HIPAA Risk Analysis

Q4 2025

Report Date: December 31, 2025

521 Lincoln Road
West Enfield, ME 04493

Executive Summary

Work Performed

RESCOR performed its thirteenth annual HIPAA risk analysis of Sample Medical Center ("the Hospital") during the period from November 2025 through January 2026. The scope of work included:

- A summary risk analysis of information technology, human, facilities, and business process assets, consistent in scope with prior years
- Interviews with key Hospital stakeholders to determine changes in the risk environment since the 2024 assessment
- Analysis of technical vulnerability assessment (TVA) data to assess changes in technical risk posture
- Review of new risk factors introduced by the Houlton Regional affiliation, AI adoption, and EMR platform changes

Seven stakeholders were interviewed during this assessment period, representing the following functions:

- Networking and IT Infrastructure
- Software Development and Reporting
- Clinical Informatics and Emergency Preparedness
- Performance Improvement
- Administration
- Finance (CFO)
- Quality

Consultant's Opinion

Overall risk decreased 15.8% from 2024 to 2025 (19 RU to 16 RU), and has decreased 52% since 2013. The primary drivers are the deployment of a Palo Alto next-generation firewall with Precision AI EDR/IDS/IPS capabilities, continued improvements to business continuity planning, and the reinstatement of governance structures including the IT Steering Committee. This reverses the 5.5% increase observed between 2022 and 2023.

The Houlton Regional affiliation is the most substantial new risk factor (8 RU). The managed services agreement is six months in progress, and introduces integration risks across several dimensions: differing EMR platforms, divergent security philosophies, ad hoc file sharing arrangements, PACS system alignment, and Active Directory Forest integration. These are typical of healthcare affiliations and are manageable with deliberate governance.

AI adoption is accelerating without a finalized governance framework (8 and 7 RU across two related findings). The Hospital's IS team uses CoPilot, ChatGPT, Whisper (OpenAI transcription), and Mandiant for operational efficiency. Clinical services are using Cerner Scribe for AI-assisted documentation, and cardiology is introducing additional AI tools. Internally reported productivity improvements range from 10-40%. A draft AI policy based on a RESCOR template is under review, and the CFO has initiated an AI workgroup, but the policy has not been formally adopted and BAA requirements for AI services have not been fully addressed.

The Hospital's EMR vendor's evolving platform strategy raises questions about the long-term continuation and support of the current clinical system (7 RU). The Hospital should develop contingency plans to ensure continuity of clinical operations regardless of vendor decisions. Any transition of this magnitude would typically require 2-3 years and a dedicated implementation firm, particularly given the Houlton affiliation and its implications for system alignment.

The retirement of a senior informatics specialist has concentrated critical clinical informatics and emergency preparedness functions in a single individual (6 RU). Informatics staffing is down, with supporting staff allocated at 25% or less. The Hospital is recruiting a CIO, which should improve governance, but operational coverage in the interim is thin.

A terminated employee retained mobile access to Hospital systems (4 RU). This gap in separation procedures was identified during interviews. Union and labor law constraints complicate mobile device policies, but the access control gap on separation represents a HIPAA exposure.

Overall Risk

Overall residual risk decreased 15.8% between 2024 and 2025 (19 RU to 16 RU). Overall residual risk has decreased 52% between 2013 and 2025.

The overall STORM (Simplified Total Risk Management) measurement for 2025 is 16 RU (HIGH), the second-lowest aggregate in 13 years of assessment, after 2021.

The qualitative rating remains HIGH (any value >= 9 RU). The Hospital's risk environment continues to be dominated by technical vulnerabilities (12 RU), obsolete software (11 RU), and email-based attacks (11 RU), offset by new investment in perimeter security and detection capabilities.

