HIPAA COMPLIANCE & SECURITY READINESS ASSESSMENT

2026 Sample Report · Illustrative Sample Deliverable

NovaCura Health & Pharmaceuticals, Inc.

Fictional Demonstration Organization · Healthcare / Pharmaceuticals / Specialty Pharmacy

CONFIDENTIAL — SAMPLE / DEMONSTRATION

FICTIONAL REPORT — NOT AN ACTUAL HIPAA ASSESSMENT

This document is a simulated HIPAA Compliance & Security Readiness Assessment created by TMG Security to demonstrate report structure, methodology, evidence handling, findings, and professional reporting standards. NovaCura Health & Pharmaceuticals, Inc. is fictional. No actual HIPAA assessment, OCR audit, certification, attestation, or compliance determination was performed or issued.

Assessment Period	01 Jan 2026 – 31 Aug 2026	**Report Date**	15 September 2026
Report Version	1.0	**Classification**	**Confidential**
Service Provider	TMG Security	**Assessment Type**	Illustrative Readiness Assessment

CONFIDENTIALITY NOTICE

This document, including all findings and illustrative data herein, is provided by TMG Security strictly as a demonstration sample. Distribution outside its intended demonstration purpose without written consent is discouraged. This report does not constitute, and must not be represented as, an actual HIPAA compliance determination, OCR audit outcome, certification, or attestation of any kind. HIPAA does not provide for a formal government "certification."

DOCUMENT CONTROL

Document Owner	TMG Security — Governance, Risk & Compliance (GRC) Practice
Prepared By	TMG Security Assessment Team
Reviewed By	TMG Security Quality Assurance Lead
Version	1.0
Issue Date	15 September 2026
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION
Assessment Type	Fictional HIPAA Compliance & Security Readiness Assessment
Assessment Period	01 January 2026 – 31 August 2026
Client	NovaCura Health & Pharmaceuticals, Inc. (Fictional Entity)
Service Provider	TMG Security

Document Change History

Version	Date	Description	Author
1.0	15 Sep 2026	Initial issue of sample report	TMG Security Assessment Team

Distribution List

Name / Role	Organization	Purpose
Chief Executive Officer (Fictional)	NovaCura Health & Pharmaceuticals, Inc.	Primary recipient
Chief Information Security Officer (Fictional)	NovaCura Health & Pharmaceuticals, Inc.	Primary recipient
Privacy Officer (Fictional)	NovaCura Health & Pharmaceuticals, Inc.	Privacy program oversight
Engagement Lead	TMG Security	Quality assurance / archival

IMPORTANT NOTICE

FICTIONAL SAMPLE REPORT — DEMONSTRATION PURPOSES ONLY

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, depth, and professional standard of a HIPAA compliance and security readiness assessment deliverable. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- NovaCura Health & Pharmaceuticals, Inc. is a fictional entity. It does not correspond to any real company, and any resemblance to an actual organization is purely coincidental.
- No actual HIPAA assessment, gap analysis, or readiness review was performed against any real environment, system, or organization.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report; no real PHI or ePHI was accessed at any point.
- No certification, attestation, or compliance determination has been issued to any party as a result of this document. HIPAA itself does not provide for a formal government-issued "certification" of compliance.
- This report does not represent, reference, or substitute for an actual OCR investigation, audit, or enforcement action.
- All findings, risk ratings, evidence references, control statuses, illustrative dates, and management responses contained in this report are illustrative and fictional. They were constructed to demonstrate realistic reporting conventions and do not describe any actual security or compliance condition.
- The fictional incident scenario referenced in Section 15 (Breach Notification Review) is provided solely to demonstrate TMG Security's breach risk assessment methodology. No actual breach, security incident, or unauthorized PHI disclosure occurred.
- TMG Security is not representing, and this document must not be interpreted as representing, that TMG Security performed an actual HIPAA audit or acted in any official OCR-recognized capacity.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's assessment methodology, documentation standards, and reporting quality. It should not be relied upon for any compliance, legal, contractual, or risk decision. Actual HIPAA compliance depends on an organization's specific facts, scope, legal obligations, risk analysis, and implemented safeguards, and should be evaluated with qualified legal and compliance counsel.

2026 Regulatory Position — Critical Note

This report is built against the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule currently in effect as of 2026. In December 2024, HHS/OCR published a Notice of Proposed Rulemaking (NPRM) proposing significant modifications to the HIPAA Security Rule. As of this report's date, that NPRM has not been finalized and does not constitute a current legal requirement. This report does not treat any provision of the 2024 NPRM as a mandatory current requirement; proposed provisions are discussed separately in Section 34 (Regulatory Watch — 2026) for awareness and future-readiness purposes only and are not scored as part of the current-state assessment in Sections 11 through 33.

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

TMG Security has prepared this fictional, illustrative HIPAA Compliance & Security Readiness Assessment sample to represent NovaCura Health & Pharmaceuticals, Inc., a hypothetical U.S.-based specialty pharmacy and patient-support organization. This section presents a fictional executive-level summary of the simulated assessment results, prepared in the style and format TMG Security would use for an actual engagement.

ALL METRICS, FINDINGS, AND SCORES ON THIS PAGE ARE FICTIONAL SAMPLE DATA

Overall Illustrative Assessment Status

PARTIALLY IN PLACE

NovaCura's simulated environment demonstrates a reasonable baseline HIPAA Security and Privacy Rule program, with a defined set of fictional gaps requiring remediation. This illustrative status reflects a sample readiness assessment and does not represent an official HIPAA compliance determination, OCR audit outcome, or certification.

Fictional Sample Findings Dashboard

19	1	4	6	4	4
Total Findings	Critical	High	Medium	Low	Observations

Executive Risk Narrative

The fictional assessment identified one critical-severity sample finding concerning the completeness of NovaCura's enterprise-wide ePHI risk analysis (Section 17), which underpins the organization's broader Security Rule program. Four high-severity findings span privileged access review evidence, information system activity review documentation, portable-device encryption coverage, and business associate security review currency. Medium-severity findings reflect gaps in incident response exercise cadence, backup restoration testing, workforce training completion tracking, minimum-necessary access design in the patient-support CRM, breach risk assessment documentation, and vulnerability remediation exception tracking. Low-severity findings and observations reflect narrower process, documentation, and configuration-consistency gaps across physical safeguards, audit log review cadence, session timeout configuration, and policy governance.

Across these fictional results, NovaCura's simulated program shows particular strength in its documented policy suite, Notice of Privacy Practices, business associate contracting, and breach notification workflow design, alongside developing maturity in enterprise risk analysis completeness, identity and access governance, ePHI audit logging consistency, third-party oversight, incident response exercising, encryption coverage on legacy devices, backup/recovery validation, workforce security awareness tracking, and privacy governance around minimum necessary access. TMG Security's simulated recommendation is that NovaCura prioritize closure of the critical-severity risk analysis finding and the four high-severity findings within the first 60 days of the fictional remediation roadmap (see Section 28), with remaining items addressed across a 90-day window.

This summary, and every figure, finding, and status on this page and throughout this report, is entirely fictional and constructed for demonstration purposes only. It does not describe the security or compliance posture of any real organization, and does not constitute a HIPAA certification, OCR audit outcome, or legal compliance determination.

02 ASSESSMENT OVERVIEW

This fictional sample report presents the results of a simulated HIPAA Compliance & Security Readiness Assessment performed by TMG Security on behalf of NovaCura Health & Pharmaceuticals, Inc. The assessment is designed to illustrate how TMG Security evaluates an organization's administrative, physical, and technical safeguards against the HIPAA Security Rule, alongside applicable Privacy Rule and Breach Notification Rule obligations, and how TMG Security documents and reports the results of that evaluation.

Engagement Summary

Assessment Type	HIPAA Compliance & Security Readiness Assessment (Illustrative)
Assessment Period	01 January 2026 – 31 August 2026 (Fictional)
Client	NovaCura Health & Pharmaceuticals, Inc. (Fictional Entity)
Service Provider	TMG Security
Regulatory Scope	HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule, applicable HITECH-related obligations, Business Associate oversight
Overall Illustrative Status	Partially In Place

Purpose of This Report

This report is intended to give NovaCura's leadership a structured, evidence-referenced view of the organization's fictional HIPAA compliance and security posture at a point in time, including illustrative control gaps, associated risk, and a prioritized remediation path. Consistent with TMG Security's actual engagement deliverables, the report combines an administrative and technical safeguards review, a Privacy Rule and Breach Notification Rule review, business associate oversight review, and a formal risk analysis into a single consulting-format deliverable.

How to Read This Report

- Sections 1–10 establish context: organization profile, objectives, scope, the regulatory framework applied, methodology, the ePHI data flow, and security governance structure.
- Sections 11–24 present the detailed control-area review, organized around the HIPAA Security Rule's Administrative, Physical, and Technical Safeguards, followed by Privacy Rule, Breach Notification, Business Associate, Risk Analysis, and supporting operational domains.
- Sections 25–30 consolidate findings into a Findings Summary, Detailed Findings, Risk Heatmap, 90-Day Remediation Roadmap, Management Action Plan, and Final Assessment & Conclusion.
- Sections 31–37 provide the supporting appendix: Evidence Register, Finding Register, HIPAA Control Matrix, the 2026 Regulatory Watch section, Assessment Limitations, Glossary, and Contact & Disclaimer.

03 ORGANIZATION PROFILE

Organization	NovaCura Health & Pharmaceuticals, Inc. (Fictional)
Industry	Healthcare / Pharmaceuticals / Specialty Pharmacy / Patient Support Services
Headquarters	Boston, Massachusetts, USA
Employees	Approximately 1,250
Regulatory Status	Treated as a HIPAA-regulated entity for purposes of this fictional demonstration

Business Description (Fictional)

NovaCura Health & Pharmaceuticals, Inc. is presented as a U.S.-based healthcare and pharmaceutical organization operating specialty pharmacy services, patient-support programs, clinical coordination services, prescription fulfillment operations, and digital patient engagement platforms. This narrative is illustrative and constructed solely to give context to the sample findings that follow.

ePHI Footprint (Fictional)

In this fictional scenario, NovaCura creates, receives, maintains, and transmits ePHI through electronic health and patient-support systems, specialty pharmacy systems, patient portals, clinical applications, CRM systems containing patient information, cloud platforms, email, file-transfer services, mobile applications, third-party business associates, and laboratory and healthcare-provider integrations. The organization's simulated environment is treated as a covered entity under HIPAA for purposes of this demonstration.

Major Strengths (Fictional)

- Documented HIPAA Security and Privacy policy suite, including a current Notice of Privacy Practices.
- Centralized identity provider with MFA enforced on primary remote-access and administrative paths.
- Executed Business Associate Agreements in place for all sampled third-party relationships.
- Defined incident response plan with assigned roles across security, legal, privacy, and communications functions.

Major Gaps (Fictional)

- Enterprise-wide ePHI risk analysis not yet updated to reflect all current in-scope systems (see HIPAA-RSK-001).
- Privileged access recertification and information system activity review evidence incomplete for select systems.
- Business associate security due-diligence review overdue for two sampled third parties.

Immediate Priorities (Fictional)

- Update the enterprise-wide ePHI risk analysis to reflect NovaCura's full current technology footprint.
- Close the four high-severity findings related to access governance, activity review, encryption coverage, and business associate oversight.
- Complete the outstanding incident response tabletop exercise and backup restoration test cycles.

