CLEARDATA®

Healthcare Guide to Ransomware Prevention & Recovery.

Contents

Executive Summary

Organizations that create, process, transmit, or store Protected Health Information (PHI) are increasingly targeted by ransomware attacks. As healthcare organizations continue to adopt cloud technologies and manage complex regulatory requirements, the need for effective ransomware preparedness and response has never been greater.

This guide provides guidance on the business and technical considerations required to prepare for and respond to ransomware attacks in healthcare environments. It is designed for leaders in risk management, compliance, security, and operations who are responsible for creating, configuring, and operating environments subject to frameworks such as HIPAA, HITRUST, GxP, and GDPR.

While extensive ransomware guidance exists from government agencies, industry organizations, and security practitioners, this guide contributes an additional perspective based on ClearDATA's experience supporting healthcare organizations securing cloud infrastructure and protecting sensitive data.

Our goal is to provide practical, healthcare-focused insights to help organizations strengthen their ransomware preparedness, response, and recovery capabilities. Throughout the guide, readers will also find additional resources to support broader security and resilience strategies.

This white paper contains information to:

- Plan, prevent, and recover from a ransomware attack
- Architect a cloud environment capable of thwarting and recovering from an attack
- Detect the indicators that could lead to a ransomware attack
- Appropriately respond to a successful attack
- Conduct the required analysis to determine whether the attack is reportable
- Recover from the attack

End-to-End Cloud Security, Compliance, and Operations for Healthcare ClearDATA is the trusted partner for healthcare organizations seeking to transform threat intelligence into secure, compliant cloud infrastructures that drive innovation and growth.

Our unique shared responsibility model combines expert services with cutting-edge technology to turn cloud security from a reactive necessity into a strategic advantage. By partnering with ClearDATA, healthcare organizations achieve measurable results in three critical areas:

- **Cloud Security:** Safeguard your infrastructure with continuous risk monitoring, advanced threat detection, and rapid incident response to minimize breaches and protect sensitive patient data in the public cloud.
- **Automated Compliance:** Ensure your cloud resources align with industry compliance standards through always-on monitoring and ClearDATA's CyberHealth Platform, which provides clear visibility into compliance status and trends.
- **Cloud Operations & Optimization:** Offload the complexities of managing AWS, Azure, and GCP environments. With support for over 200 cloud services, we provide proactive monitoring and expert troubleshooting to optimize performance and efficiency.

The Ransomware Crisis – Insights from ClearDATA's Latest Healthcare Threat Report

ClearDATA's Managed Detection and Response[1] team constantly consumes system information and identifies common attack vectors and threats targeting healthcare. This paper shares our observations, including how to thwart attacks and how resiliency should be a primary factor in your defense and preparation.

At the core of what we do is turn policy into code.[2] We analyze complex healthcare and cybersecurity industry regulations, as well as risk and security standards, and translate them into technical controls and reference architectures. These form the foundation of our CyberHealth Platform and services, which allows us to quickly automate compliance and security in the public cloud and provide the latest healthcare and industry specific protection.

We're continually updating our platform and safeguards[3] with aggregated data from the relevant industries. In addition to gleaning insights from our customers, ClearDATA continuously monitors the healthcare industry for security alerts that continue to target healthcare organizations.

Every 22 hours. That was the confirmed frequency of global healthcare ransomware attacks in the first half of 2025. [4] Unfortunately, healthcare bears the brunt of the attacks, while they should focus on delivering exceptional patient care and advancing innovation.

The potential harm to patients, the operational damage strain on the healthcare system, the threat to human life due to lack of information, and the astounding recovery costs can be catastrophic to any organization. In the most severe scenarios, an attack can effectively bring the hospital's entire system down.

This type of disruption causes scheduled surgeries to cancel, ambulances to reroute, or critical patients to be transferred to another facility or provider mid-treatment. Unfortunately, Ransomware attacks against the healthcare industry continue to outpace all other industries.

Organized crime, and now in some cases, nation-state actors, have amassed substantial financial gain by taking healthcare networks hostage. With each success and ransom paid, more ransomware attacks are guaranteed. While this may sound like a technology problem, it's much more than that.

In healthcare, there are downstream effects for every event. Whatever happens with data eventually affects a human being. In the case of ransomware, knowledge is power. Gaining insights into how you can detect intruders and know the methods they use to gain access is necessary if you are to stop them before the harm is substantial. Ransomware attacks have warning signs and attackers leave trails.

However, those who pay the ransom may think they have recovered, only to be attacked again because they've now become a "known payer."[5] Becoming a known payer of ransoms puts a long-term target on the organization and contributes to the cybercriminal economy.

Ransomware is a for-profit industry that evolves with technology and societal trends. Some variants fail, while others dominate on a global scale. Regardless, ransomware criminals adopt new techniques quickly, favoring approaches that make payment more likely and faster.

