APSIS SOLUTIONS — HEALTHCARE CYBERSECURITY RESOURCES

Healthcare Cybersecurity Field Guide 2026

Safeguards · Audit Readiness · Epic Security · Incident Response · Operational Risk

Built from documented breaches, real OCR enforcement actions, and operational experience inside Epic-based health systems.

On February 12, 2024, an ALPHV/BlackCat affiliate logged into a Change Healthcare Citrix remote access portal using stolen credentials. There was no multi-factor authentication on that portal. The attacker spent the next nine days moving silently through the network, mapping systems and exfiltrating data, while Change Healthcare — a company that processes approximately 40% of all U.S. healthcare claims — had no alerts, no anomaly detection, and no network segmentation to stop the lateral movement. On February 21, ransomware was deployed. By the time systems were isolated, the attackers had taken an estimated 4 to 6 terabytes of data covering the protected health information of 190 million Americans.

The technical root cause was a single missing control on a single remote access portal. The $2.87 billion in total losses, the 22 million dollar ransom payment that failed to recover the data, the congressional testimony, and the cascading disruption to pharmacies, hospitals, and medical practices across the country — all of it traces back to one Citrix portal without MFA.

This guide exists because that pattern — a catastrophic outcome caused by a known, preventable control gap — is not unique to Change Healthcare. It is the dominant pattern in healthcare cybersecurity. The organizations that experience the worst breaches are not the ones that lost an exotic zero-day battle. They are the ones that had documented gaps in basic controls and did not close them before an attacker found them first.

275M
healthcare records compromised in the U.S. in 2024
Equivalent to 80%+ of the American population. One year.

$10.22M
average cost of a healthcare data breach, 2025
IBM Security. Highest of any industry, 15 years running.

9 days
attacker dwell time before Change Healthcare encryption
Nine days of detectable signals that went undetected.

79.7%
of healthcare breaches caused by hacking, 2024
Up from 49% in 2019. The attack surface is expanding.

CHAPTER 1 THE HEALTHCARE BREACH LANDSCAPE

What actually happened, how it happened, and the patterns that appear in almost every major breach

Why Healthcare Is the Permanent Top Target

Healthcare records are worth more on the criminal market than any other data category. A complete medical record — name, Social Security number, diagnosis history, insurance information, billing data, prescription history — enables identity theft, insurance fraud, prescription fraud, and targeted extortion simultaneously. Financial institution records can be frozen. Healthcare records cannot be changed. The value persists indefinitely.

Beyond the data value, healthcare organizations are operationally coercible in a way that banks and retailers are not. When a hospital's systems go down, patients are at risk. That urgency creates ransom payment pressure that does not exist in other sectors. According to Verizon's 2024 Data Breach Investigations Report, financial gain accounts for 90% of attacker motive in healthcare breaches — and ransomware groups have learned that healthcare organizations pay.

The market dynamics are reinforcing themselves. OCR's enforcement actions and class action lawsuit exposure after a breach create a second financial pressure layer on top of the immediate ransom. Organizations that pay ransoms, pay settlements, and then spend years in litigation are providing a sustained revenue stream that keeps ransomware affiliates focused on healthcare specifically.

The Major Breach Timeline: 2015 to 2025

Understanding the breach history is prerequisite to understanding the current threat environment. The same control failures appear across a decade of major incidents. If your organization has not addressed these specific gaps, you are exposed to the same attack classes that have already been run successfully against organizations very similar to yours.