04 ASSESSMENT OBJECTIVES

This fictional assessment was designed to evaluate NovaCura's HIPAA compliance and security posture against five core objectives, consistent with the structure TMG Security applies to an actual HIPAA readiness engagement.

- Evaluate the design and operating effectiveness of NovaCura's Administrative, Physical, and Technical Safeguards under the HIPAA Security Rule.
- Assess NovaCura's HIPAA Privacy Rule program, including minimum necessary application, individual rights processes, and workforce privacy practices.
- Evaluate NovaCura's Breach Notification Rule readiness, including breach risk assessment and notification workflow design.
- Review NovaCura's oversight of business associates that create, receive, maintain, or transmit ePHI on its behalf.
- Assess the maturity and completeness of NovaCura's enterprise-wide ePHI risk analysis and risk management program.

Scope & Boundaries

The table below presents the fictional scope boundary defined for this sample assessment. Scope determinations shown are illustrative and follow the general structure TMG Security uses to document engagement boundaries during an actual HIPAA engagement.

Component	Description	Scope Determination
Patient Portal & Specialty Pharmacy Systems	Customer-facing prescription management, refill, and patient-support functions.	IN SCOPE
Clinical Coordination Application	Care-team coordination and clinical documentation functions.	IN SCOPE
CRM / Patient Support Platform	Case management and patient-support interaction records.	IN SCOPE
Cloud Infrastructure & Analytics Environment	Illustrative cloud compute, storage, and adherence-reporting analytics.	IN SCOPE

Component	Description	Scope Determination
Business Associates (6 sampled)	Cloud hosting, claims processing, patient communications, lab integration, MSSP, document destruction.	IN SCOPE — THIRD PARTY
Administrative / Privileged Access	Privileged access paths to in-scope ePHI systems.	IN SCOPE
Logging & Monitoring Infrastructure	Centralized SIEM and audit logging supporting in-scope systems.	IN SCOPE
Corporate HR / Payroll Systems	Human resources platforms with no ePHI content or connectivity.	OUT OF SCOPE
Manufacturing / Supply Chain Systems	Pharmaceutical manufacturing systems with no direct ePHI handling.	OUT OF SCOPE

06 REGULATORY & CONTROL FRAMEWORK

This assessment is structured around the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule as currently in effect as of 2026, codified at 45 CFR Parts 160 and 164. The table below summarizes the framework components applied throughout this report.

Framework Component	Citation	Coverage in This Report
Administrative Safeguards	45 CFR §164.308	Section 11 — Security Management, Workforce Security, Access Management, Training, Incident Procedures, Contingency Plan, Evaluation, BAA.
Physical Safeguards	45 CFR §164.310	Section 12 — Facility Access Controls, Workstation Use & Security, Device and Media Controls.
Technical Safeguards	45 CFR §164.312	Section 13 — Access Control, Audit Controls, Integrity, Authentication, Transmission Security.
Organizational Requirements	45 CFR §164.314	Section 16 — Business Associate Contracts and other organizational requirements.
Policies, Procedures & Documentation	45 CFR §164.316	Sections 11–24 — Documentation practices are assessed alongside each corresponding control area.
Privacy Rule	45 CFR Part 164, Subpart E	Section 14 — Uses/disclosures, minimum necessary, individual rights, Notice of Privacy Practices, workforce privacy training.
Breach Notification Rule	45 CFR Part 164, Subpart D	Section 15 — Breach identification, risk assessment, notification workflow.
Business Associate Oversight	45 CFR §§164.308(b), 164.314(a)	Section 16 — Business Associate Agreement execution and security due diligence.
Proposed Security Rule Modernization (Regulatory Watch)	2024 NPRM (Not Yet Final)	Section 34 — Presented separately; not scored as a current mandatory requirement.

This report evaluates NovaCura against the current, legally effective HIPAA Security Rule, Privacy Rule, and Breach Notification Rule. The December 2024 HIPAA Security Rule Notice of Proposed Rulemaking (NPRM) is not treated as an effective or final requirement anywhere in Sections 11 through 33 of this report; proposed provisions are addressed separately and clearly labeled in Section 34.

07 HIPAA APPLICABILITY

This section presents TMG Security's fictional applicability determination for NovaCura, explaining why the organization is treated as subject to HIPAA for purposes of this sample assessment.

Covered Entity / Business Associate Determination (Fictional)

NovaCura Health & Pharmaceuticals, Inc. is treated in this fictional scenario as a HIPAA-regulated entity: it operates specialty pharmacy and patient-support functions that create, receive, maintain, and transmit ePHI on behalf of patients and, in select service lines, on behalf of healthcare provider and payer business partners. Where NovaCura performs functions on behalf of another covered entity, it may additionally be treated as a business associate with respect to that relationship; both roles are addressed within this assessment's scope.

Data Types in Scope

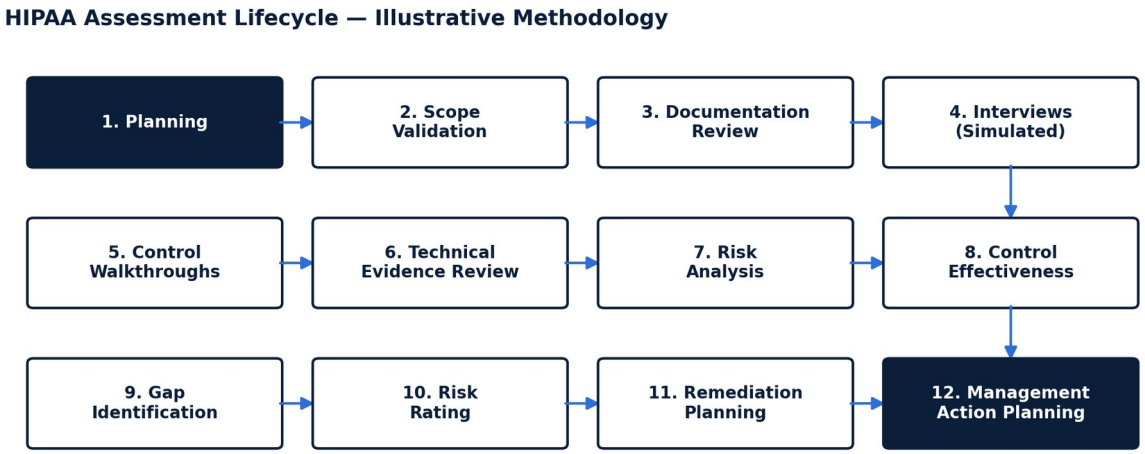
- Protected Health Information (PHI) and electronic Protected Health Information (ePHI), including patient identifiers, prescription and clinical data, and patient-support case records.
- De-identified and aggregate data derived from ePHI, to the extent it retains identifiability risk relevant to this assessment's scope.
- Business associate-transmitted data containing PHI, including laboratory results, claims data, and patient communications.

Applicable HIPAA Rules

HIPAA Privacy Rule	Governs permitted uses and disclosures of PHI, minimum necessary, individual rights, and required notices.
HIPAA Security Rule	Governs administrative, physical, and technical safeguards protecting the confidentiality, integrity, and availability of ePHI.
HIPAA Breach Notification Rule	Governs identification, risk assessment, and notification obligations following an impermissible use or disclosure of PHI.
Applicable HITECH-Related Obligations	Extends certain HIPAA obligations directly to business associates and strengthens breach notification and enforcement provisions.

08 ASSESSMENT METHODOLOGY

TMG Security applies a structured, repeatable twelve-stage methodology across every HIPAA engagement, illustrated here in a fictional context. Because this is a demonstration report, every interview, evidence review, and technical validation step referenced throughout this document is simulated: no actual NovaCura personnel were interviewed, no actual NovaCura systems were accessed, and no actual evidence was collected or reviewed.



HIPAA Assessment Lifecycle — Illustrative Methodology

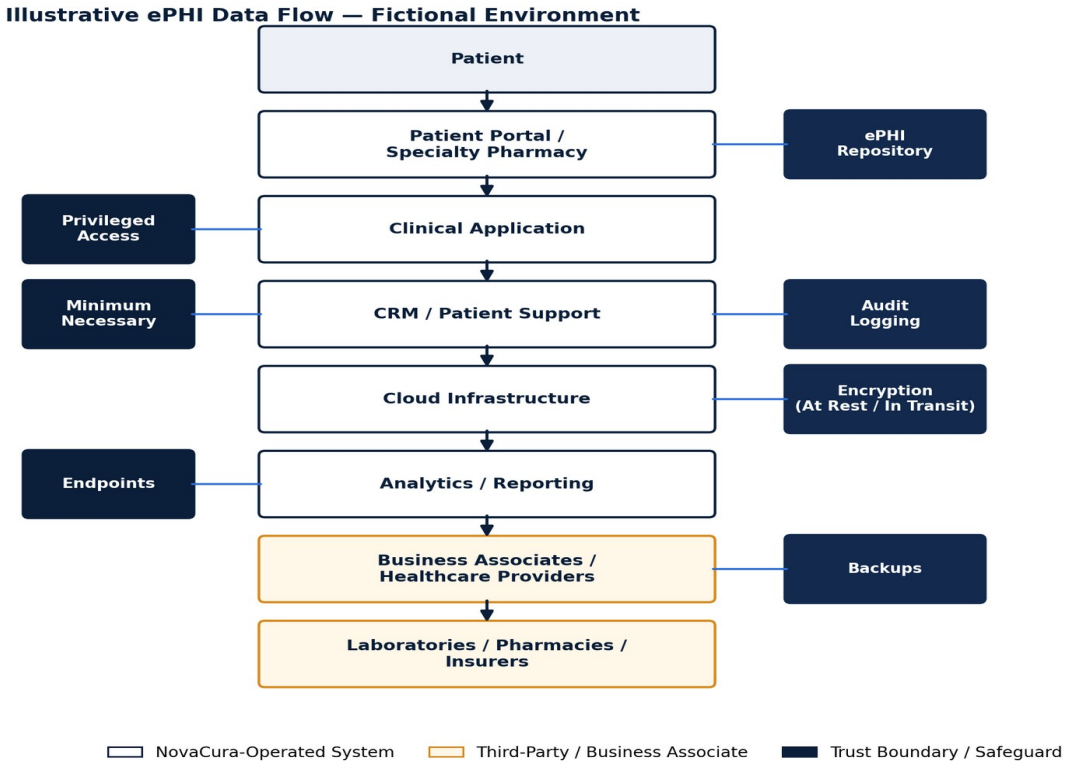
Methodology Stages

1. Planning	Define engagement objectives, regulatory scope, and assessment timeline with NovaCura stakeholders.
2. Scope Validation	Confirm the boundary of in-scope systems, business associates, and ePHI data flows.
3. Documentation Review	Review policies, standards, risk analyses, and prior assessment or audit records.
4. Interviews / Simulated Interviews	Interview (in this fictional scenario, simulate interviews with) control owners across IT, security, privacy, and clinical operations.
5. Control Walkthroughs	Observe and walk through key administrative, physical, and technical safeguard controls.
6. Technical Evidence Review	Evaluate configuration exports, access records, and technical artifacts supporting each control.
7. Risk Analysis	Assess threats, vulnerabilities, likelihood, and impact across the ePHI environment.