Top 5 Ransomware Threats to Healthcare

About 20 years ago, data breaches were often the result of lost or stolen devices. Malicious attacks like ransomware were far less common. Today, the majority of breaches now stem from malicious activities, including ransomware, phishing attempts, cloud misconfigurations, and insider threats.

The threat is not static. Government agencies from the U.S., U.K., and Australia frequently issue joint warnings about new malware variants and escalating attack campaigns. For instance, CISA[6] the FBI,[7] and the NSA[8] have issued joint advisories about specific.

The following ransomware threats are referenced from our latest Healthcare Threat Report.

Dragonforce is an evolving RaaS platform that transitioned from its hacktivist origins to a self-described "ransomware cartel" focusing on double extortion in early 2025.

- **20+** estimated HCO victims
- Post-RansomHub affiliate absorption (April 2025) fueled rapid scaling as self-declared "ransomware cartel"
- MSP supply chain exploitation/RMM targeting (SimpleHelp)

Medusa - First identified in June **2021**, has emerged as one of the more aggressive RaaS operations of **2025** in the vacuum left by exits from groups like Ransomhub and BlackCat.

- **15+** HCO victims claimed in first **2** months
- Doubled **2024** pace in targeting victims overall, with FBI/CISA issuing joint advisory March **2025**, double extortion
- Uses aggressive "Living-off- the-Land" (LotL) behaviors

Qilin - Formerly Agenda ransomware, is a well-established threat actor group which has claimed over **1200** victimssince its identification in **2022**.

- **80+** HCO victims claimed
- **+280%** growth
- October peak (**22 HCOs**)
- Frequently exploits
- Public-Facing Applications

Sinobi - An emerging RaaS brand that first appeared in late June **2025** with a smaller, diluted footprint within the overall ransomware targeting space.

- **~30** HCO victims claimed since emergence in July **2025**
- October peak **(13)**
- Use of double extortion

INC Ransom - First active in July **2023**, has been tracked regularly by ClearDATA since its entry into the ransomware ecosystem.

- **45+** HCO victims claimed
- **26%** of all INC claims were
- healthcare, **10** victims publicly
- confirmed breaches
- Relies heavily on Initial
- Access Brokers (IABs)

2025 Trends

The following ransomware threats are referenced from our latest Healthcare Threat Report.

211 HCO Attacks
Confirmed global healthcare ransomware attacks (H1 2025)

2.3M Records
Total patient records compromised

~5.5 Million Records
Records compromised in largest U.S. provider breach (Provider HCO, Mar 2025)

66%
U.S. -based targets as share of global healthcare ransomware claims (2025)

Every 22 Hours
Frequency of confirmed global healthcare ransomware attacks (H1 2025)

According to our MDR Team's latest 2025 Healthcare Threat Report (p. 28)[4], the exit of major players like Ransomhub and Blackcat created a power vacuum in the ransomware world. Newer groups, such as Dragonforce, Devman, and Nova, emerged to fill this gap.

.

These groups are expected to become more prominent in 2026 as they continue to develop their tools, build their infrastructure, and recruit new members. While we also anticipate the arrival of entirely new groups next year, the ones that appeared in 2025 are predicted to significantly expand their influence within the ransomware ecosystem.

As ransomware ecosystem instability accelerates affiliate migration and new groups emerge (especially with AI-enabled capabilities), healthcare leaders should prioritize detection aligned to adversary behavior and attack patterns rather than rely on group attribution.

For a more detailed analysis of the evolving threat landscape and emerging ransomware trends in 2025, please see our comprehensive Healthcare Threat Report.[4]

Why Healthcare is a Prime Target

Cybercriminals target healthcare for specific, calculated reasons. The data itself is immensely valuable, containing protected health information (PHI), financial details, and personally identifiable information (PII). This data can be sold on the dark web or used for identity theft and fraud.

More critically, attackers understand that healthcare organizations cannot afford significant downtime. The immense pressure to restore services and access patient data directly impacts patient outcomes, creating urgency. This urgency provides attackers leverage and increases the chances of a ransom being paid, further making healthcare a uniquely high-stakes target.

Preventative Measures

We are at a point with technology where prevention cannot just be the sole strategy. Organizations need to plan as if an attack will happen, not just try to prevent it. Security professionals know that we cannot stop every attack. We must prepare to avoid as many as possible and minimize the damage when one is successful. There are many things we can do to prevent ransomware. Below are recommendations grouped by People, Process, and Technology.

PEOPLE

Train your workforce for security awareness. Incorporate phishing, safe browsing, irregular system activity, social engineering, remote working, and working in public places. Continually learn from what others experience. Learn from real-world incidents, attend webinars and conferences that further educate the industry, and read relevant articles weekly.

Be aware of regular system activity. Observing changes to the behavior of your laptop or the observance of spikes in storage or memory use can be an incident underway.

