

SECTION I · RSP ASSESSOR'S REPORT

RSP Actively Managed Report

HIPAA compliance program · Northfield Community Hospital (HIPAA NIST Actively Managed Demo) · Covered entity

Contents: Section I, the RSP Assessor's report. Section II, management's attestation. Appendix A, the check-by-check review record.

Prepared for	Northfield Community Hospital (HIPAA NIST Actively Managed Demo)
Entity type	Covered entity under HIPAA
Program period	Oct 10, 2025 to Oct 10, 2026
Management's attestation	Tomas Berg, Chief Technology Officer, Oct 10, 2026 (Section II)
Readiness at filing	100% of HIPAA Program Path checks met and substantiated
RSP Assessor	Morgan Ellis, CISA, CISSP (Demo Assessor), RSP Assessor, MTC Group LLC
Issued	Oct 10, 2026
Assessment	RSP Actively Managed (12 months of records)
Period assessed	Oct 10, 2025 to Oct 10, 2026, the 12 months before the assessment
Interview	Oct 10, 2026, 9:15 AM ET, 60 minutes, with Tomas Berg (Chief Technology Officer), Aisha Bello (Security Lead)
Recognized Security Practices	Records in 12 of the 12 months preceding this assessment
Next assessment due	Oct 10, 2027

OPINION

Gaps identified

1. Executive summary

Northfield Community Hospital (HIPAA NIST Actively Managed Demo) attested that its HIPAA compliance program was in place from Oct 10, 2025 to Oct 10, 2026 and asked for an independent RSP Assessment of it. This report records that review: what was examined, how, what was found, and the RSP Assessor's opinion.

This is an RSP Actively Managed Report: it covers the 12 months preceding this assessment, the period 42 U.S.C. 17941(b) has the Office for Civil Rights consider, for a program implemented to NIST SP 800-66 Rev. 2. For each check the RSP Assessor drew the population of the program's own time-stamped records in that period, held each practice to its cadence (monthly, quarterly, six-monthly, annual, on each event, or standing), and tested a sample of the records against their evidence. Management's written representation and the RSP Assessor's independence are stated below.

Measure	Result
Program Path steps filed	12
Checks on the filed path	169
Checks tested and verified	166

Measure	Result
Checks that produced a finding	3
Checks not tested in this review	0
Findings recorded (critical / high / medium / low)	3 (0 / 0 / 3 / 0)
Findings open when this report was issued	3
Readiness at filing	100%

2. Opinion

Gaps identified

The program was examined on its own records for each month of the 12-month period: every practice at its operating cadence, each event with its follow-through, and the standing registers in place from the start. Suggested samples were drawn at random across the quarters of the period and tested against the records and the evidence on them. Management signed its written representation. Where the records show a missed cycle it is reported as a finding with its remediation.

3. Management's attestation

This review was made on the program management filed and attested. Tomas Berg, Chief Technology Officer signed management's attestation by typed name on Oct 10, 2026, when the program was filed for the period Oct 10, 2025 to Oct 10, 2026. It is reproduced in full as Section II of this document, which accompanies this report. Management is responsible for the program and for the assertions in its attestation; the RSP Assessor's responsibility is the opinion in section 2, formed on the program that attestation describes.

4. Scope and approach

The review covered the HIPAA program as filed on the Program Path: a snapshot of every step, check, answer, policy, training record, configuration record and evidence reference, locked at the moment of filing so the program could not change under review. SOC 2 and ISO/IEC 27001 are outside this review; they are examined by a licensed CPA firm and an accredited certification body.

Every standard is held to the same four elements, and a check is met only when each element that applies is substantiated, never on a single yes:

- Policy: the standard is addressed in an approved, active written policy or procedure.
- Training: the workforce has been trained where the standard depends on people knowing what to do.
- Configuration: systems are configured as the policy requires, shown by screenshots or exports.
- Evidence: records prove the control operates (logs, registers, exercises, signed agreements, completions).

For each check the RSP Assessor recorded one result:

- Verified: the RSP Assessor examined the records behind the check and they support it. The note says what was sampled.

- **Finding:** the records do not support the check, or a gap was identified. Each finding is described in section 11.
- **Not tested:** the check was not sampled in this review. It is not an adverse result, and it carries no assurance.

The program on file included these records at filing:

Register or inventory	Entries at filing
Workforce Roster	13
ePHI System and Asset Inventory	6
User Access Roster	60
Workforce Training Log	39
Security Incident Log	2
Information System Activity Review Log	13
Backup Job Log	13

5. Period and coverage

The assessment covered the 12 months from Oct 10, 2025 to Oct 10, 2026, frozen when it started. For each check the RSP Assessor drew the population of the program's own time-stamped records in the platform and tested whether the practice operated across the period: a recurring practice when no interval between its records exceeded its cadence plus 10%, counting the last record before the period; an event practice when every event in the period had its required follow-through; a standing practice when it was in place at the period start and still is. The organization did not hold a platform subscription for the whole period; records kept outside the platform were not examined.