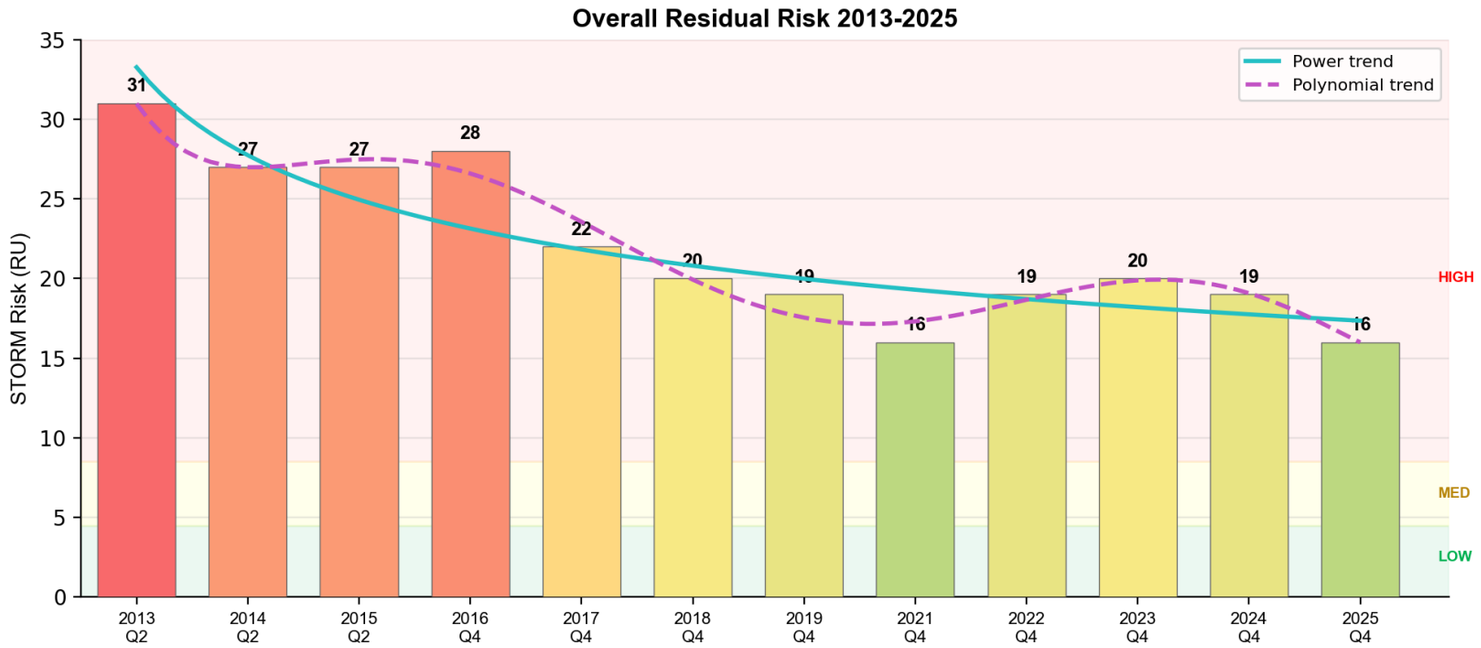

Chart 1 — Overall Residual Risk 2013-2025

Using This Report

This report uses the STORM (Simplified Total Risk Management) methodology to quantify and compare risk values across assessment periods. Risk values are expressed in Risk Units (RU) on a fixed scale.

Qualitative Rating	RU Range	Color
High	9 RU and above	

Medium	5 RU to 8 RU	
Low	1 RU to 4 RU	

Trend indicators: ↓ Decreased ↔ Stable ↑ Increased

The STORM aggregate risk value uses a geometric diminishing-weight series that sorts all findings in descending order and applies exponentially decreasing weights, ensuring that the overall risk score is dominated by the most critical findings while still reflecting the breadth of the risk landscape.

Findings

The following tables present the residual risk for each finding tracked in this assessment. Active findings are sorted by current RSK value in descending order. Findings new to this assessment period are shown in bold.

