Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/hollywood-hospital-victimized-by-ransomware-locky-spreading-fast/

HEALTHCARE RANSOMWARE RESPONSE

Ransomware Response That Protects Clinical Operations and Evidence

A ransomware event in a hospital is a patient safety emergency and the start of a HIPAA breach clock that runs from discovery, alongside the work of determining what was taken. Preserve memory, logs and images first, rebuild second and bring privacy counsel in now. Call (800) 868-8189 at any hour.

Published February 22, 2016 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST SP 800-61 Revision 3, Incident Response Recommendations.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

How Modern Double Extortion Ransomware Targets Healthcare and Critical Operations

Since the earliest hospital ransomware disruptions, the threat facing healthcare systems, medical device networks and enterprise operators has escalated from simple file encryption to double and triple extortion. Today, criminal syndicates quietly infiltrate networks through compromised VPN credentials or phishing lures, spend days mapping Active Directory domains and exfiltrating protected health information or proprietary corporate records, and only deploy encryption payloads after they have sabotaged online backups. For healthcare executives and general counsel, a ransomware incident is simultaneously a patient safety emergency and an acute HIPAA and state regulatory compliance crisis.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The HIPAA Clock and the Risk Assessment It Demands

The Breach Notification Rule at 45 CFR 164.404 requires a covered entity to notify affected individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach," as the regulation reads at Cornell's Legal Information Institute. The clock starts at discovery, and the rule treats a breach as discovered on the first day it is known, or by exercising reasonable diligence would have been known, to the entity. Sixty days is the outer limit, not a target, and the Department of Health and Human Services explains in its breach notification guidance that notice to the Secretary and, for larger breaches, to the media follows its own schedule. Every one of those notices depends on a factual determination of what protected health information was involved.

That determination runs through the four factor risk assessment: the nature and extent of the information involved, the unauthorized person who used it or to whom it was disclosed, whether the information was actually acquired or viewed, and the extent to which the risk has been mitigated. Three of those four factors are technical questions, and the examiner answers them from the technical record. Our role is to supply privacy counsel with the facts behind each factor, drawn from logs and artifacts rather than assumption, so the assessment counsel documents is ready for an Office for Civil Rights inquiry. Our healthcare industry page describes the matters we support, and the medical matters records package lists what to gather before that assessment begins.

What the Record Can Establish About Exfiltration

Modern ransomware operators steal before they encrypt, and the question that drives notification is whether they did so here. The examiner looks for the answer in several places. Firewall and proxy logs show outbound sessions by volume and destination, and a transfer of several hundred gigabytes to a cloud storage provider is visible as a spike that normal clinical traffic does not produce. Endpoint artifacts show the staging tools: archive utilities, rclone or similar synchronization clients, and their configuration files naming the destination. NetFlow and DNS logs corroborate the path. On the other side of the ledger, Event ID 1102 in the Security log shows that logs were cleared, shadow copy deletion shows intent to defeat recovery, and gaps in telemetry show where the attacker turned the lights off.

We write what each source shows and how far its coverage reaches. When egress logging covered the relevant segments and shows no anomalous volume during the dwell period, that is a finding counsel can rely on in the risk assessment, and we state the coverage behind it. For segments without egress logging, a quiet result is confirmed against logging coverage before it is read as quiet, and we work the alternative sources: the attacker's own claims and samples on a leak site, the staging artifacts on hosts, and the access records of the systems holding the records at issue. Our ransomware and data breach analysis page describes how that scoping runs. The discipline lets the hospital match its notification to the scope the record supports, narrow where the record shows a narrow scope and broader where the coverage calls for it.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The Engagement From Triage to Timeline

The first phase is triage under counsel. We identify the systems believed encrypted or accessed, the accounts the attacker used, and the segments the traffic crossed, then set a preservation order that captures memory and volatile data first, images next and log exports throughout. Clinical systems present a special case because the electronic health record, imaging and pharmacy platforms often run on vendor managed infrastructure, so vendor logs and vendor cooperation are part of the preservation plan from the start. Every system in the suspected scope is imaged first and rebuilt second, and because that step meets the pressure to restore care head on, the order of operations belongs in the incident plan, settled in advance.

Scoping and timeline follow. We reconstruct initial access, usually a compromised remote access credential or a phishing lure, then lateral movement across the domain, privilege escalation, the reconnaissance of file shares and databases, the staging, the exfiltration and finally the encryption deployment. Each step is dated from artifacts. The timeline tells counsel the dwell period, which fixes the window for the data access question, and the systems touched, which fixes the population of records at issue. Our guide to preserving evidence during incident response describes the first hours. The retainer page explains how a hospital with a standing arrangement starts this work in minutes rather than days, which matters when a sixty day clock is already running.