Measure	Result
Checks concluded	169
Operated across the period	159
Coverage gaps (each a finding)	3
Event practices with no event in the period	0
Concluded on evidence (no time-stamped record exists)	7
Records in the period	1478
Entered more than 30 days after the event	6
Entered after the assessment started	0

6. Sampling

Sample sizes followed the method: one record for an annual or six-monthly practice, two for a quarterly one, two for a monthly one (three when any record was entered late), and by population size for event and per-person practices; one exception doubled the sample once. Random samples were drawn from a stored seed, spread across the quarters of the period. Each sampled record was frozen as it stood and its evidence locked before it was tested.

Measure	Result
Samples suggested by the method	247
Samples tested (of them, drawn at random)	247 (247)
Passed	246
Exceptions	1
Checks sampled below the suggestion, with a written rationale	0
Evidence requests to the organization (accepted)	2 (2)

7. Exceptions (4)

Source	Check	Record	What the evidence did not show
Sample	A6	Activity review log, 2026-05	Review dated 2026-05-19 follows a 61-day interval since 2026-03-19; the April review was not performed. Monthly cadence not met for this window.
Coverage	C5	No record for 2025-09-17 to 2026-10-11	See the finding on this check.
Coverage	A6	No record for 2026-03-19 to 2026-05-19	See the finding on this check.
Coverage	A6	No record for 2026-03-19 to 2026-05-19	See the finding on this check.

8. Management's representation

In connection with the RSP assessment of Northfield Community Hospital (HIPAA NIST Actively Managed Demo)'s HIPAA security program for the period 2025-10-10 to 2026-10-10, management represents that:

1. The records in HealthData DueCare for the period are the organization's own records of the practices it performed, and they are complete and accurate.
2. Every record the RSP Assessor requested has been provided, or the organization has said it does not exist.
3. No record was created, backdated or changed to answer the assessment, except where the platform shows it as entered late or after the assessment started.
4. Management knows of no security incident, breach, or departure from these practices during the period that is not recorded in the platform.
5. Management is responsible for the program and for the practices it describes.

Signed by typed name: Marta Lindqvist, Administrator (Site Admin), Oct 10, 2026.

9. Independence

Morgan Ellis, CISA, CISSP (Demo Assessor), the RSP Assessor, held no program (fCISO) or advisory engagement with Northfield Community Hospital (HIPAA NIST Actively Managed Demo) in the 24 months before this report, as recorded in the platform's assignment history.

10. Results by Program Path step

Step	Met as filed	Verified	Finding	Not tested
1. Set up your organization	6/6	6	0	0
2. Load your workforce	3/3	3	0	0
3. Load your systems and assets	2/2	2	0	0
4. Assess your vendors	2/2	2	0	0
5. Map access to your systems	1/1	1	0	0
6. Assign roles and responsibilities	3/3	3	0	0
7. Adopt your policies and procedures	7/7	7	0	0
8. Analyze and treat your risks	6/6	6	0	0
9. Train the workforce	10/10	10	0	0
10. Put the agreements in place	6/6	6	0	0
11. Implement and evidence the safeguards	60/60	59	1	0
12. Operate the program	63/63	61	2	0

11. Findings (3)

Each finding is shown as it stood when this report was issued. Its current state is tracked on the organization's Program Path, on the step it belongs to.

Finding 1 · Medium · Open at issuance

Step: Operate the program · Check: A6 Information system activity review (log and report review) performed on a defined cadence · 45 C.F.R. 164.308(a)(1)(ii)(D)

Condition

Activity review log shows no information system activity review between 2026-03-19 and 2026-05-19 (61 days) against a monthly cadence; the April 2026 review was not performed.

Recommendation

Assign a backup reviewer for the monthly activity review and add a due-date reminder so a missed month is caught before the next window.

Finding 2 · Medium · Open at issuance

Step: Implement and evidence the safeguards · Check: C5 Access establishment and modification procedure · 45 C.F.R. 164.308(a)(4)(ii)(C)

Condition

Access establishment and modification procedure: the records show a gap in the period (2025-09-17T00:00:00.000Z to 2026-10-11T00:00:00.000Z, 389 days), longer than its quarterly cadence allows.

Recommendation

Perform and record the practice on its cadence, with a reminder so a missed cycle is caught within the cycle.

Finding 3 · Medium · Open at issuance

Step: Operate the program · Check: A6 Information system activity review (log and report review) performed on a defined cadence · 45 C.F.R. 164.308(a)(1)(ii)(D)

Condition

Information system activity review (log and report review) performed on a defined cadence: the records show a gap in the period (2026-03-19T10:00:00.000Z to 2026-05-19T10:00:00.000Z, 61 days), longer than its monthly cadence allows.