8. Control Effectiveness Assessment	Evaluate whether each safeguard is designed and operating as intended.
9. Gap Identification	Identify and document control gaps relative to the current HIPAA Privacy, Security, and Breach Notification Rules.
10. Risk Rating	Assign a severity rating to each gap based on likelihood and business impact to ePHI.
11. Remediation Planning	Develop actionable, prioritized remediation guidance for each finding.
12. Management Action Planning	Present findings to management and align on ownership, priority, and target dates.

09 EPHI DATA FLOW & SYSTEM LANDSCAPE

The diagram below presents a fictional, representative ePHI data flow for NovaCura's simulated environment, from initial patient interaction through downstream business associate and provider integrations. It is provided to illustrate how TMG Security documents data flow and trust boundaries in an actual assessment deliverable.



Illustrative ePHI Data Flow — Fictional Environment. Not representative of any real system.

ePHI Repositories & Trust Boundaries

- Patient Portal / Specialty Pharmacy: primary intake point for patient-initiated ePHI, including prescription and refill data.
- Clinical Application: clinical coordination records shared across care-team roles.
- CRM / Patient Support: case management records, the subject of the minimum-necessary review in Section 14.
- Cloud Infrastructure & Analytics: hosts application data stores and adherence-reporting analytics workloads.
- Business Associates / Healthcare Providers: laboratory, claims processing, and patient communication integrations exchanging ePHI outside NovaCura's direct operational control.

Diagram Notes

- Privileged Access: administrative access paths into the CRM, clinical application, and cloud environment are highlighted as an elevated-risk trust boundary (see Section 17, RA-002).
- Endpoints: field-based and office-based workstations and portable devices represent an additional ePHI trust boundary (see Section 12, Section 13).
- Backups: backup copies of ePHI-containing data stores are shown as a distinct boundary subject to the contingency planning controls in Section 23.

10 HIPAA SECURITY GOVERNANCE

This section presents NovaCura's fictional HIPAA security governance structure — the roles, committees, and reporting lines through which the organization's HIPAA Security and Privacy program is directed and overseen.

Governance Structure (Fictional)

Chief Information Security Officer	Designated HIPAA Security Official under 45 CFR §164.308(a)(2); accountable for the Security Rule program.
Privacy Officer	Accountable for the HIPAA Privacy Rule program, breach risk assessments, and individual rights processes.
Security Steering Committee	Cross-functional body (security, IT, privacy, legal, clinical operations) meeting quarterly to review program performance.
Third-Party Risk Function	Oversees business associate due diligence, BAA execution, and periodic security review.
Compliance Officer	Oversees enterprise-wide regulatory compliance, including HIPAA policy governance and workforce sanctions.
Board / Executive Oversight	Receives periodic reporting on HIPAA program status, material findings, and remediation progress.

Governance Observations (Fictional)

- The Security Official designation is current and accurate, though the supporting documentation memorandum requires updating to reflect the current organizational structure (see HIPAA-GOV-018).
- The Security Steering Committee meets on its defined quarterly cadence with documented minutes and action tracking.
- Reporting from operational functions (access governance, vulnerability management, business associate oversight) into the governance structure is in place but would benefit from further centralization, consistent with several findings in this report.

11 ADMINISTRATIVE SAFEGUARDS

45 CFR §164.308 requires covered entities and business associates to implement administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures protecting ePHI, and to manage the conduct of the workforce in relation to that protection. The table below presents NovaCura's fictional illustrative status across all nine Administrative Safeguards standards and their implementation specifications.

Standard / Specification	Citation	Description	Illustrative Status	Finding
Security Management Process — Risk Analysis	§164.308(a)(1)(ii)(A)	Accurate and thorough assessment of risks and vulnerabilities to ePHI across the enterprise.	Not In Place	HIPAA-RSK-001
Security Management Process — Risk Management	§164.308(a)(1)(ii)(B)	Implementation of security measures sufficient to reduce identified risks to a reasonable level.	Partially In Place	HIPAA-VUL-012
Security Management Process — Sanction Policy	§164.308(a)(1)(ii)(C)	Application of sanctions against workforce members who fail to comply with security policies.	In Place	—
Security Management Process — Information System Activity Review	§164.308(a)(1)(ii)(D)	Regular review of audit logs, access reports, and security incident tracking reports.	Partially In Place	HIPAA-LOG-003
Assigned Security Responsibility	§164.308(a)(2)	Identification of the security official responsible for Security Rule policies and procedures.	Partially In Place	HIPAA-GOV-018
Workforce Security	§164.308(a)(3)	Authorization, supervision, clearance, and termination procedures for workforce ePHI access.	In Place	—
Information Access Management	§164.308(a)(4)	Policies and procedures for authorizing, establishing, and modifying access to ePHI.	Partially In Place	HIPAA-IAM-002
Security Awareness and Training	§164.308(a)(5)	Security awareness and HIPAA training program for all workforce members.	Partially In Place	HIPAA-TRN-008
Security Incident Procedures	§164.308(a)(6)	Policies and procedures to identify, respond to, mitigate, and document security incidents.	Partially In Place	HIPAA-IR-006
Contingency Plan	§164.308(a)(7)	Data backup, disaster recovery, emergency mode operation, and testing/revision procedures.	Partially In Place	HIPAA-BKP-007
Evaluation	§164.308(a)(8)	Periodic technical and non-technical evaluation of security safeguards.	In Place	—
Business Associate Contracts and Other Arrangements	§164.308(b)(1)	Satisfactory assurances that business associates appropriately safeguard ePHI.	Partially In Place	HIPAA-BAA-005
Policies, Procedures & Documentation	§164.316	Documentation of policies/procedures with periodic review and update.	Partially In Place	HIPAA-DOC-015

Key Observations

- NovaCura's most recent enterprise risk analysis has not been updated to include three ePHI-relevant systems deployed during the assessment period (HIPAA-RSK-001), which this assessment treats as the report's most significant fictional gap given its foundational role in the broader Security Rule program.
- Privileged access recertification, weekly information system activity review, and the annual incident response tabletop exercise are each defined as organizational policy but were not consistently evidenced across all sampled systems and cycles (HIPAA-IAM-002, HIPAA-LOG-003, HIPAA-IR-006).
- Sanction policy, workforce security, and periodic evaluation practices were confirmed as in place and consistently evidenced across the fictional sample reviewed.
- Business associate security review evidence and policy review documentation each showed isolated currency gaps rather than a design failure (HIPAA-BAA-005, HIPAA-DOC-015).

Risk

The most significant fictional risk within this domain is the incomplete enterprise risk analysis, which limits NovaCura's visibility into risk across its full ePHI environment and undermines the evidentiary basis for its broader security program. The remaining gaps represent documentation and consistency shortfalls in otherwise-designed processes rather than the absence of a control, and are rated accordingly.

Recommendations

- Update the enterprise risk analysis to cover all current ePHI-relevant systems and formalize a recurring refresh trigger tied to change management (HIPAA-RSK-001).
- Centralize tracking and evidencing of privileged access reviews, information system activity reviews, and the incident response tabletop exercise across all in-scope systems.
- Complete overdue business associate security reviews and outstanding policy reviews, and move both into the centralized GRC platform.

12 PHYSICAL SAFEGUARDS

45 CFR §164.310 requires physical measures, policies, and procedures to protect NovaCura's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. The table below presents NovaCura's fictional illustrative status across all four Physical Safeguards standards.

Standard / Specification	Citation	Description	Illustrative Status	Finding
Facility Access Controls	§164.310(a)(1)	Policies limiting physical access to facilities housing ePHI systems while ensuring authorized access.	In Place	—
Workstation Use	§164.310(b)	Policies specifying proper functions and manner of use for workstations accessing ePHI.	Partially In Place	HIPAA-PHY-009
Workstation Security	§164.310(c)	Physical safeguards restricting access to workstations to authorized users.	Partially In Place	HIPAA-PHY-009
Device and Media Controls	§164.310(d)(1)	Policies governing receipt, removal, disposal, and re-use of hardware and electronic media.	In Place	—

Observations

- Facility access controls at NovaCura's headquarters and clinical operations center were confirmed as designed and operating consistent with the documented Facility Security Plan, including badge-based access and visitor management.
- Field-based and home-office workstation setups showed an isolated physical-safeguard gap: two of eight sampled setups did not evidence a privacy screen or documented alternative safeguard despite regular ePHI viewing (HIPAA-PHY-009).
- Device and media disposal is performed through a certified destruction business associate with documented certificates of destruction retained for the fictional sample reviewed.

Risk

The identified physical safeguard gap is narrow in scope, affecting a small subset of field-based personnel rather than a facility-wide control design issue, and is rated Low reflecting its limited population and the availability of a straightforward remediation.

Recommendations

- Include a privacy screen as a default component of the standard remote-work equipment package for all personnel with regular ePHI access (HIPAA-PHY-009).
- Continue the current facility access control and device/media disposal practices, which were confirmed as operating effectively in this fictional sample.

13 TECHNICAL SAFEGUARDS

45 CFR §164.312 requires technical policies and procedures for electronic information systems that maintain ePHI, to allow access only to authorized persons and software programs. The table below presents NovaCura's fictional illustrative status across all five Technical Safeguards standards and their implementation specifications.

Standard / Specification	Citation	Description	Illustrative Status	Finding
Access Control — Unique User Identification	§164.312(a)(2)(i)	Assignment of a unique name/number for identifying and tracking each user.	In Place	—
Access Control — Emergency Access Procedure	§164.312(a)(2)(ii)	Procedures for obtaining necessary ePHI access during an emergency.	In Place	—
Access Control — Automatic Logoff	§164.312(a)(2)(iii)	Addressable: session termination after a defined period of inactivity.	Partially In Place	HIPAA-ACC-014
Access Control — Encryption and Decryption	§164.312(a)(2)(iv)	Addressable: mechanism to encrypt/decrypt ePHI where reasonable and appropriate.	Partially In Place	HIPAA-ENC-004
Audit Controls	§164.312(b)	Hardware/software/procedural mechanisms to record and examine ePHI system activity.	Partially In Place	HIPAA-AUD-013
Integrity	§164.312(c)(1)	Mechanisms to authenticate ePHI and protect it from improper alteration or destruction.	In Place	—
Person or Entity Authentication	§164.312(d)	Verification that a person/entity seeking ePHI access is the one claimed.	Partially In Place	HIPAA-MFA-016
Transmission Security — Integrity Controls	§164.312(e)(2)(i)	Addressable: measures to ensure ePHI is not improperly modified in transit.	In Place	—
Transmission Security — Encryption	§164.312(e)(2)(ii)	Addressable: encryption of ePHI whenever deemed appropriate during transmission.	In Place	—

Observations

- Unique user identification, emergency access, integrity controls, and transmission security were each confirmed as designed and operating effectively across the fictional sample reviewed.
- Automatic logoff is standardized at 15 minutes across most ePHI-accessing applications, with one clinical application found configured at a longer 45-minute timeout not yet aligned to the current standard (HIPAA-ACC-014).
- Encryption and decryption coverage is strong across the current managed device fleet, with a residual gap on 11 legacy field-issued devices predating the current MDM enrollment standard (HIPAA-ENC-004).
- Audit controls are deployed via a centralized SIEM platform; review cadence for one application was found running behind its internally defined schedule (HIPAA-AUD-013).
- Person or entity authentication is enforced via MFA on primary paths, with one legacy remote-access path to an internal scheduling tool identified as relying on password-only authentication (HIPAA-MFA-016, reported as an internal observation).

Risk

Technical Safeguards reflect NovaCura's strongest overall control domain in this fictional assessment. The identified gaps are narrow — a legacy device population, a single application's configuration, and one legacy access path — rather than systemic design failures, and are rated accordingly.

