAA Journal: https://www.hipaajournal.com/new-data-reveals-extent-of-ransomware-attacks-on-the-healthcare-sector/

HIPAA Journal. (2022, February 14). CISA, FBI, NSA Warn of Increased Threat of Ransomware Attacks on Critical Infrastructure. Retrieved from HIPAA Journal: https://www.hipaajournal.com/cisa-fbi-nsa-warn-of-increased-threat-of-ransomware-attacks-on-critical-infrastructure/

Leventhal, R. (2021, March 15). Healthcare Innovation. Retrieved from Report: Ransomware Attacks Cost Healthcare Organizations $21B in 2020: https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21214314/report-ransomware-attacks-cost-healthcare-organizations-21b- in-2020

NIST Releases Tips and Tactics for Dealing With Ransomware. (2021, May 13). Retrieved from National Institute of Standards and Technology: https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

The CyberPeace Institute. (2021). Playing with Lives: Cyberattacks on Healthcare are Attacks on People. Geneva: The CyberPeace Institute.

Facing Malware Challenges?
Contact the experienced e4health Team

If you need help with downtime documentaion as the result of malware, **we're here for you.** We can also help healthcare organization develop downtime documentation plans. Please contact e4health for a confidential consultation at info@e4.health.

Healthcare Advisory Solutions

Revenue Cycle and Health Information Services

- Medical Coding
- Medical Coding Audits
- Department Operational Assessments
- Chargemaster Engagements
- Risk Adjustment/HCC Coding and Auditing
- Denials Management

Clinical Documentation and Quality Services

- Second Level Reviews
- Query Reviews
- CDI Department Assessments
- IP and OP Program Implementation
- IP and OP CDI Review Process
- PSI and Mortality Review/Committee Implementation

Health Information Technology Services

- Master Patient Index (MPI) Clean Up
- Enterprise Master Patient Index (EMPI) Clean Up
- Ransomware Downtime Data Resolution
- Clinical Data Abstraction
- Scanning & Indexing
  - EMR Implementation
  - HIMMS Stage 7 Point of Care
- EPIC Implementation and Management
- OnBase Implementation and Management

Education and Training Services

- Medical Coding
- Clinical Documentation Integrity
- Provider Education
- Annual Coding Updates

e4health

96 Commerce Drive, PMB #200 Wyomissing, PA 19610
info@e4.health • sales@e4.health
888.443.4782
e4.health