DATE	ORGANIZATION	ROOT CAUSE	IMPACT	LESSON
Feb 2015	**Anthem Inc. — 78.8M records**	Spear-phishing email installed credential-stealing malware. Attackers moved laterally for months undetected.	$115M settlement. Largest HIPAA settlement at the time. Social Security numbers, employment data, addresses of 78.8M members.	**Phishing is the entry point. Lateral movement detection would have caught this before scale was reached.**
Nov 2023	**HCA Healthcare — 11.3M records**	Third-party storage location used for email formatting compromised. Data exposed to unauthorized access.	11.27 million patients notified. Class action litigation ongoing. OCR investigation opened.	**Third-party and BA security is your security. A vendor's misconfiguration becomes your breach.**
Feb 2024	**Change Healthcare — 190M records**	Citrix remote access portal lacked MFA. Stolen credentials used for initial access. 9-day lateral dwell before encryption.	$2.87B total cost. $22M ransom paid. 40% of U.S. claims disrupted. 190M individuals affected.	**MFA on every remote access point is not optional. Nine days of undetected lateral movement is a detection failure.**
Jan 2025	**Yale New Haven Health — 5.6M records**	Hacking incident. Details of attack vector under OCR investigation as of mid-2025.	5.6M individuals notified. Largest disclosed healthcare breach of 2025.	**Academic medical center scale does not confer protection. Breach can originate at any point in a complex environment.**
2024–2025	**149 ransomware attacks on healthcare globally**	Phishing (16% of access vectors), credential compromise (74% of cloud-env compromises), unpatched systems, missing MFA.	52% of global healthcare ransomware attacks were U.S. targets. $10.22M average breach cost.	**The attack playbook is consistent. The control gaps are consistent. The prevention is also consistent.**

The Five Attack Vectors Responsible for Most Healthcare Breaches

Breach investigations keep returning to the same five entry points. Organizations that have addressed all five have materially reduced their attack surface. Organizations that have addressed three of the five have closed the most common vectors but left the door open to the remaining ones.

VECTOR	HOW IT WORKS IN HEALTHCARE	THE SPECIFIC CONTROL THAT STOPS IT

Credential-based remote access	Attackers obtain valid credentials (through phishing, dark web purchase, or prior breach) and authenticate to remote access systems: Citrix, VPN portals, RDP, web-based EHR access. Without MFA, valid credentials are sufficient. Change Healthcare is the definitive example.	**MFA on every remote access point without exception. No single-factor authentication on any external-facing system that touches ePHI. The NPRM proposes to make this a required — not addressable — HIPAA safeguard.**
Phishing and spear-phishing	16% of healthcare breaches begin with phishing. The Anthem breach (78.8 million records) started with a single spear-phishing email that installed credential-harvesting malware. Healthcare workers receive patient communications, insurance correspondence, and administrative emails — all of which can be convincingly spoofed.	**Email filtering at the gateway layer. Simulated phishing campaigns at least quarterly. Security awareness training completion rate tracked and enforced. DMARC/DKIM/SPF configured and verified. Phishing-resistant MFA (FIDO2, smart card) for privileged accounts.**
Third-party and business associate compromise	HCA Healthcare's 11.3 million record breach originated at a third-party storage vendor. Change Healthcare was itself the BA breach that affected the entire U.S. healthcare payment system. When a vendor has access to your ePHI or your network, their security posture is part of your attack surface.	**Annual BA security verification (proposed by the NPRM as a written certification requirement). BA contract terms that include incident notification within 24 hours. Vendor access conducted in isolated sessions with monitored, time-limited access. Vendor network access segmented from clinical production systems.**
Unpatched and legacy systems	Change Healthcare was reportedly still running 40-year-old payment processing software at the time of the breach. Legacy systems frequently cannot accept current security patches. Internet-connected medical devices often run outdated operating systems that are no longer supported. Each unpatched system is a potential pivot point after initial access.	**Complete asset inventory including medical devices, legacy applications, and end-of-life systems. Documented patch management cadence with critical patch SLAs (72 hours for Critical/High CVEs per the NPRM proposal). Network segmentation isolating unpatched legacy systems from clinical production networks. Compensating controls documented where patching is not possible.**
Insufficient network segmentation and detection	Nine days. That is how long ALPHV/BlackCat moved through Change Healthcare's network before deploying ransomware. Modern ransomware groups do not encrypt on entry. They spend weeks mapping the environment, identifying high-value data stores, exfiltrating data, and positioning for maximum impact. Without network segmentation and behavioral monitoring, that dwell time goes undetected.	**Zero-trust architecture: authenticate and authorize every access request regardless of network location. EDR deployed on all endpoints with behavioral detection enabled. SIEM with healthcare-specific alert rules, particularly for anomalous data access volumes, unusual authentication patterns, and administrative tool use outside normal hours. Network segmentation isolating clinical, administrative, and vendor access zones.**

