
# CISA, FBI, and HHS Warn of "Increased and Imminent" Threat of Ransomware Attacks Against Healthcare Industry

October 30, 2020

**AUTHORS**

**Elizabeth P. Gray | Elizabeth Bower | Daniel K. Alvarez | Heather M. Schneider**
**Richard M. Borden | Philip F. DiSanto**

On October 28, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Department of Health and Human Services (HHS) released a joint cybersecurity advisory ("Ransomware Alert") warning of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." Specifically, CISA, FBI, and HHS warned the healthcare industry to "take timely and reasonable precautions to protect their networks" from certain malware that has been used to facilitate "ransomware attacks, data theft, and the disruption of healthcare services."

Hospitals and healthcare providers should take notice of this Ransomware Alert and the protective measures that CISA, FBI, and HHS have recommended. In addition, organizations in the healthcare, pharmaceutical, and biotechnology industries should be aware of the increasing risk of cyberattacks targeting their industries. Willkie's Cybersecurity & Privacy Practice Group is closely monitoring this trend and has developed several resources outlining steps to protect against cyber risks in these industries, including on-demand CLEs concerning the risk of ransomware and recent COVID-related cybersecurity, privacy, and intellectual property risks in the pharmaceutical and biotechnology industries.

## Increased Risk of Cyberattacks Against Hospitals and Healthcare Providers

The Ransomware Alert is the most recent in a series of cybersecurity advisories published by U.S. law enforcement concerning the increasing risk of cyberattacks against organizations in the healthcare industry.

## CISA, FBI, and HHS Warn of "Increased and Imminent" Threat of Ransomware Attacks Against Healthcare Industry

Healthcare organizations have long been seen as high-value, low-risk targets for cybercriminals. But for healthcare organizations, responding to a security incident can be extremely costly: studies have shown that the cost of responding to and remediating a data breach in the healthcare industry is approximately $6.45 million per incident.[1]

Law enforcement authorities have been warning for months that during the COVID-19 pandemic the frequency and sophistication of cyberattacks against organizations conducting research and development related to vaccines and treatments has increased significantly. Those prior bulletins warn that all organizations involved in COVID-related research—including healthcare providers, pharmaceutical and biotechnology companies, contract research organizations, and universities—are facing this increased risk.

**Preparing for the Risk of Ransomware**

As organizations have taken steps to defend themselves against ransomware attacks, cybercriminals have adjusted their strategies and tactics to use ransomware in new ways. While the goals of earlier ransomware attacks were focused on merely locking up the data to extort the ransom, more recent attacks have resulted in massive credential theft and data leaks as part of ever-increasing ransom demands. Hospitals and healthcare providers have been hit particularly hard by more recent attacks, with high ransom demands driven in part by the need for such organizations to quickly regain access to critical systems and patient data and minimize any reputational damage that might be associated with the attack being made public.

Hospitals and other healthcare organizations can take several basic measures to protect against ransomware attacks before they occur, including:

- **Implementing and Updating a Comprehensive Cybersecurity Program.** A written comprehensive cybersecurity program that drives cohesive, deliberate decision-making among all stakeholders is critical to protecting the security, integrity, and availability of the organization's data and information technology systems, as well as the confidentiality of the data stored on those systems. The program should be regularly reviewed and updated, and should reflect best practices concerning patch management, access control, password expiration, audits, independent tests, and network segmentation.

- **Maintaining a Business Continuity Program.** Business continuity is an important issue to consider in the context of defending against ransomware, particularly for hospitals and healthcare providers. In conjunction with their cybersecurity program, organizations should develop business continuity policies designed to minimize disruptions and downtime in a crisis and quickly restore operations. Consider implementing policies concerning the frequency and location of backups and identification of systems that should be air gapped from the network. Specifically, try to create a backup of all critical data that cannot be seen or accessed by the standard network.

[1] *See, e.g.,* Cost of a Data Breach at 10, 16, Ponemon Institute (2019).

Additionally, backup network diagrams and critical network configuration information in the same manner as the air-gapped data backup.

- **Assessing Vendor Management Programs.** Hospitals and healthcare organizations engage myriad vendors. Several of the most high-profile data breaches have involved cyber risks introduced through a vendor with access to the victim organization's systems. Evaluate whether policies and procedures are in place to ensure that vendors also have adequate cybersecurity policies and procedures.

- **Developing Employee Awareness and Training Programs.** Studies have shown that nearly 25% of all data breaches are caused by human error, and another 25% are caused by failures in IT and business processes. Ransomware attacks, in particular, are often facilitated through phishing campaigns that target an organization's employees. Training employees as part of your cybersecurity program, such as via simulated phishing exercises, helps mitigate these threats through ongoing education.

- **Developing and Testing an Incident Response Plan.** A flexible incident response plan helps to ensure that an organization is prepared for a cyber incident, including by identifying all members of the response team and instituting appropriate escalation procedures. Because a ransomware attack may limit an organization's ability to communicate through normal means, part of your incident response plan should be an alternative communication plan to ensure that the response team is able to communicate in a crisis. Store copies of the incident response plan in an air-gapped backup. Make sure that each person listed in the incident response plan has a printed copy and contact information for all the other members of the response team in that person's phone contacts. Consider setting up in advance an incident response group on an encrypted messaging application such as Signal. Finally, tabletop exercises that are tailored to the organization's risk profile and current ransomware threats can help to identify and remediate gaps in the incident response plan before they are exploited.

## Navigating and Responding to a Ransomware Incident

It is important to act quickly to contain, stabilize, and remediate an ongoing ransomware incident. Immediate steps in responding to an incident should include engaging outside counsel and a forensic investigator to coordinate the incident response. In addition, protecting critical systems with sensitive data and backups, securing accounts with elevated privileges, confirming the accessibility of backup systems, and preserving logs that reflect the incident can help to mitigate the potential costs of recovery and any post-incident investigation.

Responding to a ransomware incident can be more complicated than responding to other types of cyberattacks. For example, organizations must decide whether or when to contact law enforcement about the incident and whether to pay the ransom amount demanded by the attackers. Law enforcement organizations discourage ransom payments to malicious cyber actors because, among other reasons, payment does not guarantee that files will be recoverable and may

encourage further ransomware attacks. Ransom payments may also violate U.S. sanctions laws and regulations if such payments are made directly or indirectly to malicious cyber actors on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals List. The facts and risks associated with a ransomware incident should therefore be weighed carefully in connection with these decisions.

Hospitals, healthcare organizations, and other organizations faced with a ransomware attack should also consider any potential regulator or public disclosure obligations and determine whether the incident triggers applicable data breach notification statutes, which vary by jurisdiction. Because ransomware attacks are highly varied, whether a particular incident triggers disclosure or notification obligations may be highly fact-specific. Disclosure and notification obligations should be analyzed with a full understanding of the relevant facts and legal obligations in coordination with outside counsel.

The threat of ransomware and other cyber risks facing healthcare organizations will continue to evolve. We are continuing to monitor these developments closely and are available to assist with the development and implementation of measures tailored to your organization's needs.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

**Elizabeth P. Gray**
202 303 1207
egray@willkie.com

**Elizabeth Bower**
202 303 1252
ebower@willkie.com

**Daniel K. Alvarez**
202 303 1125
dalvarez@willkie.com

**Heather M. Schneider**
212 728 8685
hschneider@willkie.com

**Richard M. Borden**
212 728 3872
rborden@willkie.com

**Philip F. DiSanto**
212 728 8534
pdisanto@willkie.com