Recommendations

- Re-enroll legacy field devices in MDM and verify/remediate encryption status (HIPAA-ENC-004).
- Align the clinical coordination application's session timeout to the 15-minute internal standard (HIPAA-ACC-014).
- Restore the CRM audit log review to its defined bi-weekly cadence (HIPAA-AUD-013).
- Migrate the legacy scheduling tool's remote-access path behind the primary SSO/MFA gateway (HIPAA-MFA-016).

14 HIPAA PRIVACY RULE REVIEW

This section presents NovaCura's fictional illustrative status across the HIPAA Privacy Rule areas most relevant to its patient-support and specialty pharmacy operations, codified at 45 CFR Part 164, Subpart E.

Privacy Area	Citation	Focus of Review	Illustrative Status
Notice of Privacy Practices	§164.520	Current NPP distributed to patients and posted consistent with requirements.	In Place
Permitted Uses and Disclosures	§164.502	Uses/disclosures of PHI for treatment, payment, and operations, and other permitted purposes.	In Place
Minimum Necessary	§164.502(b) / §164.514(d)	Reasonable efforts to limit PHI access/use/disclosure to the minimum necessary for the purpose.	Partially In Place
Individual Right of Access	§164.524	Process for individuals to request and receive access to their PHI.	In Place
Right to Request Amendment	§164.526	Process for individuals to request amendment of their PHI.	In Place
Accounting of Disclosures	§164.528	Process for tracking and providing an accounting of certain PHI disclosures.	In Place
Workforce Privacy Training	§164.530(b)	Workforce training on privacy policies and procedures relevant to their function.	In Place
Privacy Complaints & Sanctions	§164.530(d)-(e)	Process for receiving privacy complaints and applying sanctions for violations.	In Place

Observations

- NovaCura's Notice of Privacy Practices, individual rights processes (access, amendment, accounting of disclosures), workforce privacy training, and privacy complaint handling were each confirmed as designed and operating consistent with the fictional sample reviewed.
- The patient-support CRM's role model grants broader-than-necessary PHI visibility for the majority of sampled patient-support sub-teams, representing a minimum-necessary gap (HIPAA-PRV-010, see Section 17 for the related risk analysis entry).

Risk

NovaCura's Privacy Rule program reflects a generally mature design, with the minimum-necessary gap in CRM access provisioning representing the primary fictional exception. Because it affects a defined population and system rather than the Privacy Rule program broadly, it is rated Medium.

Recommendations

- Redesign the CRM role model around minimum-necessary access for each patient-support sub-team and re-provision affected users accordingly (HIPAA-PRV-010).
- Continue NovaCura's current individual rights, workforce privacy training, and complaint handling practices, which were confirmed as operating effectively in this fictional sample.

15 BREACH NOTIFICATION REVIEW

FICTIONAL INCIDENT SCENARIO — USED SOLELY TO DEMONSTRATE ASSESSMENT METHODOLOGY. NO ACTUAL BREACH OCCURRED.

The HIPAA Breach Notification Rule (45 CFR §§164.400–414) requires covered entities and business associates to provide notification following the discovery of a breach of unsecured PHI. This section reviews NovaCura's fictional breach identification, risk assessment, and notification workflow design, illustrated through a single fictional incident scenario constructed solely for methodology demonstration.

Fictional Incident Scenario

Scenario (entirely fictional, for demonstration only): a workforce member's email mailbox was reported as potentially compromised following an unusual login alert. A subsequent fictional review determined the mailbox contained correspondence potentially referencing PHI for approximately 2,400 fictional individuals. This scenario is used here purely to illustrate how TMG Security documents a covered entity's breach identification and response workflow; it does not describe any real event.

Illustrative Workflow Review

Identification	Fictional scenario: anomalous login alert triggered SOC investigation within the simulated timeline used for this exercise.
Containment	Fictional scenario: mailbox access was suspended and credentials reset as an illustrative containment step.
Breach Risk Assessment	Four-factor risk assessment (nature/extent of PHI, unauthorized recipient, whether PHI was acquired/viewed, mitigation extent) performed and documented for this fictional scenario, consistent with §164.402.
Documentation	Fictional incident record, including risk assessment outcome and mitigation steps, retained consistent with §164.316(b).
Notification Workflow	Fictional workflow: Privacy Officer determination of notification obligation, drafting of individual notification letters, and HHS notification scheduling consistent with §§164.404 and 164.408 timeframes.
Business Associate Escalation	Fictional scenario did not involve a business associate; the review confirmed NovaCura's documented BA-to-covered-entity notification workflow under §164.410 as designed for such a scenario.
HHS Reporting Workflow	Fictional review confirmed NovaCura's documented process for HHS breach portal reporting, including annual summary reporting for breaches affecting fewer than 500 individuals.

Observations

- NovaCura's documented Breach Response Procedure (EV-016) defines a complete workflow spanning identification, containment, risk assessment, notification, and documentation, consistent with the current Breach Notification Rule.
- A sample review of four fictional logged security events found the four-factor breach risk assessment formally documented for three events; one lower-severity single-patient event was resolved informally without a separately documented assessment (HIPAA-BRN-011).

Risk

NovaCura's breach notification workflow design is sound; the identified gap concerns consistent documentation of the risk assessment step for lower-severity events rather than a defect in the workflow itself, and is rated Medium.

Recommendations

- Require every PHI-involving security event, regardless of apparent severity, to be routed through the documented four-factor breach risk assessment workflow (HIPAA-BRN-011).
- Continue NovaCura's current notification-timeframe and HHS reporting practices, which were confirmed as designed consistent with §§164.404–408.

16 BUSINESS ASSOCIATE MANAGEMENT

45 CFR §§164.308(b) and 164.314(a) require covered entities to obtain satisfactory assurances, through a Business Associate Agreement (BAA), that business associates will appropriately safeguard PHI, and to have a process in place to respond to a business associate's material breach of that agreement. The table below presents NovaCura's fictional business associate inventory for the six sampled relationships.

Business Associate	Category	BAA Executed	Security Review	Risk Level
Cloud Hosting Provider (Fictional)	Infrastructure / Cloud Hosting	Yes	Overdue (18+ months)	High
Claims Processing Provider (Fictional)	Claims / Billing Processing	Yes	Overdue (18+ months)	High
Patient Communication Platform (Fictional)	Patient Messaging / Notifications	Yes	Current	Medium
Laboratory Integration Provider (Fictional)	Clinical / Lab Data Integration	Yes	Current	Medium
Managed Security Provider (Fictional)	SOC / Managed Detection & Response	Yes	Current	Low
Document Destruction Provider (Fictional)	Physical / Media Destruction	Yes	Current	Low

Due Diligence & Oversight Review

- All six sampled business associates had a current, executed BAA on file including required breach-notification and security-obligation clauses.
- Annual security due-diligence review evidence was current for four of six sampled business associates; the cloud hosting provider's and claims processing provider's review evidence exceeded 18 fictional months (HIPAA-BAA-005).
- Termination/offboarding provisions, including data return or destruction obligations, were confirmed present in all sampled BAA templates.
- Incident notification clauses obligating each business associate to notify NovaCura of a security incident or breach were confirmed present in all sampled BAAs.

Risk

Business associate contracting is well established across NovaCura's sampled relationships; the primary fictional gap is the currency of ongoing security due-diligence review for two higher-risk associates, rated High given those associates' direct access to ePHI-containing infrastructure.

Recommendations

- Complete overdue security reviews for the cloud hosting and claims processing providers (HIPAA-BAA-005).
- Migrate business associate review tracking into the centralized GRC platform with automated review-due reminders.
- Reaffirm the annual review cadence for all business associates classified as high-risk in NovaCura's Third-Party Risk Management Policy.

17 RISK ANALYSIS & RISK MANAGEMENT

45 CFR §164.308(a)(1)(ii)(A) requires an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI; §164.308(a)(1)(ii)(B) requires implementation of security measures sufficient to reduce those risks to a reasonable and appropriate level. This section presents NovaCura's fictional illustrative ePHI risk register, developed as part of this sample assessment's simulated risk analysis exercise.

ILLUSTRATIVE FICTIONAL RISK REGISTER — DEMONSTRATION METHODOLOGY ONLY

Risk Rating Methodology

Each fictional risk below is rated by combining a Likelihood assessment (Rare, Unlikely, Possible, Likely, Almost Certain) with an Impact assessment (Insignificant, Minor, Moderate, Major, Severe) across a 5×5 matrix, consistent with the Risk Heatmap presented in Section 27. Existing controls are then factored in to produce a residual risk rating and a recommended treatment (Mitigate, Transfer, Accept, or Avoid).

RA-001 — Unauthorized Access to Patient Portal				Risk Rating: **High**
Threat	External threat actor attempting credential-based or session-based unauthorized access.			
Vulnerability	Session and account-lockout controls on the patient portal are configured but not independently validated against current threat patterns.			
Existing Controls	MFA available on the portal, WAF, account lockout after failed attempts, SIEM alerting on anomalous login patterns.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Major	**High**	Medium	Mitigate

RA-002 — Compromised Privileged Account				Risk Rating: **Critical**
Threat	Credential theft or insider misuse of a privileged/administrative account with access to ePHI systems.			
Vulnerability	Privileged access recertification evidence is incomplete for two of three sampled systems (see HIPAA-IAM-002).			
Existing Controls	MFA on administrative paths, partial privileged access management (PAM) tooling, centralized identity provider.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Severe	**Critical**	High	Mitigate — Priority

RA-003 — Ransomware Affecting ePHI Systems				Risk Rating: **Critical**
Threat	Ransomware actor encrypting or exfiltrating ePHI-relevant systems and demanding payment for restoration.			
Vulnerability	Backup restoration testing has not been consistently completed on the defined quarterly cycle for all in-scope systems (see HIPAA-BKP-007).			
Existing Controls	EDR across in-scope endpoints and servers, network segmentation, immutable backup copies, incident response plan.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Severe	**Critical**	High	Mitigate — Priority

RA-004 — Business Associate Security Failure				Risk Rating: **High**
Threat	A business associate's own security failure (breach, misconfiguration, or ransomware) exposes ePHI shared with or hosted by that associate.			
Vulnerability	Annual security due-diligence review evidence is overdue for two of six sampled business associates (see HIPAA-BAA-005).			
Existing Controls	Executed BAAs for all sampled business associates, incident-notification clauses, informal ongoing relationship oversight.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Major	**High**	Medium	Mitigate

RA-005 — Unencrypted Endpoint Storage				Risk Rating: **Medium**
Threat	Loss or theft of a portable device that stores or caches ePHI.			
Vulnerability	Full-disk encryption status is unverified on 11 legacy field-issued devices (see HIPAA-ENC-004).			
Existing Controls	MDM enrollment and encryption enforcement for the current device fleet, endpoint asset inventory.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Unlikely	Major	Medium	Medium	Mitigate

RA-006 — Excessive User Privileges				Risk Rating: **Medium**
Threat	Insider misuse or lateral movement enabled by user access broader than functionally required.			
Vulnerability	CRM role model grants broader-than-necessary PHI visibility for a majority of sampled patient-support sub-teams (see HIPAA-PRV-010).			
Existing Controls	Defined RBAC model, periodic (though inconsistently evidenced) access recertification, activity logging.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Moderate	Medium	Medium	Mitigate

