Published on *The National Law Review* https://natlawreview.com

Ransomware Attacks at Record Levels; Healthcare Organizations Must Be Ready Via Data Security and Disaster Response Policies and Procedures

Article By:

Healthcare providers continue to rely on interconnected information technology systems and digital care delivery to improve healthcare outcomes. In response, ransomware attacks are increasing, both in number and in sophistication. The attacks threaten the clinical and clerical operations of healthcare enterprises of all sizes. JAMA published an alarming study to show that the number of ransomware attacks targeting healthcare organizations doubled in the last five years. These attacks disrupted care and exposed the personal health information of nearly 42 million patients.

Ransomware attacks usually involve the installation of malicious software on vulnerable systems and technology through any number of vulnerabilities, such as email phishing links or disguised as software updates. Once installed, the ransomware software locks healthcare organizations out of their own data, whole data storage systems, or targeted technology devices. The cybercriminals behind ransomware attacks then threaten to release, permanently encrypt, or delete patient data—in some cases, all three—unless the organization pays the ransom demand.

Even relatively minor ransomware attacks can have significant financial, regulatory, and clinical implications for even the most sophisticated healthcare operations. With the healthcare industry squarely in the sights of cybercriminals, healthcare organizations can no longer afford to assess their data security and disaster response policies and procedures *after* experiencing a breach. Ransomware attacks are unlikely to slow, so decisionmakers in healthcare organizations should proactively consider reviewing and updating policies and procedures to minimize impact *before* a ransomware attack occurs.

Implications for Data and Information Security Policies and Procedures

Whether data is in the cloud or on-site, healthcare organizations need robust data and information security policies and procedures to prevent, and respond to, ransomware attacks. These policies and procedures should address the numerous ways in which employees, contractors, vendors, and patients interact with the organization’s technology, as well as set clear boundaries around potential access points that could allow ransomware into information technology systems. Critical elements include items such as:

- Processes for inventorying all software and other technology in use by an organization
- Centralized access controls
- Protocols for controlling and monitoring edits to documents and system files
- Rules that limit software installation and updates to authorized individuals
- User and password management
- Regular audits and breach detection measures

Healthcare organizations should also consider the compliance component of their data security practices. As they do with clinical activities, healthcare regulations establish important boundaries for implementing data security practices and corresponding policies and procedures. For years, HIPAA and similar state laws highlighted the important crossover between technical systems and legal compliance, but recent developments for handling electronic health information could leave many organizations' policies and procedures out of compliance.

For example, the new Information Blocking Rules went fully into effect as of October 6, 2022. They require healthcare organizations make electronic health information readily accessible to patients, which likely requires organizations reconsider existing information security practices, and associated policies and procedures. Importantly, the Information Blocking Rules establish strict requirements for when, and how, healthcare organizations may limit patient access to electronic health information due to data security concerns. Further, the Information Blocking Rules create specific rules for handling system downtime if the downtime unduly interferes with patient access to electronic health information.

This means that healthcare organizations must strike a reasonable balance between data protection and data access. To do this, healthcare organizations should take advantage of enterprise-wide experience to assess data security protocols in light of the Information Blocking Rules. Healthcare organizations should also ensure that information systems personnel, organization leadership, and legal counsel (in-house and outside) work together so that technical protections implemented in updated policies and procedures account for ever-changing legal requirements.

Implications for Disaster Response Policies and Procedures

No matter how secure a system, breaches will eventually occur. Data integrity is a paramount concern, and healthcare organizations should be mindful of the practical effects that a breach may have on operations. Healthcare services can impact life-or-death decisions that cannot wait for systems to be back online after a successful ransomware attack. In fact, a recent Sophos survey of healthcare IT professionals found that 44% of healthcare organizations took more than a year to fully recover data after suffering a ransomware attack. This means that disaster response policies and procedures should address both steps to resolve a ransomware breach and to maintain clinical, billing and administrative functions despite limited access to data or other systems in the meantime.

Practically, healthcare organizations should consider the following when integrating ransomware threat responses into disaster response policies and procedures:

- Identifying impacted technology and systems
- Using robust data backup and recovery systems
- Seeking assistance from law enforcement and other ransomware response professionals
- Interacting with cybercriminals
- Responding to ransom demands
- Managing internal and external communications about the attack and response
- Maintaining clinical operations with existing data, including interim use of paper files
- Recovering access to, and possession of, compromised data

In addition, regulations govern compliance postures for healthcare organizations preparing and implementing disaster response policies—including the response to a ransomware attack or other cyber disaster. For example, compliant disaster response policies and procedures should address HIPAA's breach notification rule requiring individual and possible media notification when a breach of protected health information occurs. Similarly, HIPAA requires healthcare organizations implement processes to notify and work with vendors (*e.g.*, business associates) when a breach occurs, and how healthcare organizations respond if a breach occurs because of the business associate. Disaster response policies and procedures should also consider the compliance posture for processes that allow for interim provision of care without access to certain data or information technology systems. Effective and compliant care is critical.

Again, healthcare organizations should ensure that implementation or updating of disaster response policies involve individuals across the organization, including providers, support personnel, information systems personnel, organization leadership, and legal counsel (in-house and outside). Work across the organization is necessary to ensure effective and compliance policies and procedures.

Jacob Loehr also contributed to this article.

National Law Review, Volume XIII, Number 20

Source URL:https://natlawreview.com/article/ransomware-attacks-record-levels-healthcare-organizations-must-be-ready-data