Test business resiliency. Conduct disaster recovery tests on a frequent, regular basis. These tests include technology testing and evaluation and the reaction, response, and knowledge of the team responsible for ensuring business continuity.

Know how to report security incidents. And report them quickly and with as much specific information as possible.

PROCESS

Maintain offline, encrypted backups and regularly test them. Conduct backup procedures regularly. Backups must be maintained offline as many ransomware variants attempt to find and delete any accessible ones and because there is no need to pay a ransom for data readily accessible to your organization. There are several approaches to the backup strategy. Some organizations swear by the 3-2-1 rule, which is three copies, with one offsite copy on two types of media. It's important to decide on a backup strategy that aligns with your business goals and the industries within which you operate.

Maintain regularly updated "gold images" of critical systems if they need to be recovered from a ransomware attack. This approach entails maintaining image "templates" that include a prebuilt, hardened operating system (OS). It also includes associated software applications that your organization can quickly deploy to rebuild a system, such as a virtual machine or server.

Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. Hardware newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.

Ensure the availability of application source code or executables should be stored with backups, escrowed, or other air-gapped means. Taking this action will allow you to obtain pristine, up-to-date copies of the code safely. Recovery by rebuilding images is more efficient than reinstalling directly to hardware. Still, some images may not install correctly on different hardware or platforms.

Scan for vulnerabilities on an ongoing basis to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

Ensure devices are properly configured and hardened to ensure security features are enabled and other features tuned for limited use. For example, disable ports and protocols not used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389). Threat actors can potentially gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware. After auditing networks for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of. attempts, apply multi-factor authentication (MFA), and log RDP login attempts. For more information review CISA Alert AA20- 073A, Enterprise VPN Security.[9]

Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Consider disabling SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled. Then remove dependencies through upgrades and reconfiguration. Upgrade to SMBv3.1.1 (or most current version) along with SMB signing. Finally, block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Regularly patch and update software and operating systems to the latest available versions. Prioritize timely patching of internet-facing servers and software processing internet data, such as web browsers, browser plugins, and document readers for known vulnerabilities. Understand and know your patch health for all devices. Deploy those critical patches as soon as possible. WannaCry leveraged the Microsoft EternalBlue vulnerability.[10] Those who patched this did not face the WannaCry threat. Establish baseline system behavior patterns by defining key indicators that measure normal system behavior. These could be user access patterns, network traffic, endpoint locations, email patterns, compliance score patterns, and most importantly, data flow and permission patterns.

Enforce strong password security. CIS password guidance is found in its online policy guide, free to download at: https://www.cisecurity.org/white-papers/cis-password-policy-guide.[11]

- Enforce password history set to 24 or more passwords.
- Maximum password age set to 60 or fewer days, but not zero.
- Minimum password age set to one or more days.
- Minimum password length set to 14 or more characters.
- Enable – password must meet complexity requirements.
- Disable — store password using reversible encryption.
- Account lockout duration set to 15 or more minutes. Account lockout threshold set to 10 or fewer invalid login attempts, but not zero. 'Reset account lockout counter after' set to '15 or more minutes.' NIST also provides excellent guidance found online.[12]

Leverage multifactor authentication (MFA). Wikipedia explains that MFA, "is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism,"[33] for all external connections to your network. In combination with password and MFA, healthcare providers could thwart most ransomware attacks.

Whitelisting applications helps you determine which application has the right to run in your environment. Like being on the authorized guest list at a dinner party, a software application should be on the authorized software list to instantiate in your network. Restricting privileges this way is a substantial countermeasure to a ransomware installer.

Employ the principle of least privilege. If a user does not need access to a tool, don't give them access. If a user changes roles and needs greater access, review and document the request before granting it. Conversely, if that user role no longer needs access, reduce it. And by all means, departed employees should have no access after the moment they leave.

Label assets associated with sensitive data. In a sea of cloud assets (or on-premise assets), identifying which assets can touch sensitive data is essential to placing appropriate safeguards with those assets. You must follow a suitable data labeling procedure to protect data successfully.

Map data flows as they flow through your systems, including expected ingress and egress points, storage locations, API connection, and associated data calls. Not knowing where your data flows could leave you vulnerable to data exfiltration tactics common in today's double-extortion ransomware attacks.

Know and manage the data lifecycle. Effectively doing this requires knowing how and where your sensitive data is created, who accesses it, where it is distributed, and how and who maintains it. (See Figure 1 Sample Data Lifecycle)

Figure 1

TECHNOLOGY

Tune your SIEM (Security Information and Event Monitoring System) to watch for known Indicators of Compromise (IOCs) with automation if possible. Loading IoC information as quickly as possible can alert your security team early, trigger firewall rules, access and permission changes, fire off storage air-gapping rules, and keep you ahead of the attack.

Deploy and use a VPN for remote connectivity to hide your IP address and it allows you to access the web anonymously, making it more challenging to target your computer. When you share or access data online using a VPN, that data is encrypted, and it remains largely out of reach for malware creators. Reputable VPN services also blacklist URLs that may be associated with illicit activity.

