Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/most-healthcare-organizations-lacking-against-phishing-attacks/

HEALTHCARE CYBERSECURITY

HIPAA Breach Forensics for Health Records and Medical Devices

One phished clinician mailbox can hold thousands of patient identifiers, and the HIPAA notification decision turns on what the audit record shows was actually accessed. Preserve the mailbox and its audit log before remediation and let the analysis drive it. Call (800) 868-8189 at any hour.

Published October 5, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST Cybersecurity Framework 2.0.

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

Why Healthcare Networks Face Unique Clinical Availability and ePHI Pressures

Hospitals, regional health systems, specialty clinics and healthcare payers operate some of the most complex and heavily targeted digital environments in the world. Clinicians require instant, frictionless access to Electronic Health Records across emergency rooms and operating theaters, while thousands of connected infusion pumps, imaging systems and diagnostic IoT devices run on legacy operating systems whose scanning and reboots are planned around patient care. At the same time, any unauthorized access to electronic Protected Health Information triggers strict HIPAA Breach Notification Rule deadlines and Office for Civil Rights regulatory scrutiny.

Clinical Safe Penetration Testing and Granular ePHI Access Forensics

Global Digital Forensics supports healthcare CISOs, privacy officers, internal auditors and outside HIPAA counsel with specialized security testing and forensic analysis engagements. Proactively, our engineers conduct manual penetration testing and passive medical device network segmentation audits that identify paths to EHR databases while clinical care keeps running. Reactively, when a phishing compromise or ransomware event occurs, our forensic examiners analyze EHR audit logs, database queries and network egress telemetry to determine which patient records were viewed or acquired, frequently helping healthcare providers scope notification to the records actually reached.

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

The Four Factor Risk Assessment and the Evidence Behind Each Factor

HIPAA's Breach Notification Rule presumes that an impermissible use or disclosure of protected health information is a breach unless the covered entity demonstrates a low probability that the information has been compromised. Under 45 CFR 164.402, that demonstration rests on a risk assessment of at least four factors, including "the unauthorized person who used the protected health information or to whom the disclosure was made" and "whether the protected health information was actually acquired or viewed", together with the nature and extent of the information involved and the extent to which the risk has been mitigated. Each factor is a factual question, and the mailbox and system records are where the examiner looks for the answer. The forensic examination exists to give the privacy officer and counsel those facts, so that the assessment is a reasoned judgment rather than a guess under deadline pressure.

The deadline is real. 45 CFR 164.404 requires notification to affected individuals without unreasonable delay and in no case later than sixty calendar days after discovery, and the Office for Civil Rights, in its breach notification guidance, treats the sixty days as an outer limit, with notice expected without unreasonable delay inside it. Forensic analysis is planned inside that clock, which means preservation in the first day, a scoping of the exposed mailbox content in the first week and findings for the risk assessment well before the limit. Working under the direction of HIPAA counsel, we structure the engagement so that each factor receives its evidence in time, and the report records what was examined, what it showed and how each open question was addressed, because the assessment and its documentation are what the regulator will later review.

What a Mailbox Audit Record Shows About Patient Data Exposure

When a clinician's account is phished, the question that drives notification is whether the attacker viewed or acquired the messages containing patient information. In Microsoft 365 the MailItemsAccessed operation in the unified audit log records when messages were accessed and whether through a bind to specific items or a sync of the whole folder, with the session identifier, client application and IP address attached. Combined with the sign in logs, it separates the attacker's sessions from the clinician's own. SearchQueryInitiated entries show what the attacker looked for, and inbox rule operations show what was forwarded out. Google Workspace records comparable access and download events. Where the record shows that the attacker's sessions bound only a handful of messages, or synced a folder holding no patient information, the four factor assessment has a factual basis for a low probability conclusion.

The examiner reads the record with its mechanics in view, and the privacy officer receives that reading with its basis. MailItemsAccessed is throttled and aggregated under certain conditions, so the analysis accounts for sessions that touched more messages than the events record. Where audit logging was not enabled or the retention window had closed before discovery, the assessment treats everything in the mailbox as reachable, and we state those conditions plainly. In that setting the content assessment becomes the center of the work: identifying every message and attachment in the exposed mailbox that contains protected health information, the identifiers each contains and the individuals affected, so that notification, if required, is accurate and proportionate.