CHAPTER 2 EPIC-SPECIFIC SECURITY CONFIGURATION

The controls inside Epic that most organizations configure poorly — and what that looks like in an OCR audit

Why Epic Security Is a Distinct Discipline

Epic is the most widely deployed clinical EHR in the United States. Its security architecture is genuinely robust when configured correctly. Role-based access controls, comprehensive audit logging, break-glass

emergency access with mandatory justification, TLS 1.2+ enforcement, MFA integration, and granular record-level access restrictions are all available within the platform.

The problem is not Epic's security capabilities. The problem is implementation: organizations deploy Epic's security features in ways that satisfy the initial go-live checklist but drift out of alignment with actual clinical practice over months and years. New roles get created without review. Access exceptions accumulate. Audit log review processes exist on paper but not in practice. Third-party integrations are built without adequate authentication. And the RBAC model that was carefully designed during implementation ends up looking very different two years post go-live when nobody has been systematically reviewing role assignments.

OCR auditors know this. Epic's audit trail is one of the most complete access logging systems in healthcare IT — which means when OCR investigates a breach that involves unauthorized Epic access, the audit log tells the story in detail. Organizations that have not been reviewing those logs are frequently discovering, during the OCR investigation, that unauthorized access was happening for months before the breach was detected.

The Epic Security Configuration Audit Framework

This framework covers the Epic security domains that generate the most OCR findings and the most insider-access breach exposure. Each row maps to a HIPAA technical safeguard requirement, names Epic's native control, describes the most common misconfiguration pattern, and provides a self-assessment field.

CFR / DOMAIN	CONTROL	EPIC NATIVE CAPABILITY	COMMON GAP PATTERN	ASSESSMENT
164.312(a)(1) Access Control	**Role-Based Access Control — minimum necessary access by job function**	Epic RBAC: granular role templates by job function, context-aware restrictions by department/location/relationship, sensitive record protections (behavioral health, VIP charts)	*Role template drift: roles created during go-live have been modified ad hoc over time. Access exceptions granted under go-live pressure were never removed. Multiple users share roles that grant access beyond their clinical need.*	□ In place □ Partial □ Gap *164.312(a)(1) — Required. Most cited technical safeguard in Epic-related enforcement.*
164.312(a)(2)(i) Unique User ID	**Shared workstation and shared account elimination**	Epic requires individual user authentication. Shared accounts are not a supported Epic configuration, but are sometimes created as workarounds.	*Shared Epic accounts discovered during forensic investigations. Temporary accounts created for go-live support never deprovisioned. Service accounts with human-facing access not rotated or monitored.*	□ In place □ Partial □ Gap *164.312(a)(2)(i) — Required. Shared accounts destroy audit trail integrity.*
164.312(a)(2)(ii) Emergency Access	**Break-glass access with mandatory justification and immediate alert**	Epic's break-glass (emergency access) functionality requires justification entry and generates automatic alerts to supervisors and compliance teams.	*Break-glass alert routing not configured. Justifications not reviewed. Emergency access used routinely by staff who lack standard access rather than in genuine emergencies. No process for*	□ In place □ Partial □ Gap *164.312(a)(2)(ii) — Required. OCR reviews break-glass logs in investigations.*