Active Findings

Each column represents an assessment period. Cell shading reflects the RSK value on a continuous green (low) to red (high) gradient.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
2	Mission-critical systems have severe vulnerabilities	16	14	14	12	12	15	13	12	↓	High-severity findings (>=70 RU) increased 17% (16,147 to 18,882), but the deployment of Palo Alto Precision AI EDR/IDS/IPS and Global Protect VPN represents substantial new technical controls. The Hospital remains in the 68th percentile of similar organizations tested.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
6	Obsolete and unsupported software is in use	11	9	8	7	6	8	11	11	↔	Obsolete/ unsupported software findings decreased 9.3% (1,038 to 941), but VLAN isolation for end-of-life systems has not yet been implemented. The pharmacy acquisition adds endpoints with legacy software. Top TVA findings include unsupported Internet Explorer, Oracle Java JRE, Adobe Flash Player, Wireshark, and database servers, all at 100 RU.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
35	Hospital experiencing an increase in sophisticated email attacks	-	-	-	-	-	-	10	11	↑	Phishing and spoofing activity on Office 365 continues to increase. An invoice spoofing incident occurred during the reporting period, and executive administration was specifically targeted.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
3	Hospital does not have a formal, integrated, cross-functional incident response plan	8	8	8	7	11	10	10	10	↔	IRP components exist but the IT portion has not been stress-tested. The Regroup mass notification system is being implemented. Escalation procedures were identified as a gap.
1	Hospital does not perform a BIA and does not have a comprehensive BCP	16	15	14	12	15	13	10	9	↓	Each department has a BCP binder; key business processes identified; EMO procedures developed and tested. CEO engaged in emergency preparedness.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
42	Hospital affiliation (Houlton Regional) introduces integration risk	-	-	-	-	-	-	-	8	↑	Managed services agreement six months in. Differing EMR platforms, divergent security approaches, ad hoc file sharing, PACS alignment, AD Forest integration in progress. ~20% of informatics time consumed.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
39	The incident response plan needs to be stress-tested	-	-	-	-	-	-	8	8	↔	Tabletop exercises not yet conducted for IT IRP component. EP coordinator supports stress testing but has not scheduled it.
36	AI adoption should be subject to careful governance	-	-	-	-	-	-	7	8	↑	AI in use across multiple departments. Draft AI policy under review but not adopted. BAA requirements unresolved. Workgroup formed but not yet active.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
28	Insufficient network segmentation	-	8	8	8	7	7	8	7	↓	Geographic VLANs (per floor) in place. Palo Alto firewall at pharmacy. Functional segmentation for obsolete, pre-deployment, and testing systems not yet implemented.
43	**EMR platform vendor dependency and long-term uncertainty**	-	-	-	-	-	-	-	**7**	↑	**EMR vendor's platform strategy creates uncertainty about long-term continuation and support of the current clinical system.**

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
44	AI policy and governance framework incomplete	-	-	-	-	-	-	-	7	↑	Draft AI policy based on RESCOR template under review but not adopted. Vetting procedures, BAA requirements, and legal liability framework not finalized. an applicable state AI regulation introduces regulatory considerations.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
33	Cerner implementation has introduced ongoing EMR challenges	-	-	-	-	-	7	7	7	↔	Vendor transitioning platform to cloud infrastructure. Support responsiveness remains a concern.
16	IT team does not have sufficient resources	4	5	5	5	5	6	6	7	↑	Senior informatics specialist retired. EP coordinator doing double duty. Informatics staffing at <25% allocation. Houlton adding ~20% workload. CIO being recruited.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
38	Monitor M&A risks	-	-	-	-	-	-	5	7	↑	Houlton affiliation more complex than anticipated. Retail pharmacy integration ongoing. Resource consolidation and EMR strategy unresolved.
40	Civil liability exposure related to HIPAA	-	-	-	-	-	-	7	7	↔	Cyber liability policy in place. No material change.
34	Insufficient perimeter and network detection and response	-	-	-	-	-	-	8	6	↓	Palo Alto next-generation firewall with Precision AI, EDR/IDS/IPS, and Global Protect VPN deployed.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
5	Lack of consistent, cross-functional risk management program	7	7	7	7	6	6	6	5	↓	IT Steering Committee being reinstated. CEO driving structured reporting. CFO and CMO engaged.
31	Legacy systems have indeterminate business impact	-	-	-	-	-	7	6	6	↔	Three legacy systems remain (AS/400, MedHost VMs, ECW/CAPStone). MedHost VMs unpatched. Data retention requirements drive continued operation.
37	PCI risks from products/services and acquisitions	-	-	-	-	-	-	6	6	↔	Retail pharmacy PCI compliance being addressed (Pioneer Rx).