Maintain VPN appliances. VPN servers should be hardened, maintained, and regularly patched. As was the case with PulseSecure and VMWare, which recently had major VPN vulnerabilities34, VPNs can become vulnerable to compromise.

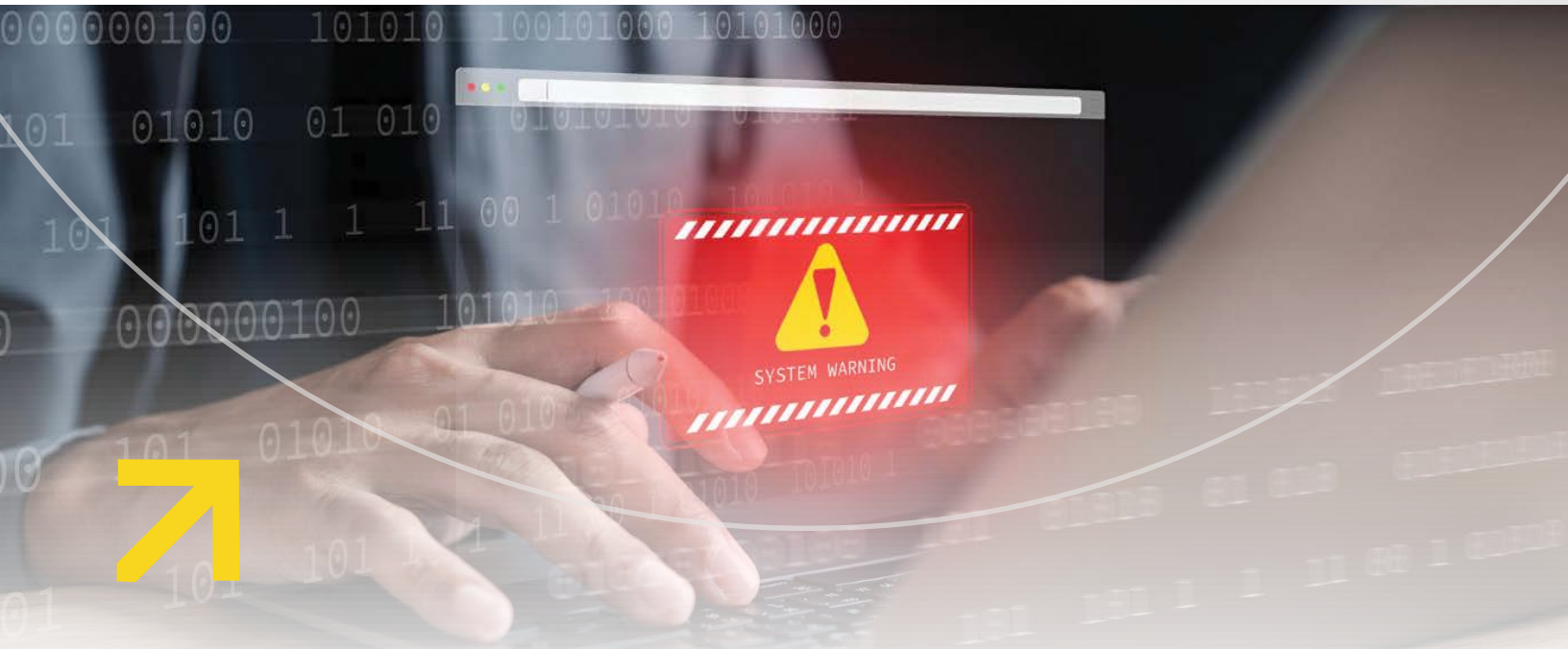
Segment your network to provide greater security and to increase performance. Network segmentation splits a network into zones that contain data with similar security, privacy, and compliance requirements. In today's world, ransomware spreads quickly through a network. Complete isolation of one network from another can save critical backups, or mission critical infrastructure from destruction.

Endpoint protection can be critical in preventing ransomware loaders from infecting a user's laptop or a production server. In fact, not having endpoint protection is like playing Russian Roulette. The odds are that serious injury will occur without it.

Harden email. Phishing is the number one attack vector for ransomware attacks. IT administrators can easily misconfigure email infrastructure. One mistake could make it possible for the unwitting user to double-click that "Urgent Invoice" carrying a secret executable payload ready to decimate your system.

Display file extensions to help you identify ransomware variants when responding to an attack. Because time is of the essence in these kinds of investigations, having instant visibility can help you in the moment. Ensure that devices go offline automatically in case of a threat. In some scenarios, an application or asset can automatically halt activity. If you can enable this safely, do so.

Deploy edge and host-based firewalls. Firewalls are network security applications that monitor and filter traffic to and from your network or your host. Good firewalls automatically deploy rules based on threat patterns leveraging artificial intelligence and machine learning (AI and ML).