			reviewing break-glass usage patterns.	
164.312(a)(2)(iii) Auto-Logoff	**Automatic session timeout on inactive workstations**	Epic enforces configurable session timeout. Workstation screen lock independent of Epic session.	*Epic timeout set but workstation OS screen lock not configured, allowing persistent Epic session on locked screen. Timeout thresholds set too long in clinical areas under go-live convenience pressure and never tightened.*	□ In place □ Partial □ Gap *164.312(a)(2)(iii) — Addressable. Standard in all OCR audits of clinical workstations.*
164.312(b) Audit Controls	**Audit log generation, centralization, and review**	Epic generates comprehensive access logs: user, patient, timestamp, action, reason for access. Logs retained for 6 years per HIPAA requirement. Reportable through Epic's compliance reporting tools.	*Logs generated but not reviewed. No alert rules configured for anomalous access patterns. Logs not centralized into SIEM. No process for responding to flagged access events. The Montefiore case: workforce member accessed records for years while log review failed to detect the pattern.*	□ In place □ Partial □ Gap *164.312(b) — Required. Log generation without review does not satisfy the standard.*
164.312(d) Authentication	**Identity verification including MFA for remote and privileged access**	Epic supports SAML SSO with MFA, smart card authentication, FIDO2 keys, and push-based MFA with number matching for phishing resistance.	*MFA configured for some access pathways but not others. Remote Epic access via Haiku/Canto (mobile) not subject to same MFA requirements as desktop. Admin and configuration access not subject to step-up MFA. Legacy remote access pathways (Citrix, RDP) not covered by Epic SSO MFA.*	□ In place □ Partial □ Gap *164.312(d) — Required. NPRM proposes to add MFA explicitly. Priority finding in audits.*
164.312(e)(1) Transmission	**Encryption of ePHI in transit including API and interface traffic**	Epic enforces TLS 1.2+ for all client connections. HL7 and FHIR API traffic subject to transport encryption and authentication. Interface engine connections configurable for encrypted transmission.	*Third-party integrations built with legacy HL7 v2 connections using unencrypted MLLP transport. FHIR API connections granted without scope restrictions. CVE-2024-52007 XXE injection vulnerability in FHIR implementations not patched. Interface engine audit logging not enabled.*	□ In place □ Partial □ Gap *164.312(e)(1) — Required. Integration layer is consistently under-secured relative to core Epic.*

164.308(a)(1) Risk Analysis	**Epic-specific threat catalog included in organizational risk analysis**	Epic provides security configuration baselines and hardening guidance. Epic security assessments available through Epic Tools and UserWeb.	*Risk analysis covers general IT infrastructure but does not include Epic-specific threat scenarios: RBAC drift, break-glass misuse, interface layer exposure, SlicerDicer PHI access governance, third-party app marketplace security.*	□ In place □ Partial □ Gap *164.308(a)(1) — Required. #1 cited HIPAA violation. Epic must be in scope.*

The Integration Layer: Your Largest Unmonitored Attack Surface

Core Epic is well-secured by most organizations. The integration layer — the HL7 interfaces, FHIR APIs, third-party application connections, and data exchange pathways that connect Epic to the rest of the clinical and operational environment — is systematically under-secured by almost all of them.

Every interface is a data pathway. Every data pathway is a potential attack vector. A 1990s-era HL7 v2 interface transmitting lab results using unencrypted MLLP transport was built in an era when the interface sat on an isolated hospital network. That same interface in a modern cloud-connected hybrid environment is transmitting PHI unencrypted across a network that is not isolated. The interface never changed. The network did.

- **most HL7 v2 interfaces use IP-based trust relationships rather than credential authentication. If the source IP is trusted, the interface accepts messages. IP spoofing or a compromised system on a trusted subnet can inject malicious HL7 messages into Epic workflows.** HL7 v2 interface authentication:
- **FHIR APIs grant access to data domains through OAuth 2.0 scope assignments. Applications that are granted over-broad scopes — read/write access to entire patient populations rather than the specific records their function requires — create exposure that a breach of the application immediately converts to a healthcare data breach.** FHIR API scope management:
- **Epic's App Orchard and connected third-party applications vary widely in their security maturity. An application with a BAA and Epic integration certification is not the same as an application with a documented security program, current penetration test results, and incident notification procedures.** Third-party app marketplace security:
- **the middleware that routes HL7 and FHIR traffic between Epic and external systems frequently does not have audit logging enabled at the message level. Interface engines can be used to intercept, redirect, or manipulate PHI in transit without generating Epic-layer alerts.** Interface engine audit logging:

⚠ The CVE-2024-52007 XXE injection vulnerability in FHIR implementations allows attackers to read files from the server, potentially including configuration files containing credentials, by submitting malicious XML in FHIR API requests. Organizations that have deployed Epic's FHIR APIs should confirm their FHIR implementation has been patched for this specific vulnerability. If you don't know the patch status of your FHIR API layer, that is a finding.