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
46	**Key person dependency in clinical informatics and EP**	-	-	-	-	-	-	-	**6**	↑	**Senior informatics specialist retired. EP coordinator covering both roles. HAZMAT staffing gap.**
30	Personnel turnover	-	-	-	-	-	5	6	5	↓	Turnover recovered from COVID peaks. Stable leadership team.
41	IS team not a stakeholder in technology decisions	-	-	-	-	-	-	5	5	↔	Hospitalist group acquired equipment without IS consultation. CIO recruitment expected to improve governance.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
45	**Quality department incident reporting involves unsecured PHI**	-	-	-	-	-	-	-	**4**	↑	**Incident reports on paper, transferred to Excel with PHI. Quality department door sometimes unlocked.**
26	IS infrastructure vulnerable to DoS from routine testing	14	8	8	8	6	5	4	3	↓	Nessus scans scheduled for weekends. Printer disruptions reduced.
17	Higher reputational risk (small, isolated community)	4	4	4	4	4	3	3	3	↔	No change from 2024.

#	Risk Description	2017	2018	2019	2021	2022	2023	2024	2025	Trend	Explanation
21	Access control problems during role changes and separation	2	4	4	6	4	3	3	4	↑	Terminated employee retained cell phone access. Union/labor law constraints complicate mobile access revocation.
32	Physical lockdown process causes accidental lockdowns	-	-	-	-	-	4	3	2	↓	Frequency reduced. Maintenance manages physical security. Drills being considered.

Deprecated Findings

The following findings have been deprecated due to three or more successive years of no measurable residual risk (RSK < 1 RU):

#	Risk Description	Last Observed	Last RSK	Explanation
7	Insufficient minimum necessary response procedures	2021	2	Cerner permits finer-grained access control.
8	Insufficient minimum necessary training	2021	2	Training improved; no longer reported by personnel.

#	Risk Description	Last Observed	Last RSK	Explanation
10	Mobile device reliance	2023	5	MDM implemented; policy in place.
4	Compartmentalized organizational structure	2023	2	Culture shifted toward collaboration under new leadership.
13	Administrative accounts with trivial login controls	2023	2	Passwords hardened; MFA deployed; Imprivata SSO.
11	Reactive rather than proactive	2023	2	Proactive posture maintained through disruptions.
27	Smart Home devices privacy risk	2023	1	Procedures documented.
9	EHR vendor lock-in (HMS/eCW)	2023	1	Migrated to Cerner; legacy EMRs read-only. New platform dependency in Finding 43.
15	Insufficient password controls	2023	1	12-15 char passwords; MFA; Imprivata SSO.
14	Insufficient disclosure monitoring and auditing	2023	1	Cerner audit trail; privacy officer; P2Sentinel.

Recommendations

The following tables list all active and completed recommendations. Active recommendations are sorted by percentage of work remaining in descending order. Recommendations new to this assessment period are shown in bold.

Active Recommendations

The % Work Remaining and Cost-Effort columns are shaded on the same green-to-red gradient as the findings table.