Recommendation

Perform and record the practice on its cadence, with a reminder so a missed cycle is caught within the cycle.

12. Basis and limitations

This report states the RSP Assessor's professional opinion on the program as attested and sampled during the review. It is not a certification, accreditation or guarantee of HIPAA compliance, and no such certification exists. The U.S. Department of Health and Human Services Office for Civil Rights determines compliance. This review is one of the organization's own evaluation records under 45 C.F.R. 164.308(a)(8) and part of its recognized security practices.

The assessment relied on the records the organization keeps in the platform and on the evidence attached to them. Operation was tested on samples of each practice; a practice is not shown to have operated beyond what its records and samples show. Conditions can change after the period assessed.

Samples were selected at random, spread across the period, and are reproducible from their stored seed. Conclusions rest on the items tested and are not projected to the whole population.

13. Document integrity

SHA-256: aec3244153f153e249c737814d2aa70d39583486f1fff98502e0b4ef5bc1d08f

The hash covers the recorded opinion, narrative, scope counts and findings of this report. The same value is shown on the organization's Trust Hub and its HealthData DueCare record; a copy whose recorded content produces a different hash has been altered. The step results and the check-by-check record are drawn from the locked filing and the review record.

Issued electronically by

Morgan Ellis, CISA, CISSP (Demo Assessor)

RSP Assessor, MTC Group LLC · Oct 10, 2026

SAMPLE

SECTION II · MANAGEMENT'S ATTESTATION

Northfield Community Hospital (HIPAA NIST Actively Managed Demo)

Management's attestation on the HIPAA compliance program

To	MTC Group LLC, the RSP Assessor, and the users of the accompanying RSP Assessment Report
Program period	Oct 10, 2025 to Oct 10, 2026
Accompanies	RSP Actively Managed Report, issued Oct 10, 2026 by Morgan Ellis, CISA, CISSP (Demo Assessor) (Section I)
Report SHA-256	aec3244153f153e249c737814d2aa70d39583486f1fff98502e0b4ef5bc1d08f

Management of the organization is responsible for designing, implementing and maintaining its HIPAA compliance program, and for the Program Path filed on HealthData DueCare that describes it (the filed program). The filed program is held to the standards of the HIPAA Security Rule carried out to NIST SP 800-66 Rev. 2. Management may engage MTC Group LLC to have an independent RSP Assessor assess the filed program and state an opinion on it in an RSP report, which this attestation then accompanies.

Management asserts that, for the period stated:

1. The filed program fairly presents the HIPAA compliance program in place at the organization: its policies and procedures, workforce training, system configurations, and the records that evidence them.
2. The policies and procedures in the filed program were approved by management and were in effect.
3. The safeguards described in the filed program were designed and implemented to meet the HIPAA standards that apply to the organization, and each standard recorded as not applicable carries the reason it does not apply.
4. The answers, records and evidence in the filed program are true and complete to the best of management's knowledge.
5. Management will give the RSP Assessor access to every record and person the assessment requires, and has disclosed, and will disclose until the RSP Assessment Report is issued, any security incident, breach of unsecured protected health information, known deviation from these policies and procedures, or other event that bears on these assertions.
6. Management is responsible for remediating the findings the assessment identifies.

Management understands that the RSP Assessment Report states a professional opinion and is not a certification of HIPAA compliance, which only the U.S. Department of Health and Human Services Office for Civil Rights determines.

I am authorized to make this attestation on the organization's behalf.

Signed electronically, by typed name, when the program was filed

Tomas Berg

Chief Technology Officer

Northfield Community Hospital (HIPAA NIST Actively Managed Demo) · Oct 10, 2026

This attestation is management's own statement, signed before the review began and reproduced here as signed. The RSP Assessor's opinion on the program it describes is in Section I.

Appendix A. Check-by-check review record

Every HIPAA check on the filed path (169), with how it stood when filed, its four elements (Yes: substantiated; Open: not substantiated; n/a: does not apply), and the RSP Assessor's result with a note of what was sampled.

Step 1. Set up your organization

45 C.F.R. 160.103; 164.302; 164.308(a)(1)(ii)(A) (scope) · 6 of 6 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
Regulatory status answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.
Where ePHI lives answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.
Who and where answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.
What you build and rely on answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.
Covered-entity privacy practices answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.
Identity and program answered	Met and substantiated					Verified No dated record backs this check; concluded on the evidence and the interview.