CHAPTER 3 OCR AUDIT READINESS

What OCR actually looks for, what documentation survives an investigation, and what doesn't

What OCR Has Been Doing and Where It Is Going

2024 and 2025 have not been quiet enforcement years. OCR closed 22 investigations with financial penalties in 2024, and its Security Risk Analysis Initiative — launched in 2024 — produced seven enforcement actions tied specifically to ransomware victims within six months. The pattern is consistent: organizations that experienced a ransomware attack and whose investigation revealed an inadequate or absent risk analysis received not just the breach response cost but an additional OCR settlement on top of it.

OCR's Phase 3 HIPAA compliance audit program, which began in early 2025 with 50 covered entities and business associates, has published its audit protocol. The focus areas are the risk analysis requirement, the risk management plan, and training and incident procedures. For covered entities running Epic, this means OCR auditors are specifically looking at whether the risk analysis covered the Epic environment in sufficient detail, whether identified risks are actively being remediated, and whether workforce security training completion is documented and enforced.

> **What OCR finds most often**
> The single most cited HIPAA Security Rule violation across every year of OCR enforcement is inadequate or absent risk analysis under 45 CFR §164.308(a)(1)(ii)(A). The second most cited is failure to implement sufficient risk management under §164.308(a)(1)(ii)(B). In plain terms: organizations that do not have a documented, current risk analysis — one that covers their actual environment, assigns likelihood and impact ratings to specific threats, and connects findings to a remediation plan — are OCR's primary audit targets.

The Documentation That Survives an OCR Investigation

OCR investigations are document-intensive. The difference between an investigation that results in a corrective action plan and one that results in a multi-million dollar settlement is frequently the quality and currency of the documentation the organization can produce. Organizations that have documentation but cannot produce it quickly, or that have documentation that predates material changes to their environment, are in a materially worse position than organizations whose documentation is current, complete, and well-organized.

DOCUMENT	WHAT OCR IS LOOKING FOR	COMMON WEAKNESS
Risk Analysis	Current (within 12 months or following material change), covers all ePHI locations, names specific threats with likelihood and impact ratings, connects to a remediation plan with owners and dates	*Last conducted 3+ years ago. Does not cover cloud systems, mobile devices, or third-party integrations added since the last assessment. Threats listed generically ('ransomware') without specific scenarios.*
Risk Management Plan	Active remediation tracker showing that identified risks are being addressed, not just documented. Includes open items, owner assignments, target dates, and progress notes.	*Risk analysis exists but there is no evidence of remediation activity. Open items have been sitting at the same status for 18 months. The plan is a document, not a program.*
Security Policies and Procedures	Documented policies covering all required HIPAA Security Rule administrative, physical, and technical safeguards. Policies reviewed and updated within the past year. Evidence that policies are communicated to workforce.	*Policies are from a vendor template and were never tailored to the organization's actual environment. Last reviewed 4 years ago. Workforce has not been trained on policies that were updated in the interim.*
Workforce Training Records	Evidence that all workforce members with ePHI access have completed security awareness training at hire and annually. Training completion tracked by	*Training records exist for some departments and not others. No evidence of follow-up for non-completers. Training content has not been updated to reflect current threat*