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

Beyond the mailbox, the same discipline applies to every system the compromised credentials could open. Single sign on means a phished password may have reached the electronic health record, the picture archiving system, the billing platform and the shared drives holding scanned charts, and each keeps its own access log with its own retention. We enumerate those systems from the identity provider's record of where the account authenticated during the attacker's sessions, then pull each log and correlate it to the same windows. A compromise that stayed in the mailbox is a different notification event from one that reached the chart system, and the records are where the examiner tells the two apart. The privacy officer receives that distinction in writing, system by system, so the assessment can address each data set on its own facts.

How a Phishing Compromise Engagement Runs Inside the Sixty Day Clock

The first phase is containment and preservation together, because in a mailbox compromise they happen in the same hour. Sessions are revoked, the password is reset and malicious inbox rules and OAuth consents are removed, while in the same hour the mailbox is placed on litigation hold and the unified audit log, the sign in logs and the rule history are exported. A copy of the mailbox is collected so that the content assessment works from a fixed set. The second phase is access analysis: reconstructing the attacker's sessions, determining what was viewed, searched, forwarded or synced and whether the attacker moved into other accounts or into SharePoint folders holding clinical documents. This phase produces the facts for the second and third factors of the risk assessment, and it also tells the security team whether the incident is contained or still running.

The third phase is the content assessment, which is often the largest. Every message and attachment the attacker could have reached is reviewed for protected health information, using search and processing tools from our eDiscovery practice to find identifiers across formats, followed by human review of the results. The output is a list of affected individuals with the data elements involved for each, which is what the notification letters and the regulator's report require. The final phase is the written report to the privacy officer and counsel, organized by the four factors with the supporting records attached. The privacy incident technical support service page describes these deliverables, and our healthcare industry page covers the clinical environment constraints that shape every phase.

How Healthcare Breach Responses Stay on Track

A well run response steers between two costly extremes. Starting the analysis on day one lets the organization scope notification to what the record supports, which keeps the cost, the regulatory attention and the reputational harm in proportion to the actual exposure, and it keeps the assessment on schedule within the sixty day limit. Preservation is the other anchor: the phishing email, the attacker's sent items and the rule history stay in place until they are exported, because they are where the examiner looks for what was forwarded and when. Writing preservation into the help desk procedure makes it routine on the day it matters.

Configuration choices made before an incident do the most good. Mailbox auditing turned on, with audit retention extended beyond the default for the license tier, gives the privacy officer an access record when it matters most and gives the four factor assessment facts to work from. Electronic health record audit logs kept on a long retention setting are the record the examiner reads to see which patient charts a compromised account opened. Clinical device networks benefit from testing that maps any path from a phished workstation

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

to systems that are hard to patch. A penetration test scoped around clinical safety looks for those paths in advance, and our medical matters records package lists what to gather so that the first call to counsel is productive.

Strengthen Your Healthcare Security and HIPAA Readiness

Our healthcare industry page describes the engagement types in detail, and our medical matters records package lists what to gather before a breach review. Call Global Digital Forensics 24/7 at (800) 868-8189 to speak with a senior healthcare cybersecurity and forensic examiner. The initial consultation is free.

The Phishing Compromise Engagement Inside the Sixty Day Clock

The guide runs a healthcare phishing response in phases that fit inside the HIPAA notification clock. This table lays out those phases, what each produces and the risk factor or deadline it serves, so a privacy officer can see how the four factor assessment gets its evidence in time. The deadline column follows the rule's requirement of notice no later than sixty calendar days after discovery, and each earlier phase is timed to feed the assessment well before it.

Phases of a healthcare phishing engagement, what each produces and the deadline or factor it serves.

Phase	What it produces	Deadline or factor served
Containment and preservation	Sessions revoked, mailbox held, audit logs exported	Completed in the first day
Access analysis	What the attacker viewed, searched, forwarded or synced	The viewed and used factors
System enumeration	Which other systems the credentials reached	Separates a mailbox event from a chart system event
Content assessment	Affected individuals and the data elements for each	The notification population
Report by the four factors	Findings with supporting records attached	The documented risk assessment
Notice to individuals	The letters the assessment supports	No later than 60 days after discovery

The drug diversion case study, a matter involving a pharmaceutical company, shows examiners preserving and recovering records from seized systems for the responsible authorities, the preservation before analysis a healthcare notification decision depends on.