RA-007 — Inadequate Audit Log Review				Risk Rating: **Medium**
Threat	Unauthorized or anomalous ePHI access that goes undetected due to inconsistent log review.			
Vulnerability	Weekly information system activity review and CRM audit log review cadence are inconsistently evidenced (see HIPAA-LOG-003, HIPAA-AUD-013).			
Existing Controls	SIEM deployed across in-scope systems with automated alert triage; manual periodic review process supplements automated alerting.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Moderate	Medium	Medium	Mitigate

RA-008 — Backup Recovery Failure				Risk Rating: **Medium**
Threat	Inability to recover ePHI systems within an acceptable timeframe following a system failure, natural event, or other contingency.			
Vulnerability	Restoration testing gaps for the CRM platform and partial testing for the specialty pharmacy database (see HIPAA-BKP-007).			
Existing Controls	Scheduled backup jobs confirmed completing successfully, documented Contingency Plan, disaster recovery test program (partial coverage).			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Unlikely	Major	Medium	Medium	Mitigate

RA-009 — Phishing / Credential Theft				Risk Rating: **High**
Threat	Workforce member falls victim to a phishing campaign resulting in credential compromise or malware execution.			
Vulnerability	Role-based supplemental privacy/security training completion is not fully tracked for all patient-support and fulfillment staff (see HIPAA-TRN-008).			
Existing Controls	Email security gateway, simulated phishing program, enterprise annual security awareness training (91% completion).			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Likely	Moderate	High	Medium	Mitigate

RA-010 — Improper PHI Disclosure		Risk Rating: **Medium**
Threat	Workforce member discloses PHI beyond what is minimally necessary for the intended purpose, whether through error or overly broad system access.	
Vulnerability	CRM access provisioning does not consistently apply the minimum necessary standard across patient-support sub-teams (see HIPAA-PRV-010).	

Existing Controls	Privacy policy and workforce privacy training, role-based CRM access (currently over-broad for some sub-teams), disclosure logging.			
Likelihood	**Impact**	**Rating**	**Residual**	**Treatment**
Possible	Moderate	Medium	Medium	Mitigate

Risk Management Summary

Two fictional risks — RA-002 (Compromised Privileged Account) and RA-003 (Ransomware Affecting ePHI Systems) — carry a Critical rating in this sample register, driven by the potential severity of impact combined with the access-governance and backup-restoration gaps identified elsewhere in this report. Three risks are rated High, reflecting realistic likelihood combined with major potential impact. The remaining five risks are rated Medium, reflecting either lower likelihood or more contained potential impact. NovaCura's simulated risk management program is recommended to prioritize the two Critical-rated risks within the first 30 days of the remediation roadmap (Section 28), consistent with the underlying findings driving each rating.

18 SECURITY INCIDENT RESPONSE

This section reviews the operational maturity of NovaCura's security incident response capability supporting the Security Incident Procedures standard (45 CFR §164.308(a)(6)) reviewed at a policy level in Section 11, focusing on the people, process, and tooling used to detect, triage, and respond to security events affecting ePHI systems.

Program Components Reviewed

- Documented Incident Response Plan (EV-012) with defined roles across security, IT, legal, privacy, and communications functions.
- SOC-based detection and triage workflow, integrated with the centralized SIEM platform (see Section 21, Audit Controls & Logging).
- Escalation paths from SOC triage into formal incident response activation, including breach risk assessment hand-off to the Privacy Officer (see Section 15).
- Annual tabletop exercise program intended to validate plan assumptions, roles, and communication paths.

Observations

- NovaCura's Incident Response Plan is current, comprehensive, and assigns clear ownership across functions.
- The most recent documented tabletop exercise was performed approximately 19 fictional months prior to the assessment date, exceeding NovaCura's own defined annual cadence (HIPAA-IR-006).
- SOC-to-incident-response escalation criteria are documented and were confirmed as understood by SOC personnel during simulated interviews for this fictional exercise.

Risk

An extended gap between incident response exercises increases the likelihood that plan assumptions, contact lists, or escalation paths are outdated when a real incident occurs, potentially slowing containment. This is rated Medium given the plan itself remains current and comprehensive.

Recommendations

- Assign formal ownership of the annual tabletop exercise and schedule the next exercise within 60 days (HIPAA-IR-006).
- Incorporate lessons learned from each exercise into a documented plan revision cycle.

19 VULNERABILITY & PATCH MANAGEMENT

This section reviews NovaCura's vulnerability identification, prioritization, and remediation program supporting ePHI-relevant systems. The current HIPAA Security Rule does not itself prescribe a specific vulnerability scanning frequency or numeric patching deadline; this review evaluates NovaCura's program against its own defined, risk-based internal SLAs, which the organization has adopted as one of the risk management measures implementing §164.308(a)(1)(ii)(B).

Program Components Reviewed

- Vulnerability identification coverage across in-scope servers, endpoints, and cloud workloads, including third-party/business-associate-facing interfaces.
- Risk-based prioritization and internal SLA-based remediation timeframes (organizational policy).
- Formal exception and compensating-control workflow for vulnerabilities exceeding the internal SLA.
- Validation testing confirming remediated vulnerabilities are closed.

Observations

- Vulnerability identification coverage was confirmed across the fictional sampled asset population, including cloud workloads and internet-facing interfaces.
- 14% of open vulnerabilities affecting ePHI-relevant systems had exceeded NovaCura's internal SLA remediation timeframe, and a subset of those lacked a documented exception or compensating control (HIPAA-VUL-012).
- Validation testing for remediated vulnerabilities was confirmed as consistently performed for the fictional sample reviewed.

Risk

Overdue vulnerabilities without a documented risk decision represent unmanaged risk to ePHI-relevant systems; this is rated Medium reflecting a defined but inconsistently enforced exception process rather than an absent vulnerability management program.

Recommendations

- Make the formal exception workflow mandatory for every vulnerability exceeding the internal SLA on ePHI-relevant systems (HIPAA-VUL-012).
- Report aggregate SLA performance to the Security Steering Committee monthly.

20 ACCESS CONTROL & AUTHENTICATION

This section reviews the operational implementation of NovaCura's access control and authentication program supporting the Technical Safeguards Access Control and Person or Entity Authentication standards reviewed in Section 13, focusing on identity and access management (IAM) tooling, privileged access, and multi-factor authentication (MFA) coverage.

Program Components Reviewed

- Centralized identity provider supporting single sign-on (SSO) across the majority of ePHI-relevant applications.
- MFA enforcement on primary remote-access and administrative paths.
- Privileged/administrative access provisioning and periodic recertification (see also Section 11, Information Access Management).
- Role-based access design within the patient-support CRM (see also Section 14, Minimum Necessary).

Observations

- MFA and SSO coverage is strong across the primary VPN, administrative consoles, and the majority of ePHI-relevant applications.
- One legacy remote-access path to an internal scheduling tool was found relying on password-only authentication, outside the primary SSO/MFA gateway (HIPAA-MFA-016).

- Privileged access recertification evidence was incomplete for two of three sampled systems during the most recent semi-annual review cycle (HIPAA-IAM-002).

Risk

NovaCura's access control and authentication program is well designed around a centralized identity provider; the identified gaps are narrow — a single legacy access path and incomplete recertification evidence for select systems — and are rated accordingly.

Recommendations

- Migrate the legacy scheduling tool's remote-access path behind the primary SSO/MFA gateway (HIPAA-MFA-016).
- Centralize privileged access recertification tracking with documented sign-off for every in-scope system (HIPAA-IAM-002).

21 AUDIT CONTROLS & LOGGING

This section reviews the operational implementation of NovaCura's audit logging and monitoring program supporting the Audit Controls standard (45 CFR §164.312(b)) and the Information System Activity Review specification (§164.308(a)(1)(ii)(D)). HIPAA does not itself prescribe a specific log retention period; this review evaluates NovaCura's program against its own defined internal Logging & Monitoring Standard.

Program Components Reviewed

- Centralized SIEM aggregating logs from ePHI-relevant systems, network infrastructure, and cloud environments.
- Automated alert correlation and SOC analyst triage workflow.
- System-specific manual audit log review cadence defined by data sensitivity and criticality.
- Log integrity protections preventing unauthorized modification of retained audit records.

Observations

- Automated SIEM alert triage operates continuously across in-scope systems with documented escalation criteria into the incident response workflow (see Section 18).
- The documented weekly information system activity review checklist showed gaps in seven of twenty-six fictional sampled weeks for the patient portal and specialty pharmacy application logs (HIPAA-LOG-003).
- The CRM platform's defined bi-weekly manual audit log review was found running on an approximately monthly cadence during the assessment period (HIPAA-AUD-013).
- Log integrity protections, including write-once storage for centralized SIEM logs, were confirmed as configured consistent with NovaCura's internal standard.

Risk

Gaps in the documented review cadence reduce assurance that anomalous or unauthorized ePHI access would be identified in a timely manner through manual review, though automated SIEM alerting continues to operate as a compensating layer; this is rated Medium to High depending on the specific system population affected.

Recommendations

- Assign a documented backup reviewer for the weekly information system activity review and automate checklist completion tracking (HIPAA-LOG-003).
- Reassign CRM audit log review to a fixed analyst with automated review-completion reminders (HIPAA-AUD-013).

22 ENCRYPTION & TRANSMISSION SECURITY

This section reviews NovaCura's use of encryption to protect ePHI at rest and in transit. The HIPAA Security Rule identifies encryption as an addressable implementation specification under both Access Control (§164.312(a)(2)(iv)) and Transmission Security (§164.312(e)(2)(ii)): NovaCura must implement it as specified, implement an equivalent alternative, or document why it is not reasonable and appropriate given its own risk analysis. This review uses risk-based, "reasonable and appropriate safeguards" language throughout rather than asserting a specific mandated algorithm.

Program Components Reviewed

- Encryption at rest for databases and cloud storage supporting ePHI-relevant systems.
- Encryption in transit for application traffic, API integrations, and email transmission of PHI.
- Full-disk encryption on portable devices and laptops capable of storing ePHI.
- Encryption of backup copies of ePHI-containing data stores.

Observations

- Encryption at rest for in-scope databases and cloud storage, encryption in transit for application and API traffic, and encryption of backup copies were each confirmed as implemented using industry-standard, currently supported cryptographic protocols.
- Full-disk encryption is enforced and verified on 94% of sampled laptops; 11 legacy field-issued devices predating the current MDM enrollment standard were found without confirmed encryption status (HIPAA-ENC-004).
- Secure email transmission of PHI to external parties is supported through an encrypted-email gateway, confirmed as configured and in use for the fictional sample reviewed.

Risk

NovaCura's encryption posture is strong across centrally managed infrastructure and applications; the identified gap is confined to a legacy population of field-issued devices and is rated High given the loss/theft exposure characteristic of portable devices.

Recommendations

- Re-enroll all legacy field devices in MDM and verify/remediate encryption status (HIPAA-ENC-004).
- Add device-encryption verification as a mandatory step in the device issuance and periodic asset audit process.

23 BACKUP, DISASTER RECOVERY & CONTINGENCY PLANNING

45 CFR §164.308(a)(7) requires NovaCura to establish policies and procedures for responding to an emergency or other occurrence that damages systems containing ePHI, including a data backup plan, disaster recovery plan, and emergency mode operation plan, along with (addressable) testing and revision procedures and applications/data criticality analysis.