	department. Sanctions documented for non-completion.	*landscape (e.g., no specific phishing recognition content).*
Incident Response Documentation	Documented IR plan with defined roles, severity levels, notification timelines, and Epic-specific response procedures. Evidence of tabletop exercises. Records of prior incidents and their resolution.	*IR plan exists but has never been tested. No Epic-specific procedures. Ransomware scenario not covered. The plan describes a general IT incident response that does not account for the clinical operational consequences of EHR downtime.*
Business Associate Agreements and Oversight	Current BAAs with all BAs that handle ePHI. Evidence of BA security review (annual verification per the NPRM proposal). Incident notification clauses in all BAA contracts.	*BAAs on file but many predate current vendor services. No evidence of BA security review beyond the initial BAA execution. BA incident notification clauses missing or require 30+ days notification rather than 24 hours.*
Audit Log Review Records	Documentation of regular audit log reviews for Epic and other systems containing ePHI. Defined review schedule, reviewer, escalation criteria, and records of investigations triggered by anomalous findings.	*Epic generates comprehensive logs but there is no documented review schedule. No SIEM integration. No alert rules. The logs are produced; they are not read.*
Breach Notification Records	Documentation of breach risk-of-compromise analysis for each suspected incident. Notification records for breaches that met the reporting threshold. Evidence of 60-day notification timeline compliance.	*Prior incidents were not formally documented as to whether they met the breach notification threshold. Analysis conducted verbally and not documented. OCR cannot determine whether notifications were timely without documentation.*

CHAPTER 4 HEALTHCARE INCIDENT RESPONSE

The 72 hours that determine whether a breach becomes a settlement or a recovery

Why Healthcare Incident Response Is Different

Most general-purpose incident response frameworks are not designed for the clinical operational environment. They address systems. Healthcare incident response has to address the simultaneous failure of systems and the operational continuity of patient care.

When Epic goes down — whether from ransomware, a targeted attack, or an unexpected infrastructure failure — the clinical consequence is immediate. Nurses cannot see medication orders. Physicians cannot access labs or imaging. Pharmacists cannot verify prescriptions. The clinical downtime procedures that most organizations have are underinvested, untested, and frequently discovered to be inadequate on the day they are actually needed.

The 72-hour window after a ransomware event is the most consequential period in the entire incident lifecycle. The decisions made in those 72 hours — about isolation scope, clinical downtime procedures, law enforcement notification, ransom negotiation, public communication, and regulatory notification — determine the total impact of the event. Organizations that have a tested, clinical-context-aware IR plan make better decisions in that window. Organizations that are improvising make worse ones.

The Healthcare Incident Response Timeline

PHASE	TIME	ACTIONS	EPIC-SPECIFIC ACTIONS	OWNER
DETECT	**Hour 0–1**	SOC alert or user report triggers initial triage.	**Pull Epic audit logs immediately for affected**	SOC / Security Lead

		Determine: is this a false positive, a security incident, or a clinical emergency? Assign severity level. Notify incident commander.	**users and systems. Do not wait for forensics team. Epic's real-time audit trail may show lateral movement that has not yet triggered EDR alerts.**	
CONTAIN	**Hours 1–4**	Isolate affected systems. Scope the isolation: is this one endpoint, one network segment, or does containment require taking Epic offline? Activate clinical downtime procedures if Epic is being isolated. Notify clinical leadership immediately — they need to activate paper/downtime workflows.	**Epic isolation sequence: confirm Hyperspace connectivity status, initiate downtime ASAP documentation procedures, activate downtime dictation workflows, confirm Haiku/Canto offline mode status for mobile clinical staff. Do NOT restart Epic systems before forensics baseline is captured.**	CISO + CMO + CIO
ASSESS	**Hours 4–24**	Engage forensic IR firm. Preserve evidence before remediation. Determine: what systems were accessed, what data was exfiltrated, what is the estimated scope? Begin breach notification threshold analysis under 45 CFR §164.402.	**Epic forensics: export complete audit log for the suspected compromise window (minimum 30 days prior to detection). Review for: unusual access volumes, off-hours access, access from unexpected locations, bulk PHI queries, break-glass access patterns, and admin account activity.**	Forensic IR Firm + Compliance Counsel
NOTIFY	**Hours 24–72**	HHS OCR notification if breach threshold confirmed (within 60 days of discovery for breaches >500 individuals). Law enforcement notification (FBI, CISA). State AG notification per applicable state law. Affected individual notification planning. Executive leadership and board notification.	**Epic breach data quantification: use Epic audit logs and Clarity reporting to identify the specific patient records accessed by unauthorized users. OCR requires identification of each individual affected. Epic's access logs provide the granular data needed for this analysis — if they were being retained.**	Privacy Officer + Legal Counsel
RECOVER	**Days 3–30**	Restore from clean backups (confirmed isolated from compromised network). Re-image or replace compromised endpoints. Implement remediation for the specific vulnerability exploited. Restore Epic connectivity in staged sequence with enhanced monitoring.	**Epic restoration sequence: restore from pre-incident backup, confirm ETL integrity before analytics layer reconnection, reset all credentials and session tokens, review and tighten RBAC configurations before restoring full access, enable enhanced audit log alerting for 90-day post-incident monitoring period.**	IT Operations + Epic Team
REVIEW	**Days 30– 90**	Post-incident review: root cause analysis documented, lessons learned incorporated into IR plan, security program gaps identified and remediated. OCR corrective action plan	**Epic post-incident hardening: RBAC audit, MFA verification across all access pathways, integration layer security review, break-glass**	CISO + Compliance + Board