Description	New?	% Work Remaining	Cost-Effort	Findings
Develop security integration framework for Houlton affiliation	**X**	**95%**	**9**	**42, 38**
Develop EMR platform contingency and continuity plan	**X**	**95%**	**6**	**43, 33**
Finalize and adopt AI governance policy and BAA framework	**X**	**90%**	**4**	**44, 36**
Develop data retention policy for cloud-based storage	**X**	**90%**	**2**	**5, 31**
Create segregated VLAN for Pre-Deployment Systems		90%	4	28
Ensure that all AI decisions affecting third parties are ratified by humans		90%	1	35, 44
Digitize quality department incident reporting and secure PHI	**X**	**85%**	**3**	**45**
Establish IT governance dashboard for executive leadership	**X**	**85%**	**3**	**41, 5**

Description	New?	% Work Remaining	Cost-Effort	Findings
Create segregated VLAN for End-of-Life Systems		85%	4	28, 6
Develop an SDLC process based on DevSecOps or similar process		85%	2	24
Evaluate Hospital's protection against civil liability related to HIPAA		85%	3	40
Evaluate PCI risks from M&A and third-party services		85%	4	37, 38
Document and risk-assess all AI use and potential use within the Hospital		85%	2	36
Address key-person dependency in clinical informatics and EP	**X**	**80%**	**4**	**46, 16**
Implement AI-based email protections to intercept sophisticated attacks		80%	6	35, 36
Stress-test the incident response plan with tabletop exercises		75%	4	39, 3
Address the recommendations in the technical vulnerability assessment		75%	6	2
Create segregated VLANs for servers, workstations, and infrastructure		75%	4	28
Create segregated VLAN for laboratory environment		75%	4	26, 28
Remediate terminated-employee mobile/BYOD access revocation gap	**X**	**70%**	**2**	**45, 21**

Description	New?	% Work Remaining	Cost-Effort	Findings
Integrate existing incident planning, BIA, BCP, and DRP		70%	6	1
Develop a Hospital-wide, cross-functional incident response plan		70%	4	3
Document existing auditing, monitoring, and investigation capabilities		70%	3	14
Develop procedures to assess impact of legacy systems and plan for retirement		55%	3	31
Plan for continuation of security operations under extraordinary circumstances		55%	4	1, 3, 5, 16
Increase the IT department's budget and permit additional staffing		55%	6	16
Migrate obsolete operating systems and applications		55%	6	2, 6
Involve IS implementor and support representative in technology decision-making		55%	2	41
Reinstate IT Steering Committee or equivalent governance body	**X**	**50%**	**1**	**5, 41**
Perform a detailed risk analysis and BIA of physical security issues		45%	3	12

Description	New?	% Work Remaining	Cost-Effort	Findings
Implement AI-based perimeter and network detection and response (PNDR)		40%	9	34, 36
Monitor existing community outreach and quality assurance programs		35%	1	17
Optimize incident response plan for unexpected infrastructure outages		35%	6	26
Develop a formal mobile device policy and strategy		25%	2	10, 21
Use unencrypted electronic mail with care		25%	1	23, 35
Create a standard security testing schedule focusing on high-risk resources		20%	2	1, 6
Adopt strong password requirements		15%	1	13, 15
Create a central disclosure authorization and review function		15%	4	7
Adopt a lightweight, continuous adaptation ("agile") process		15%	4	1, 3, 5
Improve physical lockdown procedures		5%	2	32
Upgrade and harden infrastructure		5%	9	26
Provide ongoing security and privacy training to new and existing staff		5%	2	8

Description	New?	% Work Remaining	Cost-Effort	Findings
Document operations of "smart home" devices and develop procedures for patient privacy		5%	1	27

Fully Remediated

The following recommendations have been fully implemented and are carried for historical reference.

Description	Findings
Purchase and use a security testing tool	2, 6
Harden the physical records storage facility	18
Ensure all user accounts disabled or have strong passwords	13, 15
Develop core systems (EHR) migration strategy	9

Appendix A — HIPAA Control Review Matrix

The HIPAA Control Review Matrix evaluates each implementation specification from 45 CFR 164 against the Hospital's current controls. The Residual Risk column represents the STORM aggregate of all active findings related to each control. The CMM (Capability Maturity Model) column rates the organizational maturity of each control on a 1-4 scale.