Incident Response

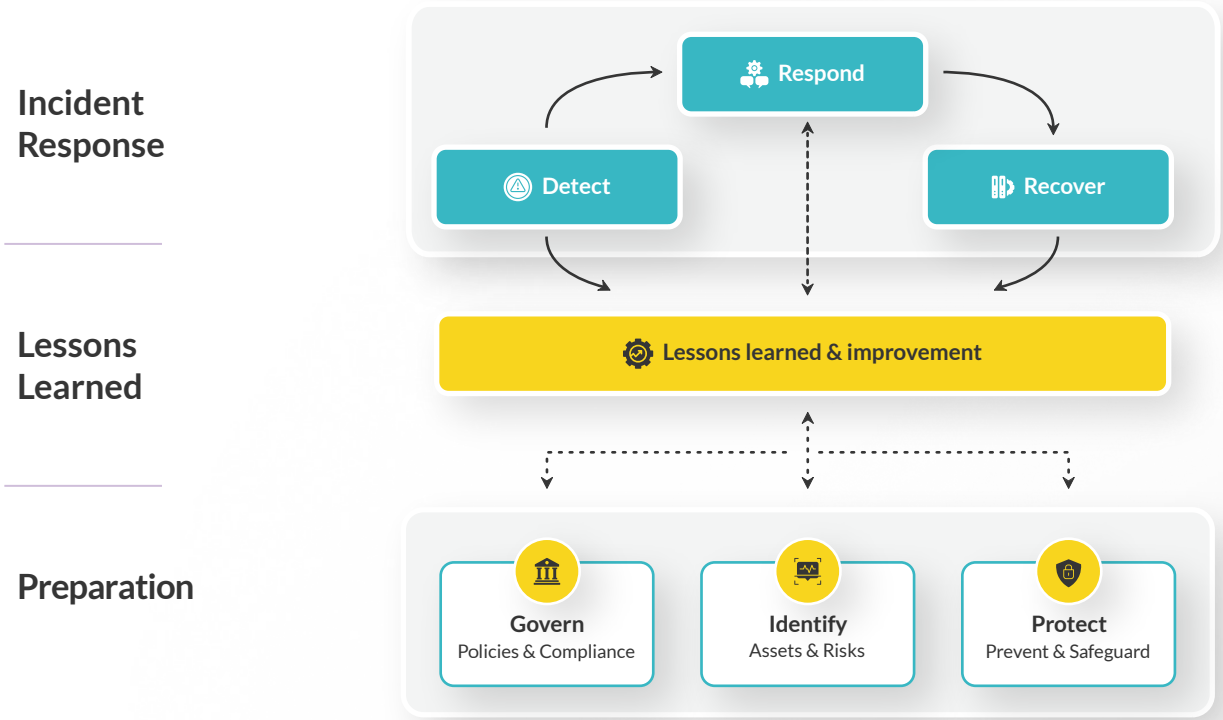


Figure 2

NIST Incident Response [17] Created February 29, 2024, Updated November 20, 2025

Responding to a ransomware attack requires a different response than other cyberattacks. Time is of the essence. The response should be methodical and rapid. The following eight steps can guide you to a successful outcome if you are prepared for an attack (see Figure 2 above). There are many ransomware incident response playbooks available on the web. But, we draw from CISA,[12] NSA, FBI, and industry best practices along with adding a human approach to detection, prevention, and recovery.

Take a deep breath – Quickly

Find a way to stay calm, cool, and collected. You'll need to be calm to think clearly. As soon as humanly possible, isolate the infected system by disconnecting from the network. Report the attack to your helpdesk team. They should be trained to escalate the issue to the incident response team. Take pictures of your screen, ransom messages, encrypted files and their extensions, system error messages, and anything else that doesn't look right. Make sure you are using your smart phone and not taking screenshots – your computer may cease to exist soon! Take notes about the issues.

Try to answer as many of these questions as possible, including:

- What did you notice?
- Why did you think it was a problem?
- What were you doing at the time you detected it?
- When did it first occur and how often since?
- Where were you when it happened, and on what network?
- (Office, home, wired, wireless, with/without VPN, etc.)
- What systems are you using? (Operating system, hostname, etc.)
- What account were you using?
- What data do you typically access?
- What were you doing when this occurred?
- Who else have you contacted about this incident, and what did you tell them?

Be aware that your incident response team may be available to assist with answering these questions. Early in the investigation, contact your CISO. They will likely contact the cyber insurance provider to give them warning. This is important because they only pay settlements from the time they are notified. Insurance providers can also leverage security experts to assist in the investigation, as covered by your cyber policies.