Step 2. Load your workforce

45 C.F.R. 164.308(a)(3), (a)(4) (workforce security and access management) · 3 of 3 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
At least one workforce member is loaded	Met and substantiated					Verified Tested on the records of the period: 13 in the population, the suggested sample drawn at random and agreed to the records.
Every person in scope has a hire date, a position and a supervisor (the org chart)	Met and substantiated					Verified Tested on the records of the period: 13 in the population, the suggested sample drawn at random and agreed to the records.
Everyone who owes onboarding is onboarded: background check, performance review, training and policy acknowledgment	Met and substantiated					Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Step 3. Load your systems and assets

45 C.F.R. 164.308(a)(1)(ii)(A) (scope), 164.310(d) (device and media) · 2 of 2 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
At least one system that holds ePHI is in the inventory	Met and substantiated					Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
Every in-scope system that holds ePHI has an owner and was reviewed in the last 12 months	Met and substantiated					Verified Tested on the records of the period: 12 in the population, the suggested sample drawn at random and agreed to the records.

Step 4. Assess your vendors

45 C.F.R. 164.308(a)(1)(ii)(A) (risk analysis covers vendor systems), 164.308(b) (business associate assurances) · 2 of 2 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
At least one vendor is listed	Met and substantiated					Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
Every vendor has been risk-scored	Met and substantiated					Verified Tested on the records of the period: 30 in the population, the suggested sample drawn at random and agreed to the records.

Step 5. Map access to your systems

45 C.F.R. 164.308(a)(4) (access management), 164.308(a)(3)(ii)(B) (access is appropriate) · 1 of 1 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
At least one person is connected to a system they access	Met and substantiated					Verified Tested on the records of the period: 60 in the population, the suggested sample drawn at random and agreed to the records.

Step 6. Assign roles and responsibilities

45 C.F.R. 164.308(a)(2); 164.530(a) · 3 of 3 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
A Security Official is designated	Met and substantiated					Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
A Privacy Official is designated	Met and substantiated					Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
A privacy complaint contact is named	Met and substantiated					Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.

Step 7. Adopt your policies and procedures

45 C.F.R. 164.316(a)-(b); 164.530(i) · 7 of 7 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
The policy set has been set up from the library	Met and substantiated					Verified Tested on the records of the period: 15 in the population, the suggested sample drawn at random and agreed to the records.
J1 All required policies and procedures reduced to writing 45 C.F.R. 164.316(a)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 15 in the population, the suggested sample drawn at random and agreed to the records.
Every policy has been sent for approval	Met and substantiated					Verified Tested on the records of the period: 15 in the population, the suggested sample drawn at random and agreed to the records.
A4 Sanction policy written and on file 45 C.F.R. 164.308(a)(1)(ii)(C)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
Every policy in the library for your entity type is approved and active	Met and substantiated					Verified Tested on the records of the period: 15 in the population, the suggested sample drawn at random and agreed to the records.
J4 Documentation periodically reviewed and updated for environmental or operational changes 45 C.F.R. 164.316(b)(2)(iii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 15 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
A4-N1 Sanction policy is tiered, proportional to the harm, and communicated to the workforce before it is applied 45 C.F.R. 164.308(a)(1)(ii)(C)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Step 8. Analyze and treat your risks

45 C.F.R. 164.308(a)(1)(ii)(A) (risk analysis), 164.308(a)(1)(ii)(B) (risk management) · 6 of 6 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
At least one risk is in the register	Met and substantiated					Verified Tested on the records of the period: 8 in the population, the suggested sample drawn at random and agreed to the records.
Every open risk has an inherent likelihood and impact	Met and substantiated					Verified Tested on the records of the period: 8 in the population, the suggested sample drawn at random and agreed to the records.
Every open risk has a treatment decision	Met and substantiated					Verified Tested on the records of the period: 8 in the population, the suggested sample drawn at random and agreed to the records.
Every risk treated as mitigate is linked to at least one control	Met and substantiated					Verified Tested on the records of the period: 8 in the population, the suggested sample drawn at random and agreed to the records.
Every open risk is approved	Met and substantiated					Verified Tested on the records of the period: 8 in the population, the suggested sample drawn at random and agreed to the records.
A risk assessment has been completed in the last 12 months	Met and substantiated					Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.

Step 9. Train the workforce

45 C.F.R. 164.308(a)(5); 164.530(b) · 10 of 10 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
B4 Security awareness training delivered to 100% of workforce with ePHI access 45 C.F.R. 164.308(a)(5)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 69 in the population, the suggested sample drawn at random and agreed to the records.
B5 Training refreshed on at least an annual cycle 45 C.F.R. 164.308(a)(5)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 69 in the population, the suggested sample drawn at random and agreed to the records.
B6 Periodic security reminders issued to workforce 45 C.F.R. 164.308(a)(5)(ii)(A)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
B7 Malicious-software protection procedure and workforce guidance 45 C.F.R. 164.308(a)(5)(ii)(B)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
B8 Log-in monitoring and anomaly-reporting procedure 45 C.F.R. 164.308(a)(5)(ii)(C)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
B9 Password management procedure (creation, change, safeguarding) 45 C.F.R. 164.308(a)(5)(ii)(D)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
L8 Every workforce member trained on the privacy policies and procedures relevant to their role: new members within a reasonable period after joining, all affected members after a material change, with completion documented 45 C.F.R. 164.530(b)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 69 in the population, the suggested sample drawn at random and agreed to the records.
B4-N1 A training needs assessment identifies what each role must learn 45 C.F.R. 164.308(a)(5)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
B4-N2 An approved training strategy and plan sets audiences, topics, cadence and delivery, including contractors and business associates 45 C.F.R. 164.308(a)(5)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
B5-N1 Training effectiveness is measured and the plan is updated from the results 45 C.F.R. 164.308(a)(5)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Step 10. Put the agreements in place