Fictional Tabletop Scenario

FICTIONAL RANSOMWARE RECOVERY TABLETOP — DEMONSTRATION METHODOLOGY ONLY

Scenario (fictional, for demonstration only): a simulated ransomware event encrypts the specialty pharmacy database and a subset of file storage. The fictional tabletop walked NovaCura's contingency plan through activation of emergency mode operation, isolation of affected systems, restoration from the most recent immutable backup copy, and validation of data integrity prior to returning the system to production. The exercise is used here solely to illustrate TMG Security's contingency-planning assessment methodology.

Observations

- NovaCura's documented Contingency Plan defines a data backup plan, disaster recovery plan, and emergency mode operation plan with assigned roles, consistent with §164.308(a)(7).
- Backup jobs for in-scope ePHI systems were confirmed as completing successfully on schedule across the fictional sample reviewed.

- Restoration testing records evidenced two of four fictional quarterly test cycles for the specialty pharmacy database; the CRM platform's backup restoration had not been tested during the assessment period, pending coordination with the managed-hosting business associate (HIPAA-BKP-007).
- Backup copies are stored in an isolated, immutable configuration separate from production credentials, reducing exposure to a ransomware event that also compromises production access.

Risk

Untested backup restoration procedures create uncertainty as to whether ePHI could be recovered accurately and within an acceptable timeframe following a ransomware event or other contingency; this is rated Medium given backups themselves are confirmed as completing successfully and stored in an isolated configuration.

Recommendations

- Coordinate and complete a CRM platform restoration test with the managed-hosting business associate (HIPAA-BKP-007).
- Complete the outstanding specialty pharmacy restoration test cycles and formalize restoration testing as a scheduled, tracked activity across all in-scope systems.

24 SECURITY AWARENESS & WORKFORCE TRAINING

45 CFR §164.308(a)(5)(i) requires a security awareness and training program for all workforce members, including management. This section reviews the operational execution of NovaCura's program, building on the policy-level review in Section 11.

Program Components Reviewed

- Enterprise-wide annual HIPAA and security awareness training, tracked through the central learning management system (LMS).
- Role-based supplemental privacy/security training for personnel handling ePHI directly, including patient-support and pharmacy fulfillment staff.
- Phishing simulation program and completion/response tracking.
- New-hire onboarding training and periodic annual refresh cycle.

Observations

- Enterprise annual training completion was evidenced at approximately 91% of the fictional 1,250-person workforce as of the assessment date, with new-hire onboarding training consistently completed prior to system access provisioning.
- Role-based supplemental training for patient-support and pharmacy fulfillment staff is administered outside the central LMS for a subset of departments, and completion status could not be fully confirmed for a sampled department (HIPAA-TRN-008).
- The phishing simulation program runs on a regular cadence with completion and click-rate metrics tracked and reported to the Security Steering Committee.

Risk

Incomplete tracking of role-based supplemental training limits NovaCura's ability to confirm that workforce members handling ePHI directly have completed role-appropriate training, and is rated Medium.

Recommendations

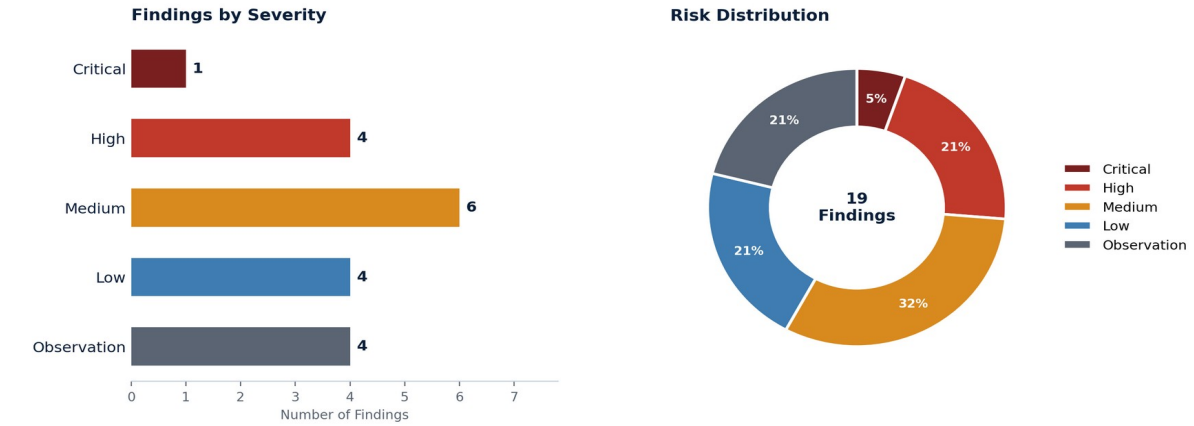
- Migrate all role-based supplemental training tracking into the central LMS and close the identified completion gap (HIPAA-TRN-008).
- Report enterprise-wide and role-based completion rates to management quarterly.

25 FINDINGS SUMMARY

This fictional sample assessment produced a total of 19 illustrative findings and observations across NovaCura's Administrative, Physical, and Technical Safeguards, Privacy Rule, Breach Notification Rule, and Business Associate management domains. The dashboard below summarizes findings by severity for demonstration purposes; the illustrative HIPAA Control Matrix in Section 33 presents status by control area.

1	4	6	4	4
Critical	High	Medium	Low	Observations

Fictional Sample Findings Dashboard — Illustrative Data Only



Fictional Sample Findings Dashboard — Illustrative Data Only

Findings by Domain

Domain	Findings
Administrative Safeguards	**9**
Technical Safeguards	**4**
Business Associate Management	**1**
Privacy Rule	**1**
Breach Notification Rule	**1**
Vulnerability & Patch Management	**1**
Physical Safeguards	**1**
Regulatory Watch	**1**

Interpretation

One critical-severity finding was identified relating to the completeness of NovaCura's enterprise-wide ePHI risk analysis (Requirement §164.308(a)(1)(ii)(A)). Four high-severity findings span privileged access review evidence, information system activity review documentation, portable-device encryption coverage, and business associate security review currency. Six medium-severity findings are distributed across incident response exercising, backup restoration testing, workforce training tracking, minimum-necessary CRM access design, breach risk assessment documentation, and vulnerability remediation exception tracking. Four low-severity findings and four observations reflect narrower process, configuration, and documentation-currency gaps that, while not urgent, warrant remediation to strengthen overall control maturity.

26 DETAILED FINDINGS

Every fictional sample finding is presented below in full consulting-format detail: control objective, criteria, condition, cause, risk/business impact, evidence reference, recommendation, management response, owner, target date, and status. All findings, evidence, and management responses on this page are entirely fictional.

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

HIPAA-RSK-001 — Incomplete Enterprise-Wide ePHI Risk Analysis	CRITICAL
HIPAA Reference: 45 CFR §164.308(a)(1)(ii)(A)	**Illustrative Assessment Status: Not In Place**
Control Objective	NovaCura conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it creates, receives, maintains, or transmits, covering the full enterprise environment.
Criteria	45 CFR §164.308(a)(1)(ii)(A) requires covered entities and business associates to conduct an accurate and thorough risk analysis. HHS/OCR guidance describes this as an enterprise-wide exercise covering all systems, applications, and locations that create, receive, maintain, or transmit ePHI, not a subset of the environment.
Condition	NovaCura's most recent enterprise risk analysis, last updated in fictional Q1 2025, was found not to include three ePHI-relevant systems brought into production during the fictional 2025–2026 period: the patient-support CRM platform, a newly deployed specialty pharmacy fulfillment application, and a cloud analytics environment used for adherence reporting. The existing risk analysis document also did not evidence a documented likelihood/impact rating methodology consistently applied across the systems it did cover.
Cause	No formal trigger exists in NovaCura's change management or system-onboarding process requiring the enterprise risk analysis to be revisited when a new ePHI-relevant system, application, or significant business change is introduced.
Risk / Business Impact	Without a current, complete risk analysis, NovaCura cannot reliably demonstrate that risks to ePHI across its full technology footprint have been identified and are being managed, undermining the foundation on which its broader HIPAA Security Rule program is built and increasing the likelihood that emerging risks in newer systems go unaddressed.
Evidence Reference	*EV-002 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Update the enterprise risk analysis to formally incorporate the CRM platform, fulfillment application, and analytics environment, apply a consistent likelihood/impact methodology across all in-scope systems, and add a mandatory risk-analysis-refresh checkpoint to the system onboarding and change management process.
Management Response	*Agreed. NovaCura will commission an updated enterprise-wide risk analysis covering all current ePHI systems and will formalize a recurring refresh trigger tied to the change management process.*
Owner / Target Date / Status	**Chief Information Security Officer** | 15 Oct 2026 | **Open**

HIPAA-IAM-002 — Privileged Access Review Evidence Incomplete	HIGH
HIPAA Reference: 45 CFR §164.308(a)(4)(ii)(C)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Access to ePHI systems, and particularly privileged/administrative access, is granted, modified, and periodically reviewed consistent with defined roles and business need.
Criteria	45 CFR §164.308(a)(4)(ii)(C) requires policies and procedures for granting access to ePHI, such as through role-based access, and for establishing, documenting, reviewing, and modifying a user's right of access. NovaCura's own Access Governance Policy commits to a semi-annual review of privileged and administrative accounts across ePHI-relevant systems.
Condition	A sample review of privileged account recertification records for the specialty pharmacy system, patient portal administrative console, and CRM platform found that formal sign-off evidence for the most recent semi-annual review cycle was available for the specialty pharmacy system only; recertification for the patient portal and CRM administrative accounts was reported as performed informally by system owners but was not documented.
Cause	The privileged access review process is decentralized across system owners, with no centralized tracking tool or reminder workflow ensuring each in-scope system's review is completed and evidenced on the defined semi-annual cadence.

Risk / Business Impact	Undocumented privileged access reviews increase the risk that excessive, stale, or inappropriate administrative access to ePHI-containing systems persists undetected, and limit NovaCura's ability to demonstrate access governance in the event of an incident or regulatory inquiry.
Evidence Reference	*EV-005 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Centralize privileged access recertification tracking across all ePHI-relevant systems in a single governance tool, require documented sign-off from each system owner for every review cycle, and report completion status to the Security Steering Committee quarterly.
Management Response	*Agreed. NovaCura will implement centralized recertification tracking and require documented sign-off for all in-scope systems beginning with the next semi-annual cycle.*
Owner / Target Date / Status	**IAM Program Manager** | 30 Oct 2026 | **Open**

HIPAA-LOG-003 — Information System Activity Review Not Consistently Documented	**HIGH**
HIPAA Reference: 45 CFR §164.308(a)(1)(ii)(D)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Records of system activity, such as audit logs, access reports, and security incident tracking reports, are regularly reviewed for ePHI-relevant systems.
Criteria	45 CFR §164.308(a)(1)(ii)(D) requires the implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Condition	NovaCura's SOC performs automated SIEM alert triage continuously; however, a sample review of the documented weekly information-system-activity-review checklist found gaps in seven of the twenty-six fictional sampled weeks within the assessment period, where the checklist was not completed or archived for the patient portal and specialty pharmacy application logs.
Cause	The weekly activity review checklist is a manual process performed by a single SOC analyst role without a formal backup assignment, resulting in gaps during periods of staff absence.
Risk / Business Impact	Gaps in the documented information system activity review reduce assurance that anomalous or unauthorized ePHI access would be identified in a timely manner and weaken NovaCura's evidentiary record of ongoing monitoring.
Evidence Reference	*EV-007 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Assign a documented backup reviewer for the weekly information system activity review, automate checklist completion tracking within the SIEM platform, and escalate any missed review week to the SOC Manager within 24 hours.
Management Response	*Agreed. A backup reviewer will be assigned and checklist completion will be tracked automatically within the SIEM platform going forward.*
Owner / Target Date / Status	**SOC Manager** | 15 Oct 2026 | **Open**

HIPAA-ENC-004 — Encryption Coverage Gap on Selected Portable Devices	**HIGH**
HIPAA Reference: 45 CFR §164.312(a)(2)(iv)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Reasonable and appropriate safeguards, including encryption where determined appropriate through NovaCura's risk analysis, protect ePHI stored on portable and mobile devices.
Criteria	45 CFR §164.312(a)(2)(iv) identifies encryption and decryption as an addressable implementation specification: NovaCura must implement it as specified, implement an equivalent alternative measure, or document why it is not reasonable and appropriate given its own risk analysis. NovaCura's risk analysis and internal Endpoint Security Standard determined full-disk encryption to be a required safeguard for all devices capable of storing ePHI.
Condition	A sample review of the managed device inventory found full-disk encryption enforced and verified on 94% of sampled laptops issued to patient-support and clinical-coordination staff; a subset of 11 devices issued to field-based patient support personnel prior to the current MDM enrollment standard were found without confirmed encryption status.
Cause	Devices issued before the current MDM enrollment standard was adopted were not retroactively brought into the encryption compliance monitoring scope.