Keeping Clinical Operations Running While Preserving the Record

Patient care continues while the forensic examination runs alongside it. Downtime procedures, paper charting and diversion decisions proceed under clinical leadership. What we ask is that the systems within the suspected scope be imaged before they are rebuilt, that restoration run from known clean media onto fresh or imaged hardware, and that the medical device and biomedical networks be assessed separately, because infusion pumps, imaging modalities and laboratory analyzers often run operating systems that call for specialized patching and imaging methods and may have been the attacker's quiet foothold. Segmenting those networks during recovery and capturing their traffic protects both patient safety and the record.

The security team's choices during recovery also create evidence. The order of restoration, the credential resets, the accounts disabled and the domain rebuilt or retained are all decisions a regulator may later ask about, and documenting them as they happen is far easier than reconstructing them from memory. We maintain a response log alongside the technical work so that counsel has a dated account of what was done and why. Hospitals that have read our guide on phishing exposure in healthcare will recognize that the initial access vector is usually a human one, and the recovery plan should close that door while the examination runs. Doing both at once is how clinical continuity and a defensible record are achieved together.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Decisions That Hold Up Under Ransomware Pressure

Scoping comes before any payment decision. Whatever the hospital decides about a decryption key, the scoping work is how the examiner determines what was taken, so the notification decision rests on facts. Imaging comes before rebuilding, because the image is the record. Any contact with the attacker runs through counsel with the negotiation preserved in full, because the chat transcripts and the sample files the attacker provides are evidence about what was taken. The managed service provider and the EHR vendor work inside one coordinated response directed by counsel, so each vendor's work serves the hospital's regulatory position alongside its own systems and contract.

The guidance from the Cybersecurity and Infrastructure Security Agency at StopRansomware and the reporting path through the FBI at the Internet Crime Complaint Center both assume that the organization preserves evidence and reports promptly, and both are easier to follow when the preservation order was written into the plan in advance. We recommend that the incident plan name counsel as the director of the response engagement, name the examiner, state that preservation precedes rebuild within the suspected scope, and require that any contact with the attacker be preserved in full. Those four sentences, agreed in a calm month, carry the response through a loud one and support the hospital's position with the Office for Civil Rights, the state attorney general and the insurer.

From Scope Finding to OCR Response, Insurer and Courtroom

The report that ends the engagement serves several readers at once. Privacy counsel uses the scope and timeline to complete the four factor risk assessment and draft the notices. The breach report to the Secretary and any state attorney general filings draw on the same facts. The cyber insurer's panel reads the root cause, dwell time and data access findings to evaluate the claim. Each finding in the report is tied to a named artifact, a hash and a tool version, with inferences labeled and coverage stated, so the account given to the regulator matches the account given to the insurer and both match what the hospital tells its patients.

Healthcare breaches increasingly produce class actions, and the technical record is the center of those cases. Our examiners have testified in federal and state courts and our work has been accepted by courts, and we build every ransomware report so the examiner can defend each sentence under cross examination, including the sentences that describe how far the record reaches. Counsel receives a document that distinguishes observation from inference, a chronology that can be walked step by step, and a witness who can explain Event IDs and egress logs to a judge. Our expert witness services page describes how we support counsel from the declaration through trial. Preparing the record to that standard during the incident is what protects the hospital in the proceedings that follow it.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Rapid Containment and Exfiltration Forensics Under Privilege

Working directly under the direction of retained healthcare privacy counsel, internal audit and hospital IT security leadership, Global Digital Forensics executes rapid ransomware containment and forensic analysis engagements. Our specialists help your engineers isolate clinical and operational networks safely, capture volatile memory and firewall egress logs before systems are rebuilt, and examine whether patient records or sensitive corporate files were exfiltrated, giving your legal team the documented findings that accurate regulatory reporting and cyber insurance recovery rely on. Our guide to preserving volatile evidence in the first hours explains what to freeze before anything is rebuilt. Call our 24/7 emergency hotline at (800) 868-8189 the moment ransomware or unauthorized network activity is detected.

The HIPAA Four Factor Assessment and the Evidence Behind It

The guide ties a ransomware response to the HIPAA breach notification rule and its four factor risk assessment. This table states each factor, the technical source that speaks to it and how the examiner confirms what that source shows, so a privacy officer can see the evidence behind each factor. Read the last column before concluding a low probability of compromise. The sixty day outer limit runs from discovery, and three of the four factors are technical questions the examiner works from the record.

The HIPAA four factor risk assessment, the evidence behind each factor and how each is confirmed.