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

How to Begin and What Happens on the First Call

Have ready the affected accounts and their roles, the date and manner of discovery, what remediation has already been done, the email platform and license tier, whether mailbox and EHR auditing are enabled and whether privacy counsel and the privacy officer are engaged. The examiner asks whether sessions have been revoked, whether the audit logs and the mailbox have been preserved, what kinds of patient information the account handled, whether other systems were reachable from it and what the notification timeline requires. Counsel then receive a written scope describing preservation, access analysis, the content assessment and the report organized by the four factors, with timing against the sixty day limit and a proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

Technical References and Further Reading

Earlier reporting on this subject: Healthcare IT News, Phishing threats cause sleepless nights for security pros.

Authorities cited in this guide: 45 CFR 164.402, Definitions (Breach Notification Rule). Defines breach and sets the four factor risk assessment that rebuts the presumption of compromise, current codified text. 45 CFR 164.404, Notification to individuals. Requires notice without unreasonable delay and no later than sixty calendar days after discovery, current codified text. HHS Office for Civil Rights, Breach Notification Rule. Summarizes the notification obligations to individuals, the Secretary and the media and the regulator's expectations on timing, current HHS guidance page. Microsoft Learn, Manage audit log retention policies. Documents how long Microsoft 365 mailbox audit records such as MailItemsAccessed are retained by license level, current Microsoft documentation.

FREQUENTLY ASKED

Patient Notice, Audit Logs and the Sixty Day Clock

Do we have to notify patients if we cannot prove the attacker opened the emails?

Under the rule, an impermissible disclosure is presumed to be a breach unless the covered entity demonstrates a low probability of compromise through the four factor assessment. The audit record is where that demonstration begins: where it records the attacker's sessions and which messages they touched, the assessment rests on those facts, and where no audit record was kept, counsel typically weighs notification for the protected health information in the reachable mailbox. That is why preserving and analyzing the audit log is the first task.

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

How far back does the Microsoft 365 audit log go?

It depends on the license tier assigned to the mailbox and on any audit retention policies the organization configured, and Microsoft documents the periods by license. Organizations on standard tiers often find the window shorter than they expected, so we confirm it for each mailbox, and for a compromise discovered months after it began, the examiner compares the start of the window with the start of the attacker's activity. We export the full available range on the first day, note where the window begins and address any earlier period in the risk assessment. Extending audit retention before an incident is one of the least expensive controls a healthcare privacy program can adopt.

When does the sixty day notification clock start?

Discovery of the breach under the rule occurs on the first day the breach is known to the covered entity or, by exercising reasonable diligence, would have been known, and knowledge of workforce members and agents is attributed to the entity. The clock runs while the forensic analysis proceeds. Notification must go without unreasonable delay and no later than sixty calendar days after discovery, so the examination is planned backward from that limit, with preservation immediately, access analysis in the first days and the content assessment completed in time for the letters.

Can you tell which patient records a compromised account viewed in the electronic health record?

Yes, when the system's audit logs were active and retained. Electronic health record platforms record chart access by user, workstation, time and action, and we correlate those entries with the attacker's session windows from the identity logs to separate legitimate clinical access from the intruder's. That correlation often narrows the affected population considerably compared with assuming every chart the clinician could open was viewed. Where the EHR logs had short retention or were disabled for performance reasons, the report records the setting and the assessment proceeds on the broader basis.

Does a phishing click alone count as a breach?

A click is the starting point for the assessment. A breach under the rule is an impermissible acquisition, access, use or disclosure of protected health information that compromises its security or privacy. A click that harvested credentials but was followed by no sign in, or a sign in that was blocked by conditional access, may involve no access to patient information at all, and the identity and mailbox logs are where the examiner checks. The assessment begins with what the attacker actually did after the click, a factual question the examiner reads those records to answer. Counsel make the determination. We supply the record it rests on.

Web Addresses for the Sources Cited

1. NIST Cybersecurity Framework 2.0: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
2. 45 CFR 164.402: https://www.law.cornell.edu/cfr/text/45/164.402
3. 45 CFR 164.404: https://www.law.cornell.edu/cfr/text/45/164.404
4. breach notification guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
5. Healthcare IT News, Phishing threats cause sleepless nights for security pros: https://www.healthcareitnews.com/news/phishing-threats-cause-sleepless-nights-security-pros
6. Microsoft Learn, Manage audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

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

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.