Risk / Business Impact	Unencrypted or unverified portable devices that may store or cache ePHI represent an elevated exposure in the event of device loss or theft, consistent with the loss/theft scenarios most frequently cited in HHS/OCR breach reporting for portable media.
Evidence Reference	*EV-009 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Bring all legacy field devices into current MDM enrollment, verify and remediate encryption status for the 11 identified devices, and add device-encryption verification as a mandatory step in the device issuance and periodic asset audit process.
Management Response	*Agreed. All legacy field devices will be re-enrolled in MDM and encryption status verified and remediated where required.*
Owner / Target Date / Status	**IT Endpoint Security Lead** | 30 Oct 2026 | **Open**

HIPAA-BAA-005 — Business Associate Security Review Evidence Incomplete	**HIGH**
HIPAA Reference: 45 CFR §164.308(b)(1) / §164.314(a)(1)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Business associates that create, receive, maintain, or transmit ePHI on NovaCura's behalf operate under a compliant Business Associate Agreement (BAA) and are subject to periodic security due-diligence review.
Criteria	45 CFR §164.308(b)(1) and §164.314(a)(1) require satisfactory assurances, documented through a BAA, that a business associate will appropriately safeguard ePHI. NovaCura's internal Third-Party Risk Management Policy additionally commits to an annual security review of business associates classified as high-risk.
Condition	All six sampled business associates had an executed BAA on file. However, annual security review evidence (such as a completed security questionnaire, SOC 2 report review, or equivalent due-diligence artifact) was current for four of the six sampled business associates; the cloud hosting provider's and the claims processing provider's most recent security review evidence was more than eighteen fictional months old.
Cause	Business associate security review scheduling is tracked manually in a spreadsheet without automated reminders, and did not surface the two overdue reviews to the Third-Party Risk Management function in time for the review cycle.
Risk / Business Impact	Lapsed security due-diligence review of business associates handling ePHI reduces NovaCura's visibility into the current security posture of those third parties and its ability to identify and respond to a business associate security failure before it affects NovaCura's own ePHI.
Evidence Reference	*EV-010 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Complete overdue security reviews for the cloud hosting and claims processing providers, migrate business associate review tracking into the centralized GRC platform with automated reminders, and formally re-affirm the annual review cadence for all business associates classified as high-risk.
Management Response	*Agreed. Overdue reviews will be completed and business associate review tracking will move to the centralized GRC platform with automated scheduling.*
Owner / Target Date / Status	**Third-Party Risk Manager** | 30 Nov 2026 | **Open**

HIPAA-IR-006 — Security Incident Response Testing Not Consistently Documented	**MEDIUM**
HIPAA Reference: 45 CFR §164.308(a)(6)(i)-(ii)	**Illustrative Assessment Status: Partially In Place**
Control Objective	NovaCura implements policies and procedures to identify, respond to, mitigate, and document security incidents affecting ePHI, and periodically exercises those procedures to confirm their effectiveness.
Criteria	45 CFR §164.308(a)(6) requires policies and procedures to address security incidents, including identification, response, mitigation, and documentation of outcomes. NovaCura's internal Incident Response Plan commits to an annual tabletop exercise as organizational policy; this cadence is an internal commitment and is not itself a specific numeric HIPAA requirement.
Condition	NovaCura's Incident Response Plan (EV-012) is current and assigns clear roles across security, legal, privacy, and communications functions. A sample review found that the most recent documented tabletop exercise was performed approximately 19 fictional months prior to the assessment date, exceeding NovaCura's own defined annual cadence.

Cause	Ownership of scheduling the annual tabletop exercise was not formally assigned to a single role following a fictional 2025 reorganization of the security team.
Risk / Business Impact	Extended gaps between incident response exercises increase the risk that plan assumptions, contact lists, or escalation paths are outdated when a real security incident occurs, potentially slowing containment and the breach risk assessment process described in Section 15.
Evidence Reference	*EV-012 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Formally assign ownership of the annual incident response tabletop exercise to the Incident Response Manager, schedule the next exercise within 60 days, and incorporate lessons learned into the Incident Response Plan.
Management Response	*Agreed. Ownership has been assigned and the next tabletop exercise will be scheduled within 60 days.*
Owner / Target Date / Status	**Incident Response Manager** | 15 Nov 2026 | **Open**

HIPAA-BKP-007 — Backup Restoration Testing Not Performed on Defined Cycle	**MEDIUM**
HIPAA Reference: 45 CFR §164.308(a)(7)(ii)(A)/(D)	**Illustrative Assessment Status: Partially In Place**
Control Objective	ePHI is backed up on a defined cycle, and backup restoration procedures are periodically tested to confirm data can be recovered accurately and within an acceptable timeframe.
Criteria	45 CFR §164.308(a)(7)(ii)(A) requires a data backup plan to create and maintain retrievable exact copies of ePHI; the testing and revision procedures implementation specification at §164.308(a)(7)(ii)(D) is addressable, and NovaCura has adopted quarterly restoration testing as its own internal contingency-plan standard implementing that specification.
Condition	Backup jobs for in-scope ePHI systems were confirmed as completing successfully on schedule. Restoration testing records, however, evidenced two of the four fictional quarterly test cycles within the assessment period for the specialty pharmacy database; the CRM platform's backup restoration had not been tested during the assessment period.
Cause	Restoration testing for the CRM platform depends on a maintenance window coordinated with the platform's managed-hosting business associate, which was not scheduled during the assessment period.
Risk / Business Impact	Untested backup restoration procedures create uncertainty as to whether ePHI could be recovered accurately and within an acceptable timeframe following a ransomware event, system failure, or other contingency, directly affecting NovaCura's emergency mode operation capability.
Evidence Reference	*EV-013 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Coordinate and complete a CRM platform restoration test with the managed-hosting business associate, complete the outstanding specialty pharmacy restoration test cycles, and formalize restoration testing as a scheduled, tracked activity across all in-scope systems.
Management Response	*Agreed. Restoration testing will be scheduled and completed for all in-scope systems, including coordination with the managed-hosting business associate for the CRM platform.*
Owner / Target Date / Status	**Backup & Infrastructure Manager** | 15 Nov 2026 | **Open**

HIPAA-TRN-008 — Workforce HIPAA Training Completion Not Fully Tracked	**MEDIUM**
HIPAA Reference: 45 CFR §164.308(a)(5)(i)	**Illustrative Assessment Status: Partially In Place**
Control Objective	All workforce members, including management, complete security awareness and HIPAA training appropriate to their role, on a periodic basis, with completion tracked and evidenced.
Criteria	45 CFR §164.308(a)(5)(i) requires implementation of a security awareness and training program for all workforce members, including management. NovaCura's internal training policy commits to annual completion for all workforce members and role-based supplemental training for personnel handling ePHI directly.
Condition	Enterprise annual HIPAA and security awareness training completion was evidenced at approximately 91% of the fictional 1,250-person workforce as of the assessment date. Role-based supplemental privacy/security training for patient-support and pharmacy fulfillment staff, however, was tracked in a separate departmental spreadsheet that had not been reconciled with the central learning management system, and completion status for that supplemental training could not be fully confirmed for a sampled department.

Cause	Role-based supplemental training is administered outside the central learning management system for a subset of departments, creating a fragmented tracking process.
Risk / Business Impact	Incomplete training completion tracking limits NovaCura's ability to confirm that workforce members handling ePHI directly have completed role-appropriate training, and complicates the sanction policy process described in Section 11 for confirmed non-completion.
Evidence Reference	*EV-014 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Migrate all role-based supplemental training tracking into the central learning management system, close the outstanding completion gap for the sampled department, and report enterprise-wide and role-based completion rates to management quarterly.
Management Response	*Agreed. Supplemental training tracking will be consolidated into the central learning management system and completion gaps closed.*
Owner / Target Date / Status	**Training & Awareness Lead** | 15 Nov 2026 | **Open**

HIPAA-PRV-010 — Minimum Necessary Standard Not Consistently Applied in CRM Access Provisioning	**MEDIUM**
HIPAA Reference: 45 CFR §164.502(b) / §164.514(d)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Access to PHI within the patient-support CRM is provisioned consistent with the minimum necessary standard, limiting workforce access to the PHI reasonably necessary to carry out each role's function.
Criteria	45 CFR §164.502(b) and §164.514(d) require covered entities to make reasonable efforts to limit PHI access, use, and disclosure to the minimum necessary to accomplish the intended purpose, including through role-based access provisioning.
Condition	A sample review of CRM access provisioning found that a broad "Patient Support — General" role, assigned to approximately 60% of sampled CRM users, provided visibility into full patient case history rather than the subset of fields relevant to each user's specific support function, for three of five sampled sub-teams.
Cause	The CRM's role model was originally built around functional department rather than the specific data fields each sub-team requires, and has not been revisited since the patient-support function was reorganized into specialized sub-teams.
Risk / Business Impact	Overly broad CRM role design increases the population of workforce members with access to PHI beyond what is necessary for their specific function, expanding the potential impact of workforce error, insider misuse, or account compromise.
Evidence Reference	*EV-015 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Redesign the CRM role model to align with minimum-necessary access for each patient-support sub-team, re-provision affected users under the refined roles, and incorporate a minimum-necessary review checkpoint into future CRM role changes.
Management Response	*Agreed. The CRM role model will be redesigned around minimum-necessary principles for each sub-team and affected users re-provisioned accordingly.*
Owner / Target Date / Status	**Data Governance Lead** | 15 Dec 2026 | **Open**

HIPAA-BRN-011 — Breach Risk Assessment Documentation Incomplete for Sampled Security Events	**MEDIUM**
HIPAA Reference: 45 CFR §164.402 / §164.404–408	**Illustrative Assessment Status: Partially In Place**
Control Objective	Following any impermissible use or disclosure of PHI, NovaCura performs and documents a four-factor breach risk assessment to determine whether a reportable breach has occurred, and completes any required notification within applicable timeframes.