45 C.F.R. 164.308(b); 164.502(e); 164.504(e) · 6 of 6 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
Every vendor that touches PHI is listed	Met and substantiated					Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
H6 Every vendor that creates, receives, maintains, or transmits PHI on the organization's behalf is identified as a business associate and recorded in the BAA tracker before any PHI is shared 45 C.F.R. 160.103; 164.502(e)(1)	Met and substantiated	n/a	n/a	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
H7 Signed Business Associate Agreement containing every required element on file with each business associate before PHI is disclosed to it, documenting the satisfactory assurances the Privacy Rule requires 45 C.F.R. 164.502(e); 164.504(e)(2)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
H8 Due diligence on a business associate's safeguards performed before contracting and repeated on a periodic cycle for those that hold or process ePHI supports 164.308(a)(1) scope; 164.308(b)	Met and substantiated	n/a	n/a	n/a	Yes	Verified Tested on the records of the period: 30 in the population, the suggested sample drawn at random and agreed to the records.
H9 A known material violation of a BAA by a business associate is cured or the arrangement terminated where feasible, and the steps taken are documented 45 C.F.R. 164.504(e)(1)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
K1 Cybersecurity supply chain risk management extends beyond BAA-centric due diligence to supplier concentration risk, fourth-party (N-tier) visibility, and component/software provenance 45 C.F.R. 164.308(b); 164.314(a)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.