Investigate

Determine the Type of Ransomware:

1. Find any related messages and check the following

- Application screens or graphical user interfaces (GUIs) for the malware itself.
- Text, HTML files, or executable files, sometimes open automatically after encryption (make sure you also look behind existing, open screens).
- Look for new image files; they often appear as wallpaper on infected systems.
- Take photos of contact emails in encrypted file extensions, Observe and document pop-ups after trying to open an encrypted file.
- Check your system for any voice messages that could be irregular.

2. Analyze the messages looking for clues to the ransomware-type:

- Ransomware name
- Language, structure, phrases, artwork
- Contact email addresses
- Format of the user ID
- Ransom demand specifics (e.g., digital currency, gift cards)
- Payment address in case of digital currency
- Support chat or support page.

3. Analyze affected and/or new files. Identify which data the attacker managed to encrypt. Check for:

- File renaming scheme of encrypted files including extensions.
- Files that have been corrupted or encrypted.
- Targeted file types and locations, if possible.
- Who the user of the system should be (the "owning user") and determine the group of affected files.
- Any icons for encrypted files.
- Existence of file markers.
- Existence of file listings, key files, or other data files.

4. Analyze affected software or system types. Some ransomware variants only affect certain tools (e.g., databases) or platforms (e.g., NAS products).

Determine the Scope of the Infection

1. Which systems are affected?

- Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc. Use endpoint protection/EDR, endpoint telemetry, system logs, cloud logs, netflow logs, and other sources of information where possible.
- Check similar systems for infection such as similar users, groups, data, tools, department, configuration, and patch status.
- Find external command and control (C2) traffic. If present, find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, NetFlow or router logs.

2. Find out what data is affected, such as file types, department, or group, affected software, customer environments, management planes, scanning tools, etc.

- Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools.
- Find changes to normally stable or critical data files. Check file integrity monitoring tools.

Assess the Impact

Prioritize and motivate resources.

1. Assess functional impact and the impact to business.

- How much money is lost or at risk?
- How is the business degraded or at risk?

2. Assess information impact: impact to confidentiality, integrity, and availability of data.

- How critical is the data to the business and to your customers?
- How sensitive is the data (e.g., trade secrets)?
- What is the regulatory status of data (e.g., PII, PHI)?

Find the Infection Vector

Check the tactics captured in the Initial Access tactic of MITRE ATT&CK.[14]

Common specifics and data sources include:

- Email attachment: check email logs, email security appliances and services, e-discovery tools, etc.
- Insecure remote desktop protocol (RDP): check vulnerability canning results, firewall configurations, etc.
- Self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, etc.).
- Infection via removable drives (worm or virus).
- Delivery by other malware or attacker tool: expand investigation to include additional attacker tools or malware.
- Scan all IT environments for potential entry points.

Remediate

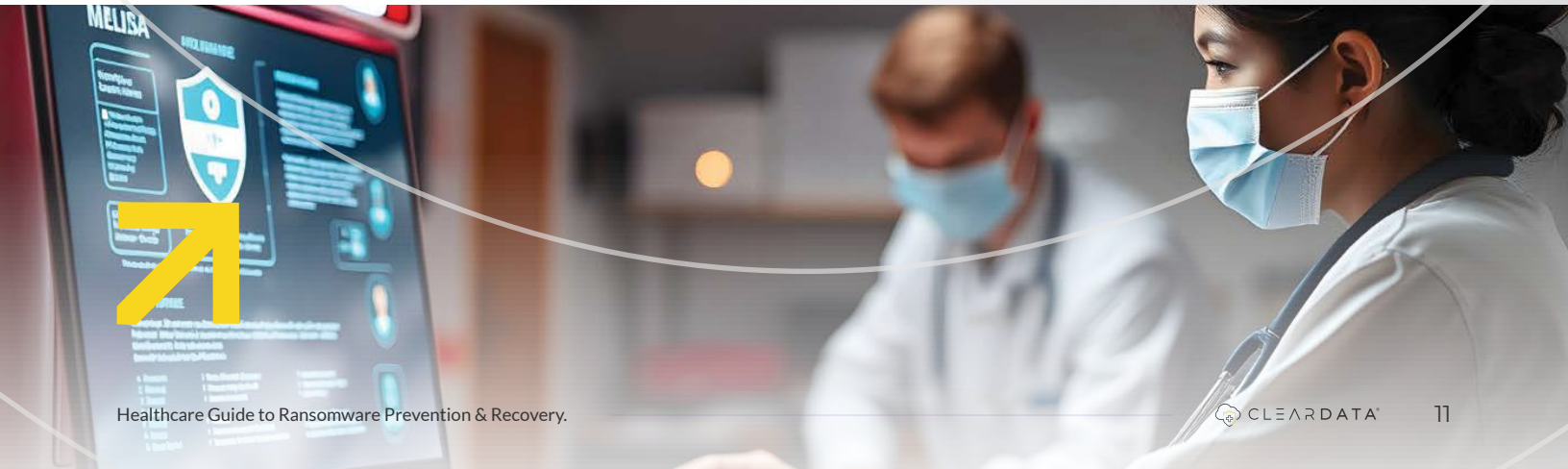
Plan remediation events where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.