		implementation if required. Insurance claim documentation.	**procedure audit, audit log review process formalization. This is the control program improvement that prevents recurrence.**	

The Ransom Payment Decision

If your organization experiences a ransomware event and the attacker demands payment, the decision about whether to pay requires legal counsel, your cyber insurance carrier, and an honest assessment of the backup situation — before any payment decision is made. There is no general right answer.

What the Change Healthcare case demonstrates clearly is what paying does not guarantee: it does not guarantee data deletion, it does not guarantee decryption, and it does not resolve the OCR investigation. UnitedHealth paid $22 million. ALPHV exited the operation and kept the money. An affiliate retained the data and joined RansomHub, which then listed the data for a second extortion. The ransom payment did not stop the breach notification requirement, did not stop the class action lawsuits, and did not stop the OCR investigation.

⚠ Ransomware payment may not be legally available to your organization. OFAC enforces sanctions against payments to sanctioned threat actors. Payments to ALPHV/BlackCat affiliates may involve sanctions exposure that requires Treasury Department guidance before any payment decision. Engage legal counsel and your cyber insurance carrier before authorizing any ransom payment.

CHAPTER 5 BUILDING THE OPERATIONAL SECURITY PROGRAM

The controls that prevent breaches, not just the documentation that responds to them

The Control Hierarchy: What Stops Attacks, What Limits Damage, What Proves Compliance

Not all security controls have equal operational value. Some controls prevent attacks at the entry point. Some controls limit lateral movement and damage after initial access. Some controls primarily satisfy the documentation requirements that determine the organization's posture in a regulatory investigation. An effective healthcare security program has all three, implemented in the right sequence.

LAYER	THE CONTROLS IN THIS LAYER	THE CHANGE HEALTHCARE LESSON
① Prevent Entry	MFA on every remote access point · Email filtering and phishing-resistant authentication for privileged accounts · Vulnerability scanning and critical patch SLA enforcement · BA security verification and vendor access isolation · Asset inventory (you cannot protect what you haven't catalogued)	*A single Citrix portal without MFA was the entry point. MFA would have stopped the attack entirely. Entry prevention is the highest-leverage control tier — it makes the rest of this list less necessary.*
② Limit Damage	Network segmentation preventing lateral movement · Zero-trust architecture requiring authentication for every access request · EDR with behavioral detection on all endpoints · Backup isolation from production network · Immutable backups tested quarterly · Privileged access management for admin accounts	*Nine days of undetected lateral movement caused the scale. Network segmentation would have contained the blast radius. Behavioral detection would have surfaced the anomalous data access before exfiltration was complete.*