Step 11. Implement and evidence the safeguards

45 C.F.R. 164.308(a)(3)-(4), (a)(7); 164.310; 164.312 · 60 of 60 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
B1 Authorization and/or supervision procedure for workforce with ePHI access 45 C.F.R. 164.308(a)(3)(ii)(A)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
B2 Workforce clearance (background screening) procedure 45 C.F.R. 164.308(a)(3)(ii)(B)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
B3 Termination procedure that revokes system access on the effective date 45 C.F.R. 164.308(a)(3)(ii)(C)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
C1 Unique user ID assigned to every person accessing ePHI systems 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
C2 Emergency access procedure documented and tested 45 C.F.R. 164.312(a)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
C3 Health care clearinghouse functions isolated from larger organization systems (if applicable) 45 C.F.R. 164.308(a)(4)(ii)(A)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
C4 Access authorization decisions documented per role, tied to job function 45 C.F.R. 164.308(a)(4)(ii)(B)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
C5 Access establishment and modification procedure 45 C.F.R. 164.308(a)(4)(ii)(C)	Met and substantiated	Yes	n/a	n/a	Yes	Finding Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
C6 Periodic access review performed on active accounts, not only at onboarding 45 C.F.R. 164.308(a)(4)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 282 in the population, the suggested sample drawn at random and agreed to the records.
C7 Automatic session logoff configured on workstations and applications 45 C.F.R. 164.312(a)(2)(iii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
E1 Data backup plan 45 C.F.R. 164.308(a)(7)(ii)(A)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 30 in the population, the suggested sample drawn at random and agreed to the records.
E2 Disaster recovery plan 45 C.F.R. 164.308(a)(7)(ii)(B)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
E3 Emergency mode operation plan 45 C.F.R. 164.308(a)(7)(ii)(C)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
E4 Contingency plans tested in the past 12 months with documented results 45 C.F.R. 164.308(a)(7)(ii)(D)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
E5 Applications and data criticality analysis 45 C.F.R. 164.308(a)(7)(ii)(E)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
F1 Facility security plan for any location housing ePHI systems 45 C.F.R. 164.310(a)(2)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
F2 Facility access control and validation procedures 45 C.F.R. 164.310(a)(2)(iii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F3 Contingency operations procedure for facility access during an emergency 45 C.F.R. 164.310(a)(2)(i)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
F4 Maintenance record log for physical security repairs and modifications 45 C.F.R. 164.310(a)(2)(iv)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F5 Written workstation-use policy defining permitted functions and environment 45 C.F.R. 164.310(b)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
F6 Physical workstation security controls in place (siting, screen privacy, locking) 45 C.F.R. 164.310(c)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
F7 Device and media disposal procedure 45 C.F.R. 164.310(d)(2)(i)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
F8 Device and media re-use (sanitization) procedure 45 C.F.R. 164.310(d)(2)(ii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F9 Media movement accountability log 45 C.F.R. 164.310(d)(2)(iii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F10 Data backup and storage procedure prior to equipment relocation 45 C.F.R. 164.310(d)(2)(iv)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G1 Unique user identification enforced at the system level 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
G2 Emergency access procedure implemented technically 45 C.F.R. 164.312(a)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G3 Automatic logoff enforced by configuration 45 C.F.R. 164.312(a)(2)(iii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G4 Encryption of ePHI at rest, or documented compensating rationale 45 C.F.R. 164.312(a)(2)(iv)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
G5 Audit control mechanisms recording and examining system activity 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
G6 Mechanism to authenticate ePHI has not been improperly altered or destroyed 45 C.F.R. 164.312(c)(2)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G7 Person-or-entity authentication (credential verification; multifactor is the accepted 2026 standard for remote and privileged access) 45 C.F.R. 164.312(d)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
G8 Transmission integrity controls for ePHI in transit 45 C.F.R. 164.312(e)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G9 Encryption of ePHI in transit, or documented compensating rationale 45 C.F.R. 164.312(e)(2)(ii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
B1-N1 Job descriptions define the security responsibilities of every role that touches ePHI 45 C.F.R. 164.308(a)(3)(ii)(A)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
B2-N1 Documented criteria and procedures govern hiring and assigning tasks to roles with ePHI access 45 C.F.R. 164.308(a)(3)(ii)(B)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
E1-N1 At least one backup copy is kept offline or immutable, and backup logs are reviewed 45 C.F.R. 164.308(a)(7)(ii)(A)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 19 in the population, the suggested sample drawn at random and agreed to the records.
E2-N1 The recovery strategy documents the order and the time targets for restoring systems and data 45 C.F.R. 164.308(a)(7)(ii)(B)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
E4-N1 Contingency testing includes an actual restore of ePHI from backup, with the results recorded 45 C.F.R. 164.308(a)(7)(ii)(D)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
E5-N1 Preventive measures are identified to reduce the likelihood and impact of disruptions 45 C.F.R. 164.308(a)(7)(ii)(E)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
F1-N1 Physical security vulnerabilities are analyzed, with an inventory of every facility access point 45 C.F.R. 164.310(a)(2)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F1-N2 Corrective measures for facility vulnerabilities are tracked to completion 45 C.F.R. 164.310(a)(2)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F5-N1 Workstations and devices, including mobile, IoT and medical devices, are inventoried and classified by permitted function 45 C.F.R. 164.310(b)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F5-N2 Expected performance and permitted uses are defined for each type of workstation and device 45 C.F.R. 164.310(b)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F5-N3 The physical surroundings of workstations are analyzed for unauthorized viewing and access 45 C.F.R. 164.310(b)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F6-N1 Every method of physical access to workstations and devices is identified and its risk analyzed 45 C.F.R. 164.310(c)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F6-N2 Device encryption, screen locks, multi-factor sign-in and mobile device management are applied to workstations and devices 45 C.F.R. 164.310(c)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F7-N1 Media are sanitized to NIST SP 800-88 before disposal, with the method recorded 45 C.F.R. 164.310(d)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
F9-N1 A named custodian records the receipt and removal of hardware and media, including media that leave the facility 45 C.F.R. 164.310(d)(2)(iii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G1-N1 Technical access control capabilities are identified for each ePHI system, including network segmentation 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
G1-N2 Access control procedures are implemented in the selected hardware and software for each ePHI system 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G5-N1 The audit scope is set from the risk analysis, with defined record content: user, event, date and time 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G5-N2 Audit and activity review tools are selected and deployed 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G6-N1 Sources that could alter or destroy ePHI without authorization are identified 45 C.F.R. 164.312(c)(2)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G6-N2 Integrity mechanisms are monitored, with a response process when alteration is detected 45 C.F.R. 164.312(c)(2)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G7-N1 Where authentication applies is documented for every system and application holding ePHI 45 C.F.R. 164.312(d)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G7-N2 Authentication options (something known, held, or biometric) are evaluated for each system 45 C.F.R. 164.312(d)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G7-N3 Multi-factor authentication is enforced for remote and privileged access 45 C.F.R. 164.312(d)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G8-N1 Every path ePHI travels (email, file transfer, portals, apps) is inventoried with who could intercept it 45 C.F.R. 164.312(e)(2)(i)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G9-N1 Encryption in transit uses algorithms of sufficient strength, configured so they cannot silently downgrade 45 C.F.R. 164.312(e)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Step 12. Operate the program