Consider the timing and tradeoffs of remediation actions: your response has consequences.

Contain

In ransomware situations, containment is critical. Inform containment measures with facts from the investigation. Prioritize quarantines and other containment measures higher than during a typical response. Quarantines (logical, physical, or both) prevent spread from infected systems and prevent spread to critical systems and data. Quarantines should be comprehensive: include cloud/SaaS access, single-sign-on, system access such as to enterprise resource planning (ERP) or other business tools, etc.

- Quarantine infected systems.
- Quarantine affected users and groups.
- Quarantine file shares (not just known infected shares; protect uninfected shares too).
- Quarantine shared databases (not just known infected servers; protect uninfected databases too).
- Quarantine backups, if not already secured.
- Quarantine backups, if not already secured.
- Remove vector emails from inboxes.
- Confirm endpoint protection (AV, NGAV, EDR, etc.) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, operating systems, software, etc.)
- Deploy custom signatures to endpoint protectionand network ecurity tools based on discovered indicator of compromise (IOC).



Eradicate

- Rebuild infected systems from known-good media.
- Restore from known-clean backups.
- Confirm endpoint protection (AV, NGAV, EDR, etc.) is up-to-date and enabled on all systems. Confirm patches are deployed on all systems (prioritizing targeted systems, operating systems, software, etc.).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs.
- Watch for re-infection – consider increased priority for alarms/alerts related to this incident.

Communicate

1. Escalate the incident and communicate with leadership per company procedure.
2. Document the incident per procedure.
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, etc.
4. Communicate with internal users:

- Communicate incident response updates per procedure.
- Communicate impact of incident and incident response actions (e.g., containment: "Why is the file share down?"), which can be more intrusive/disruptive during ransomware incidents.
- Communicate requirements (refer to best practices within your industry).

5. Communicate with customers with focus particularlyon those whose data was affected.

- Generate required notifications based on applicable regulations (particularly those that may consider ransomware a data breach or otherwise requires notifications, such as with HIPAA, or GDPR).

6. Contact insurance provider(s):

- Discuss what resources they can make available, what tools and vendors they support and will pay for, etc.
- Comply with reporting and claims requirements to protect eligibility.
- Communicate with regulators, including a discussion of what resources they can make available (not just boilerplate notification: many can actively assist).

7. Consider notifying and involving law enforcement:

- Local law enforcement, state or regional law enforcement, and Federal or national law enforcement.[14]

8. Communicate with security and IT vendors:

- Notify and collaborate with managed providers per procedure. Notify and collaborate with incident response consultants per procedure.

Recover

- Launch business continuity/disaster recovery plan(s): e.g., consider migration to alternate operating locations, fail- over sites, backup systems.
- Recover data from known clean backups to known clean, patched, monitored systems (post-eradication), in accordance with our well-tested backup strategy. Check backups for indicators of compromise.
- Consider partial recovery and backup integrity testing.
- Find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page.[16]
- If you consider paying the ransom for irrecoverable critical assets/data, in accordance with policy, then be sure to consider ramifications with appropriate stakeholders.
- Understand finance implications and budget.
- Understand legal, regulatory, and insurance implications.
- Understand mechanisms (e.g., technologies, platforms, intermediate vendors/go-betweens).
- Remove the malware by uninstalling everything on the infected device and reinstalling the operating system.
- Restore data from the most recent backup available.
- Determine how the intruder breached the system and make improvements to ensure the same attack does not happen again. Remember, those who pay the ransom may think they have recovered, only to be attacked again because they've now become a "known payer." Becoming a known payer of ransoms puts a long-term target on the organization and contributes to the cybercriminal economy. For this reason, the FBI discourages the payment of a ransom.[15]

Conclusion

Ransomware is going to continuously evolve and become more sophisticated and prolific. The consequences are costly, and more importantly, in healthcare it is a threat to patient safety. Right now, is the time to prepare your organization for when, not if, an attack occurs. Consider paying the ransom for irrecoverable critical assets/data, in accordance with your organizations' policies and in cooperation with appropriate stakeholders. Understand finance implications and budget. Understand legal, regulatory, and insurance implications. Understand mechanisms (e.g., technologies, platforms, intermediate vendors/go-betweens).

Remove the malware by uninstalling everything on the infected device and reinstalling the operating system. Restore data from the most recent backup available. Determine how the intruder breached the system and make improvements to ensure the same attack does not happen again.

Remember, those who pay the ransom may think they have recovered, only to be attacked again because they've now become a "known payer." Becoming a known payer of ransoms puts a long-term target on the organization and contributes to the cybercriminal economy. For this reason, the FBI discourages the payment of a ransom.

Building resilience today ensures that healthcare organizations can continue delivering critical services—even in the face of evolving cyber threats.