③ Detect Fast	SIEM with healthcare-specific alert rules · Epic audit log review on a defined schedule · Anomaly detection for bulk PHI access and off-hours administrative activity · 24/7 SOC or MDR coverage · UEBA for insider threat detection	*Detection failed for nine days. Modern ransomware groups generate detectable behavioral signals during reconnaissance and exfiltration phases. Behavioral monitoring for anomalous authentication and data access would have provided intervention opportunity.*
④ Respond Clean	Tested incident response plan with Epic-specific procedures · Clinical downtime procedures tested annually · Breach notification workflow documented · Legal counsel and cyber insurance pre-engaged · Forensic retainer in place before the incident	*Every hour of delay in the response window adds cost and regulatory exposure. Organizations with pre-engaged forensic retainers and tested IR plans contain incidents faster and document them better for OCR.*
⑤ Prove Compliance	Current risk analysis covering full environment · Active risk management plan · Updated policies and training records · Audit log review documentation · BA agreement and oversight records · Incident documentation for all threshold events	*The OCR investigation added settlement exposure on top of operational breach costs. Organizations with current, complete compliance documentation reduced their regulatory exposure. Documentation does not prevent breaches; it limits the additional damage after one.*

The 10 Security Questions Every Healthcare CIO and CISO Should Answer Right Now

These are not rhetorical. Each one maps to a specific control gap documented in at least one major healthcare breach. If the answer to any of them is 'I'm not sure,' the uncertainty is itself a finding.

- **1.** Is MFA enforced on every remote access point that touches ePHI — including Citrix, VPN, RDP, and Epic's Haiku/Canto mobile access? Is there any pathway through which valid credentials alone grant remote access?
- **2.** When were Epic audit logs last reviewed by a human? What anomalous access patterns would trigger an alert, and is that alert process documented and tested?
- **3.** What is the most recent vulnerability scan result for internet-facing systems? When was the last critical patch applied, and what is the SLA for critical patching?
- **4.** Which business associates have access to ePHI, and when was the last evidence-based verification that they have the required security controls in place?
- **5.** What are the Epic RBAC role assignments for every active user, and when was the last formal review of whether those assignments match current job functions?
- **6.** What network segmentation separates clinical systems, administrative systems, and vendor/third-party access? Can a compromised vendor device reach Epic production systems without crossing a monitored boundary?
- **7.** When was the clinical downtime procedure last tested? Do all nurses, physicians, and clinical support staff in every department know what to do if Epic is unavailable for 72 hours?
- **8.** Is the backup environment isolated from the production network? When was the last tested recovery from backup, and what was the recovery time result?
- **9.** When was the risk analysis last updated? Does it cover cloud systems, mobile devices, third-party integrations, and the Epic integration layer, or only the core data center?
- **10.** If OCR contacted you today requesting documentation of your security program, how long would it take to produce: the current risk analysis, the risk management plan, training completion records, audit log review records, and BA agreements?

A final note on the Change Healthcare lesson

Change Healthcare did not fail because it lacked security expertise or security investment. It failed because a known, basic control — multi-factor authentication on a remote access portal

— was not applied to a critical system. The gap was not exotic. The consequences were unprecedented.

The healthcare organizations that will avoid the next major breach are not necessarily the ones with the most sophisticated security programs. They are the ones that have made sure the basics are actually implemented, not just documented. MFA on every remote access point. Audit log review on a schedule. RBAC that reflects actual job functions. Backups that are tested and isolated. These are not advanced controls. They are the controls that Change Healthcare was missing. They are the controls that most major healthcare breaches since 2015 were missing.

About Apsis Solutions Inc.

Apsis Solutions Inc. is a Tampa-based healthcare IT consulting firm specializing in Epic implementation, HIPAA compliance, cybersecurity risk management, and IT workforce staffing. We serve health systems, academic medical centers, federal agencies, and prime contractors as a capable prime vendor, strategic subcontractor, and managed services partner. Our cybersecurity practice combines Epic-specific security configuration expertise with NIST CSF, HITRUST, and SOC 2-aligned security program design. We have worked inside Epic environments on the specific control failures described in this guide. The agility of a boutique firm. The capability of a prime. — apsisinc.com | 813-999-4853 | info@apsisinc.com