Standard	Control Class	45 CFR Section	Implementation Specification	Reviewed	Depth	CMM	Residual Risk (RU)	Related Findings
Security Management Process	Administrative	164.308(a)(1)(ii)(A)	Risk Analysis (R)	Yes	Deep	4	5	5
Security Management Process	Administrative	164.308(a)(1)(ii)(B)	Risk Management (R)	Yes	Deep	4	5	5
Security Management Process	Administrative	164.308(a)(1)(ii)(C)	Sanction Policy (R)	Yes	Shallow	2	5	30
Security Management Process	Administrative	164.308(a)(1)(ii)(D)	Information System Activity Review (R)	Yes	Moderate	4	3	26
Assigned Security Responsibility	Administrative	164.308(a)(2)	Assigned Security Responsibility (R)	Yes	Moderate	3	9	46, 16
Workforce Security	Administrative	164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A)	Yes	Shallow	2	4	21
Workforce Security	Administrative	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A)	Yes	Moderate	3	4	21
Workforce Security	Administrative	164.308(a)(3)(ii)(C)	Termination Procedures (A)	Yes	Deep	3	9	21, 42

Standard	Control Class	45 CFR Section	Implementation Specification	Reviewed	Depth	CMM	Residual Risk (RU)	Related Findings
Information Access Management	Administrative	164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (R)	Yes	Shallow	3	4	[1]
Information Access Management	Administrative	164.308(a)(4)(ii)(B)	Access Authorization (A)	Yes	Moderate	3	9	21, 42
Information Access Management	Administrative	164.308(a)(4)(ii)(C)	Access Establishment and Modification (A)	Yes	Moderate	3	9	21, 42
Security Awareness and Training	Administrative	164.308(a)(5)(ii)(A)	Security Reminders (A)	Yes	Moderate	3	11	35
Security Awareness and Training	Administrative	164.308(a)(5)(ii)(B)	Protection from Malicious Software (A)	Yes	Moderate	3	14	2, 34
Security Awareness and Training	Administrative	164.308(a)(5)(ii)(C)	Log-in Monitoring (A)	Yes	Moderate	2	6	34
Security Awareness and Training	Administrative	164.308(a)(5)(ii)(D)	Password Management (A)	Yes	Moderate	3	4	[1]
Security Incident Procedures	Administrative	164.308(a)(6)(ii)	Response and Reporting (R)	Yes	Deep	3	12	3, 39
Contingency Plan	Administrative	164.308(a)(7)(ii)(A)	Data Backup Plan (R)	Yes	Moderate	3	6	31
Contingency Plan	Administrative	164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R)	Yes	Moderate	3	11	1, 43
Contingency Plan	Administrative	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R)	Yes	Deep	3	11	1, 43

Standard	Control Class	45 CFR Section	Implementation Specification	Reviewed	Depth	CMM	Residual Risk (RU)	Related Findings
Contingency Plan	Administrative	164.308(a)(7)(ii)(D)	Testing and Revision Procedures (A)	Yes	Moderate	3	8	39
Contingency Plan	Administrative	164.308(a)(7)(ii)(E)	Application and Data Criticality Analysis (A)	Yes	Moderate	2	9	31, 43
Evaluation	Administrative	164.308(a)(8)	Evaluation (R)	Yes	Moderate	4	2	[1]
Business Associate Agreements	Administrative	164.308(b)(4)	Business Associate Agreements (R)	Yes	Shallow	3	11	36, 44, 42
Facility Access Controls	Physical	164.310(a)(2)(i)	Contingency Operations (A)	Yes	Moderate	3	9	1
Facility Access Controls	Physical	164.310(a)(2)(ii)	Facility Security Plan (A)	Yes	Moderate	4	2	32
Facility Access Controls	Physical	164.310(a)(2)(iii)	Access Control and Validation Procedures (A)	Yes	Moderate	3	4	45
Facility Access Controls	Physical	164.310(a)(2)(iv)	Maintenance Records (A)	Yes	Shallow	2	11	6
Workstation Use	Physical	164.310(b)	Workstation Use (R)	Yes	Moderate	3	11	6
Workstation Security	Physical	164.310(c)	Workstation Security (R)	Yes	Moderate	3	16	2, 6, 34
Device and Media Controls	Physical	164.310(d)(2)(i)	Disposal (R)	Yes	Moderate	3	4	[1]
Device and Media Controls	Physical	164.310(d)(2)(ii)	Media Re-use (R)	Yes	Moderate	3	4	[1]