Factor	Evidence that speaks to it	How the examiner confirms it
Nature and extent of the information	Content assessment of the touched records	Review of the preserved records themselves
The unauthorized person	Sign in logs by address, device and method	Addresses tied to people through provider and device records
Whether actually acquired or viewed	Egress logs and staging artifacts	Quiet results checked against egress logging coverage
Extent of mitigation	Containment and recovery response log	A response log kept as each step happens
Deletion of recovery	Shadow copy deletion and Event ID 1102	Read with the timeline to set the full scope
Whether data left	Firewall and proxy volume to a destination	Volume read with staging artifacts and any capture for content
Notice deadline	Discovery date on the record	No later than 60 calendar days under 45 CFR 164.404

The drug diversion case study describes examiners preserving and imaging seized systems under strict chain of custody for the authorities to evaluate, the same preservation before analysis a hospital needs under a notification clock.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Have the time and manner of discovery, the ransom note and any attacker communications, a list of systems believed encrypted or accessed, your network and clinical system diagrams, the names of your EHR and managed service vendors, and the steps already taken toward containment or restoration. The examiner asks which systems hold protected health information, what logging exists for egress and authentication, whether any system has been rebuilt, who holds backups and whether they are intact, and when privacy counsel was engaged. Counsel then receives a written preservation and scoping plan, a timing estimate aligned to the sixty day outer limit, and a written proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers at any hour.

Technical References and Further Reading

Authorities cited in this guide: 45 CFR 164.404, Notification to individuals. Establishes the discovery standard and the sixty calendar day outer limit for individual notice, current CFR text hosted by Cornell LII. HHS Office for Civil Rights, Breach Notification Rule. Establishes the four factor risk assessment and the Secretary and media notice schedules, HHS guidance page current as of October 2026. CISA StopRansomware. Establishes the federal response guidance that assumes evidence preservation and prompt reporting, CISA resource hub current as of October 2026. FBI Internet Crime Complaint Center. Establishes the federal reporting path for ransomware and extortion incidents, IC3 portal current as of October 2026.

FREQUENTLY ASKED

Ransomware Response for Hospitals

How long does a hospital have to report a ransomware breach under HIPAA?

The Breach Notification Rule requires notice to affected individuals without unreasonable delay and in no case later than sixty calendar days after discovery, with notice to the Secretary of Health and Human Services and, for breaches affecting more than five hundred residents of a state, to prominent media on the schedules the rule sets. Sixty days is the outer limit. The notification decision depends on a four factor risk assessment, and three of those factors are technical questions the forensic record addresses.

Is a ransomware attack automatically a HIPAA breach?

HHS guidance treats encryption of protected health information by ransomware as a presumed breach unless the entity demonstrates a low probability that the information was compromised through the four factor risk assessment. That demonstration has to rest on evidence: what systems held the data, whether the attacker accessed or exfiltrated it, and what the logs show. Our role is to supply privacy counsel with those facts so the assessment is documented and ready for review by the Office for Civil Rights.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Can forensics determine whether patient data was exfiltrated during a ransomware attack?

Often, when the environment logged egress and endpoint activity. Firewall, proxy and NetFlow records show anomalous outbound volume and destinations, endpoint artifacts show staging and transfer tools, and leak site samples corroborate. Where those logs were not kept, the report says which sources cover the period, and we work the alternative sources. A negative finding draws its strength from the log coverage behind it, and we state that coverage in every report so counsel knows what the finding can bear.

What should a hospital preserve in the first hours of a ransomware incident?

Memory and volatile data from affected hosts before they are powered down, forensic images of systems within the suspected scope before any rebuild, firewall, VPN, proxy and DNS logs, domain controller and endpoint logs, cloud tenant audit logs, EHR and vendor platform logs, backup system logs, the ransom note and any attacker communications in full. Document who did each step and when. Those actions protect the record the risk assessment, the insurer and any litigation will depend on.

How much does a healthcare ransomware forensic engagement cost?

Cost follows scope: the number of systems and segments involved, how well the environment was logged, whether vendor managed clinical platforms are in scope, whether exfiltration analysis and leak site monitoring are needed, and whether a declaration or testimony is anticipated. A single site practice with a contained event is a different engagement from a multi hospital system with domain wide encryption. The initial consultation is free, and the written proposal fixes the scope before work begins.

Web Addresses for the Sources Cited

1. NIST SP 800-61 Revision 3, Incident Response Recommendations: https://csrc.nist.gov/pubs/sp/800/61/r3/final
2. Cornell's Legal Information Institute: https://www.law.cornell.edu/cfr/text/45/164.404
3. breach notification guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
4. StopRansomware: https://www.cisa.gov/stopransomware
5. Internet Crime Complaint Center: https://www.ic3.gov/

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.