45 C.F.R. 164.308(a)(1)(ii)(D), (a)(6); 164.400-414; 164.520-530 · 63 of 63 met as filed

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
A5 Sanction policy applied at least once when warranted, or documented that no violation has occurred 45 C.F.R. 164.308(a)(1)(ii)(C)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
A6 Information system activity review (log and report review) performed on a defined cadence 45 C.F.R. 164.308(a)(1)(ii)(D)	Met and substantiated	Yes	n/a	n/a	Yes	Finding Tested on the records of the period: 12 in the population, the suggested sample drawn at random and agreed to the records.
D1 Written security incident response plan 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
D2 Incident log maintained with root cause and disposition for each entry 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
D3 Breach risk-assessment procedure applying the four-factor test 45 C.F.R. 164.402	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
D6 Law-enforcement delay provision understood and documented 45 C.F.R. 164.412	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
D7 Breach notification sent to each affected individual without unreasonable delay and no later than 60 calendar days after discovery, with the required content, by first-class mail or agreed e-mail, and by substitute notice where contact information is out of date 45 C.F.R. 164.404	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
D8 Notice to the Secretary of HHS made contemporaneously with individual notice for a breach of 500 or more people, or by annual submission within 60 days after year end for smaller breaches, and notice to prominent media when more than 500 residents of one State are affected 45 C.F.R. 164.406; 164.408	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 1 in the population, the suggested sample drawn at random and agreed to the records.
D9 Every business associate is contractually required to report security incidents and breaches within a set window, and reports received are logged and handled under this procedure 45 C.F.R. 164.410; 164.504(e)(2)(ii)(C)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
I1 Minimum-necessary standard applied to routine PHI use and disclosure 45 C.F.R. 164.502(b)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
I5 Uses and disclosures of PHI limited to treatment, payment, and health care operations, those made with an opportunity to agree or object, the public-interest categories the rule lists, and those made under a valid authorization, with the workforce trained on which is which 45 C.F.R. 164.502(a); 164.506; 164.510; 164.512	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
I6 Identity and authority of a requester verified before any disclosure, including personal representatives and public officials, and the verification documented 45 C.F.R. 164.514(h); 164.502(g)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
I7 Reasonable safeguards in place to limit incidental uses and disclosures of PHI in every form: oral, paper, and electronic 45 C.F.R. 164.530(c)(2); 164.502(a)(1)(iii)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
I8 No sale of PHI, and no marketing or fundraising communications, without the authorization or opt-out the Privacy Rule requires 45 C.F.R. 164.502(a)(5)(ii); 164.508(a)(3)-(4); 164.514(f)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
J2 All actions, activities, and assessments the rule requires to be documented, are in fact documented 45 C.F.R. 164.316(b)(1)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
J3 Documentation retained six years from creation date or last-effective date, whichever is later 45 C.F.R. 164.316(b)(2)(i)	Met and substantiated	n/a	n/a	n/a	n/a	Verified No dated record backs this check; concluded on the evidence and the interview.
L1 Notice of Privacy Practices developed, provided at first service delivery (or as otherwise required), and posted; good-faith effort made to obtain written acknowledgment of receipt for a direct treatment relationship 45 C.F.R. 164.520	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L2 Minimum-necessary standard applied as the covered entity's own comprehensive policy governing routine and non-routine PHI uses, disclosures, and requests -- broader than the narrow business-associate duty in Domain I 45 C.F.R. 164.502(b); 164.514(d)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L3 Written, HIPAA-compliant authorization obtained before any use or disclosure of PHI not otherwise permitted for treatment, payment, health care operations, or another Privacy Rule exception 45 C.F.R. 164.508	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
L4 Process to receive, verify the requester's identity for, and respond to an individual's request to access, inspect, or obtain a copy of their PHI within the required timeframe 45 C.F.R. 164.524	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L5 Process to receive and act on an individual's request to amend their PHI, including a timely acceptance or denial and the required documentation 45 C.F.R. 164.526	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L6 Process to track disclosures of PHI and produce an accounting of disclosures on an individual's request 45 C.F.R. 164.528	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L9 Complaint process available to individuals and described in the Notice; complaints and their disposition documented; no intimidation, retaliation, or waiver of rights as a condition of treatment, payment, enrollment, or eligibility 45 C.F.R. 164.530(d); 164.530(g); 164.530(h)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L10 Requests to restrict uses or disclosures considered and documented, the restriction on disclosure to a health plan for a service paid in full out of pocket always granted, and reasonable requests for confidential communications accommodated 45 C.F.R. 164.522	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
L11 Harmful effects of a known use or disclosure in violation of policy or the Privacy Rule mitigated to the extent practicable, and privacy documentation retained for six years 45 C.F.R. 164.530(f); 164.530(j)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 0 in the population, the suggested sample drawn at random and agreed to the records.
A6-N1 Information system activity review names the reviewer, the frequency, and where the logs are kept, including any cloud service 45 C.F.R. 164.308(a)(1)(ii)(D)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