Strengthen Your Organization's Ransomware Readiness

Ransomware defense does not end with incident response planning—it requires continuous improvement. Healthcare organizations should treat ransomware preparedness as an ongoing program that evolves alongside their cloud infrastructure, regulatory requirements, and threat landscape.

Moving forward, organizations should focus on several key priorities:

- Regularly conduct security risk assessments to identify vulnerabilities across cloud and on-premises environments
- Maintain and test backup and disaster recovery capabilities to ensure rapid restoration of critical systems
- Implement layered security controls that address identity, data protection, and cloud infrastructure risks
- Develop and rehearse ransomware response playbooks with leadership and technical teams
- Continuously monitor for emerging threats targeting healthcare systems
- No single framework or tool can eliminate ransomware risk entirely. However, organizations that take a proactive and disciplined approach to security, governance, and operational readiness will be far better positioned to withstand and recover from attacks.

References and Additional Resources

The following resources provide additional guidance on ransomware threats, cybersecurity frameworks, and incident response practices relevant to healthcare and regulated cloud environments.

1 **ClearDATA.** *Managed Detection and Response (MDR).* https://www.cleardata.com/cspm/managed-detection-and-response/

2 **ClearDATA.** *Policy as Code: Springing Compliance Frameworks into Action.* https://cspm.cleardata.com/cleardata-blog/blog/policy-as-code-springing-compliance-frameworks-into-action

3 **ClearDATA.** *Why Technical Safeguards Are Critical for Protected Health Information (PHI).* https://cspm.cleardata.com/cleardata-blog/blog/why-technical-safeguards-are-critical-for-protected-health-information-phi

4 **ClearDATA.** *Healthcare Threat Report / MDR Threat Intelligence Report.*

5 **ClearDATA.** *Healthcare Ransomware Attack: Understanding the Threat Landscape.* https://cspm.cleardata.com/cleardata-blog/blog/healthcare-ransomware-attack

6 **Cybersecurity and Infrastructure Security Agency (CISA).** https://www.cisa.gov

7 **Federal Bureau of Investigation (FBI).** https://www.fbi.gov

8 **National Security Agency (NSA).** https://www.nsa.gov

9 **Cybersecurity and Infrastructure Security Agency (CISA).** *Cybersecurity Advisory AA20-073A: Ransomware Activity Targeting the Healthcare and Public Health Sector.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a

10 **Microsoft Security Response Center.** *WannaCry Leveraged the Microsoft EternalBlue Vulnerability.*

11 **National Institute of Standards and Technology (NIST).** *Digital Identity Guidelines (NIST SP 800-63-4).* https://pages.nist.gov/800-63-4/

12 **Cybersecurity and Infrastructure Security Agency (CISA).** https://www.cisa.gov

13 **National Institute of Standards and Technology (NIST).** *Computer Security Incident Response Resources.* https://csrc.nist.gov/projects/incident-response

14 **MITRE.** *MITRE ATT&CK Framework – Initial Access (TA0001).* https://attack.mitre.org/tactics/TA0001/

15 **Federal Bureau of Investigation (FBI).** *The FBI Discourages the Payment of Ransomware Demands.*

16 **No More Ransom Project.** *Decryption Tools for Ransomware Victims.* https://www.nomoreransom.org/en/decryption-tools.html

17 **NIST Information Technology Laboratory. Incident Response.** https://csrc.nist.gov/projects/incident-response

About ClearDATA

CASE STUDY

See how our partnership helps organizations like yours achieve measurable results.

wondr HEALTH

In partnership with ClearDATA, Wondr Health improved alert triage speed by up to 70%, protecting patient data from evolving threats.

Learn How

r2 HITRUST CERTIFIED

HIPAA COMPLIANT

NIST

AICPA SOC

aws PARTNER L1 MSSP Service Competency

Gold Microsoft Partner

Microsoft

Google Cloud Partner

End-to-End Cloud Security, Compliance, and Operations for Healthcare

ClearDATA is healthcare's leading trusted partner helping organizations turn threat intelligence into a secure and compliant cloud infrastructure for innovation and growth.

Our shared responsibility model unites expert services and technology to safeguard your public cloud, turning security from a reactive measure into a strategic advantage.

Why Leading Healthcare Organizations Choose ClearDATA

- **Cloud Security:** Protect your infrastructure with continuous risk monitoring, threat detection, and incident response to reduce breaches and protect sensitive information in the public cloud.
- **Automated Compliance:** Automatically align cloud resources with compliance standards through always-on monitoring, and maintain clear visibility of your compliance status and trends in our CSPM, CyberHealth Platform.
- **Cloud Operations & Optimization:** We manage the day-to-day operations of AWS, Azure, and GCP environments, supporting over 200 cloud services with proactive monitoring and expert troubleshooting.

CLEARDATA®

Our team of experts and managed services gives you everything you need to protect sensitive data in the cloud

Request a Consult