Standard	Control Class	45 CFR Section	Implementation Specification	Reviewed	Depth	CMM	Residual Risk (RU)	Related Findings
Device and Media Controls	Physical	164.310(d)(2)(iii)	Accountability (A)	Yes	Moderate	3	4	[1]
Device and Media Controls	Physical	164.310(d)(2)(iv)	Data Backup and Storage (A)	Yes	Moderate	3	6	31
Access Control	Technical	164.312(a)(2)(i)	Unique User Identification (R)	Yes	Moderate	3	4	21
Access Control	Technical	164.312(a)(2)(ii)	Emergency Access Procedure (R)	Yes	Moderate	3	9	1
Access Control	Technical	164.312(a)(2)(iii)	Automatic Logoff (A)	Yes	Moderate	3	4	[1]
Access Control	Technical	164.312(a)(2)(iv)	Encryption and Decryption (A)	Yes	Moderate	3	11	35
Audit Controls	Technical	164.312(b)	Audit Controls (R)	Yes	Moderate	3	3	26
Integrity	Technical	164.312(c)(2)	Mechanism to Authenticate ePHI (A)	Yes	Moderate	3	12	2
Person or Entity Authentication	Technical	164.312(d)	Person or Entity Authentication (R)	Yes	Moderate	3	4	21
Transmission Security	Technical	164.312(e)(2)(i)	Integrity Controls (A)	Yes	Moderate	3	15	2, 35
Transmission Security	Technical	164.312(e)(2)(ii)	Encryption (A)	Yes	Moderate	3	11	35
Policies and Procedures	Documentation	164.316(a)	Policies and Procedures (R)	Yes	Moderate	3	11	44, 36, 42
Documentation	Documentation	164.316(b)(2)(i)	Time Limit (R)	Yes	Shallow	4	2	[1]

Standard	Control Class	45 CFR Section	Implementation Specification	Reviewed	Depth	CMM	Residual Risk (RU)	Related Findings
Documentation	Documentation	164.316(b)(2)(ii)	Availability (R)	Yes	Shallow	4	2	[1]
Documentation	Documentation	164.316(b)(2)(iii)	Updates (R)	Yes	Moderate	4	2	[1]

[1] *Controls with no directly associated findings have their residual risk imputed from the CMM level: Initiating = 8 RU, Developing = 6 RU, Sustaining = 4 RU, Optimizing = 2 RU. This ensures all controls carry a risk measurement proportional to their maturity.*

Level	Name	Description
1	**Initiating**	Need identified; implementation not begun
2	**Developing**	Implementation begun; not yet consistent or fully operational
3	**Sustaining**	Implemented, operational, and consistently applied
4	**Optimizing**	Mature, regularly reviewed, continuously improved

2025 CMM Change: Workforce Clearance Procedure (2 → 3): Workforce reconciliation process implemented; HR comparison lists used for periodic verification of active accounts. All other controls maintained their 2024 levels. No decreases.

Intellectual Property Notices

This report is the proprietary work product of RESCOR and is provided to Sample Medical Center under the terms of the engagement agreement. This report contains confidential information and should be treated accordingly.