D1-N1 The incident response capability has documented goals and scope 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
D1-N2 An incident response team, or the alternative structure the organization chose, is named with its roles 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
D1-N3 The incident response plan is tested by an exercise at least annually, with results recorded 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	Yes	n/a	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
D2-N1 Post-incident analysis feeds documented updates to the incident response plan 45 C.F.R. 164.308(a)(6)(ii)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
A6 Information system activity review (log and report review) performed on a defined cadence 45 C.F.R. 164.308(a)(1)(ii)(D)	Met and substantiated	Yes	n/a	n/a	Yes	Finding Tested on the records of the period: 12 in the population, the suggested sample drawn at random and agreed to the records.
A6-N1 Information system activity review names the reviewer, the frequency, and where the logs are kept, including any cloud service 45 C.F.R. 164.308(a)(1)(ii)(D)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
B7 Malicious-software protection procedure and workforce guidance 45 C.F.R. 164.308(a)(5)(ii)(B)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
B8 Log-in monitoring and anomaly-reporting procedure 45 C.F.R. 164.308(a)(5)(ii)(C)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
B9 Password management procedure (creation, change, safeguarding) 45 C.F.R. 164.308(a)(5)(ii)(D)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
C1 Unique user ID assigned to every person accessing ePHI systems 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
C2 Emergency access procedure documented and tested 45 C.F.R. 164.312(a)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
C6 Periodic access review performed on active accounts, not only at onboarding 45 C.F.R. 164.308(a)(4)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 282 in the population, the suggested sample drawn at random and agreed to the records.
C7 Automatic session logoff configured on workstations and applications 45 C.F.R. 164.312(a)(2)(iii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
E1 Data backup plan 45 C.F.R. 164.308(a)(7)(ii)(A)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 30 in the population, the suggested sample drawn at random and agreed to the records.
E4 Contingency plans tested in the past 12 months with documented results 45 C.F.R. 164.308(a)(7)(ii)(D)	Met and substantiated	Yes	n/a	n/a	Yes	Verified Tested on the records of the period: 6 in the population, the suggested sample drawn at random and agreed to the records.
E1-N1 At least one backup copy is kept offline or immutable, and backup logs are reviewed 45 C.F.R. 164.308(a)(7)(ii)(A)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 19 in the population, the suggested sample drawn at random and agreed to the records.
F6 Physical workstation security controls in place (siting, screen privacy, locking) 45 C.F.R. 164.310(c)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
F8 Device and media re-use (sanitization) procedure 45 C.F.R. 164.310(d)(2)(ii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F9 Media movement accountability log 45 C.F.R. 164.310(d)(2)(iii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F10 Data backup and storage procedure prior to equipment relocation 45 C.F.R. 164.310(d)(2)(iv)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F6-N2 Device encryption, screen locks, multi-factor sign-in and mobile device management are applied to workstations and devices 45 C.F.R. 164.310(c)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
F7-N1 Media are sanitized to NIST SP 800-88 before disposal, with the method recorded 45 C.F.R. 164.310(d)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G1 Unique user identification enforced at the system level 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
G2 Emergency access procedure implemented technically 45 C.F.R. 164.312(a)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G3 Automatic logoff enforced by configuration 45 C.F.R. 164.312(a)(2)(iii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G5 Audit control mechanisms recording and examining system activity 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G6 Mechanism to authenticate ePHI has not been improperly altered or destroyed 45 C.F.R. 164.312(c)(2)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G7 Person-or-entity authentication (credential verification; multifactor is the accepted 2026 standard for remote and privileged access) 45 C.F.R. 164.312(d)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 5 in the population, the suggested sample drawn at random and agreed to the records.
G8 Transmission integrity controls for ePHI in transit 45 C.F.R. 164.312(e)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G9 Encryption of ePHI in transit, or documented compensating rationale 45 C.F.R. 164.312(e)(2)(ii)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G1-N1 Technical access control capabilities are identified for each ePHI system, including network segmentation 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G1-N2 Access control procedures are implemented in the selected hardware and software for each ePHI system 45 C.F.R. 164.312(a)(2)(i)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G5-N1 The audit scope is set from the risk analysis, with defined record content: user, event, date and time 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.

Check	As filed	Pol.	Trn.	Cfg.	Evd.	Review result
G5-N2 Audit and activity review tools are selected and deployed 45 C.F.R. 164.312(b)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G6-N2 Integrity mechanisms are monitored, with a response process when alteration is detected 45 C.F.R. 164.312(c)(2)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 3 in the population, the suggested sample drawn at random and agreed to the records.
G7-N3 Multi-factor authentication is enforced for remote and privileged access 45 C.F.R. 164.312(d)	Met and substantiated	Yes	Yes	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.
G9-N1 Encryption in transit uses algorithms of sufficient strength, configured so they cannot silently downgrade 45 C.F.R. 164.312(e)(2)(ii)	Met and substantiated	Yes	n/a	Yes	Yes	Verified Tested on the records of the period: 2 in the population, the suggested sample drawn at random and agreed to the records.