Criteria	45 CFR §164.402 defines breach and the four-factor risk assessment (nature and extent of PHI involved, unauthorized recipient, whether PHI was actually acquired or viewed, and extent of mitigation); §§164.404–408 govern individual, media, and HHS notification timeframes once a breach determination is made.
Condition	Of four fictional sampled security events logged as potential PHI exposures during the assessment period, three had a documented four-factor risk assessment on file; one sampled event — a misdirected fax containing PHI for a single fictional patient — was resolved informally with a documented mitigation call to the recipient, but the four-factor assessment itself was not separately documented.
Cause	Lower-severity, single-patient events are sometimes handled directly by the department involved without being formally routed through the documented breach risk assessment workflow.
Risk / Business Impact	Undocumented breach risk assessments — even for events ultimately determined not to be reportable — weaken NovaCura's evidentiary record of its breach determination process and could complicate demonstrating a defensible, good-faith risk assessment if the same event pattern were later questioned by OCR.
Evidence Reference	*EV-016 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Require every PHI-involving security event, regardless of apparent severity, to be routed through the documented four-factor breach risk assessment workflow, and complete a retrospective documented assessment for the sampled fax event.
Management Response	*Agreed. All PHI-involving events, including lower-severity events, will be routed through the documented breach risk assessment workflow going forward.*
Owner / Target Date / Status	**Privacy Officer** | 30 Nov 2026 | **Open**

HIPAA-VUL-012 — Vulnerability Remediation Exceptions Not Formally Tracked	**MEDIUM**
HIPAA Reference: 45 CFR §164.308(a)(1)(ii)(B)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Vulnerabilities identified across ePHI-relevant systems are prioritized and remediated (or formally accepted as an exception with compensating controls) consistent with NovaCura's own risk-based vulnerability management program.
Criteria	The HIPAA Security Rule does not itself specify a numeric vulnerability remediation deadline; §164.308(a)(1)(ii)(B) requires risk management measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. NovaCura has adopted internal SLA-based remediation timeframes (organizational policy) as one of the risk-based measures implementing that requirement.
Condition	A sample review of the vulnerability management tracker found that 14% of open vulnerabilities affecting ePHI-relevant systems had exceeded NovaCura's internal SLA remediation timeframe. Of those, a subset lacked a documented formal exception, compensating control, or revised target date, appearing instead as simply overdue with no recorded rationale.
Cause	The vulnerability management platform supports a formal exception workflow, but its use is not currently mandatory, allowing overdue items to remain open without a documented risk decision.
Risk / Business Impact	Overdue vulnerabilities without a documented risk decision or compensating control represent unmanaged risk to ePHI-relevant systems and limit management's visibility into the organization's true risk-acceptance posture.
Evidence Reference	*EV-017 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Require every vulnerability exceeding the internal SLA to have either completed remediation, a documented compensating control, or a formally approved exception with a defined review date, and report aggregate SLA performance to the Security Steering Committee monthly.
Management Response	*Agreed. Mandatory exception workflow will be enforced for all SLA-exceeding vulnerabilities on ePHI-relevant systems.*
Owner / Target Date / Status	**Vulnerability Management Lead** | 15 Dec 2026 | **Open**

HIPAA-PHY-009 — Workstation Physical Safeguard Gaps at Remote / Field-Based Sites	**LOW**
HIPAA Reference: 45 CFR §164.310(b) / §164.310(c)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Workstations that access ePHI, including those used by field-based patient-support personnel, are physically safeguarded against unauthorized viewing or access, consistent with NovaCura's workstation use and security policies.

Criteria	45 CFR §164.310(b) and (c) require policies and procedures governing the proper functions to be performed on workstations that access ePHI and physical safeguards restricting access to authorized users.
Condition	A sample review of field-based patient-support personnel found documented workstation-use policy acknowledgement for all sampled personnel; however, two of eight sampled home-office workstation setups, reviewed through a fictional self-assessment checklist submitted by the employee, did not evidence use of a privacy screen or a documented alternative safeguard despite regular ePHI viewing.
Cause	Privacy screen provisioning for field-based and home-office personnel is requested on an opt-in basis rather than being a default component of the remote-work equipment package.
Risk / Business Impact	The absence of a privacy screen or equivalent safeguard in a home or shared-space environment increases the risk of incidental ePHI viewing by unauthorized individuals such as household members or visitors.
Evidence Reference	*EV-018 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Include a privacy screen as a default component of the standard remote-work equipment package for all personnel with regular ePHI access, and close the gap for the two sampled workstations.
Management Response	*Agreed. Privacy screens will be issued by default with remote-work equipment for all ePHI-accessing personnel.*
Owner / Target Date / Status	**Facilities & IT Asset Manager** | 15 Dec 2026 | **Open**

HIPAA-AUD-013 — Audit Log Review Cadence Inconsistent Across ePHI Systems	**LOW**
HIPAA Reference: 45 CFR §164.312(b)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Hardware, software, and procedural mechanisms record and examine activity in information systems that contain or use ePHI, consistent with NovaCura's own defined audit log review cadence for each system.
Criteria	45 CFR §164.312(b) requires the implementation of hardware, software, and/or procedural mechanisms to record and examine activity in information systems containing or using ePHI. HIPAA does not itself prescribe a specific review frequency; NovaCura's internal Logging & Monitoring Standard defines system-specific review cadences based on data sensitivity and criticality.
Condition	The specialty pharmacy system and patient portal were confirmed as reviewed on their defined weekly cadence. The CRM platform's audit logs, defined internally as a bi-weekly review item, were found to have been reviewed on an approximately monthly cadence during the assessment period.
Cause	The CRM platform's audit log review is performed manually by a rotating analyst assignment that has not consistently kept pace with the defined bi-weekly schedule.
Risk / Business Impact	A slower-than-defined audit log review cadence for the CRM platform increases the time to detect anomalous or unauthorized PHI access within that system.
Evidence Reference	*EV-007 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Reassign CRM audit log review to a fixed analyst with a defined backup, and configure automated review-completion reminders consistent with the defined bi-weekly cadence.
Management Response	*Agreed. CRM audit log review ownership will be fixed and automated reminders configured to enforce the bi-weekly cadence.*
Owner / Target Date / Status	**Security Operations Manager** | 15 Dec 2026 | **Open**

HIPAA-ACC-014 — Automatic Logoff Configuration Inconsistent Across Clinical Applications	**LOW**
HIPAA Reference: 45 CFR §164.312(a)(2)(iii)	**Illustrative Assessment Status: Partially In Place**
Control Objective	Sessions on systems that access ePHI automatically terminate after a defined period of inactivity, consistent with NovaCura's addressable-specification determination and internal session-timeout standard.
Criteria	45 CFR §164.312(a)(2)(iii) identifies automatic logoff as an addressable implementation specification. NovaCura's risk analysis determined a 15-minute inactivity timeout to be reasonable and appropriate and adopted it as an internal standard applicable to all ePHI-accessing applications.

Condition	The patient portal administrative console and specialty pharmacy application enforced the defined 15-minute timeout. The clinical coordination application, reviewed as part of the sample, was configured with a 45-minute inactivity timeout that had not been updated to reflect the current internal standard.
Cause	The clinical coordination application's session-timeout configuration is managed by its vendor and was not included in the most recent internal standard rollout communicated to application owners.
Risk / Business Impact	A longer-than-standard inactivity timeout increases the window during which an unattended, authenticated session could be used by an unauthorized individual to view or act on ePHI.
Evidence Reference	*EV-001 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Update the clinical coordination application's session-timeout configuration to align with the internal 15-minute standard, and confirm the standard has been communicated to and applied by all ePHI-application owners.
Management Response	*Agreed. The clinical coordination application's timeout configuration will be updated and the standard reconfirmed with all application owners.*
Owner / Target Date / Status	**Application Security Lead** | 15 Dec 2026 | **Open**

HIPAA-DOC-015 — Policy Review and Update Documentation Gaps	**LOW**
HIPAA Reference: 45 CFR §164.316(a) / §164.316(b)(1)	**Illustrative Assessment Status: Partially In Place**
Control Objective	NovaCura's HIPAA Security and Privacy policies are documented, periodically reviewed, and updated as needed in response to environmental or operational changes, consistent with §164.316.
Criteria	45 CFR §164.316(a) requires implementation of reasonable and appropriate policies and procedures; §164.316(b)(1) requires documentation of those policies, and periodic review and update as needed. NovaCura's internal Policy Governance Standard commits to an annual review cycle for all HIPAA-related policies.
Condition	A sample review of NovaCura's 22 HIPAA-related policy documents found four policies — including the Remote Access Standard and the Third-Party Risk Management Policy — with a documented last-review date exceeding the internal annual review cycle by approximately four to seven fictional months.
Cause	Policy review ownership is distributed across multiple functional leads without a centralized policy governance calendar or escalation process for overdue reviews.
Risk / Business Impact	Policies that are not reviewed on the defined cycle risk becoming misaligned with current operational practice, increasing the likelihood of a gap between documented procedure and actual control performance.
Evidence Reference	*EV-001 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Complete the outstanding reviews for the four identified policies, and implement a centralized policy governance calendar with automated escalation for any policy approaching its review due date.
Management Response	*Agreed. Outstanding policy reviews will be completed and a centralized policy governance calendar implemented.*
Owner / Target Date / Status	**Policy & Documentation Manager** | 15 Dec 2026 | **Open**

HIPAA-MFA-016 — Multi-Factor Authentication Not Enforced on All Remote Access Paths	**OBSERVATION**
HIPAA Reference: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	Remote access paths to ePHI-relevant systems are protected by authentication mechanisms appropriate to the risk determined through NovaCura's risk analysis.
Criteria	45 CFR §164.312(d) requires procedures to verify that a person or entity seeking access to ePHI is the one claimed; it does not by name require multi-factor authentication (MFA). NovaCura's own risk analysis and Remote Access Standard identify MFA as the organization's chosen risk-based control for satisfying this requirement on primary remote access paths. Because this item concerns a specific technical control implementation choice rather than a directly cited Security Rule deficiency, it is reported as an internal security observation.

Condition	MFA was confirmed as enforced for the primary VPN and single sign-on gateway used by the large majority of NovaCura's workforce. One legacy remote-access path, used by a small number of specialty pharmacy operations staff to reach an older internal scheduling tool, was found to rely on username/password authentication only.
Cause	The legacy scheduling tool's remote-access path was provisioned prior to the current Remote Access Standard and has not yet been migrated behind the primary SSO/MFA gateway.
Risk / Business Impact	The legacy path represents a narrower authentication control than NovaCura's own risk-based standard calls for; it does not itself constitute a Security Rule citation but is a security-maturity gap relative to the organization's own defined control objective.
Evidence Reference	*EV-006 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Migrate the legacy scheduling tool's remote-access path behind the primary SSO/MFA gateway, or formally document a risk-based compensating control if migration is not feasible within the current environment.
Management Response	*Agreed. The legacy scheduling tool's remote-access path will be migrated behind the primary SSO/MFA gateway.*
Owner / Target Date / Status	**Identity & Access Engineering Lead** | 15 Dec 2026 | **Open**

HIPAA-RET-017 — Documentation Retention Tracking Not Centralized	**OBSERVATION**
HIPAA Reference: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	HIPAA-related documentation, including policies, risk analyses, training records, and security incident documentation, is retained consistent with §164.316(b)(2)'s six-year retention requirement and is readily retrievable.
Criteria	45 CFR §164.316(b)(2)(i) requires HIPAA-related documentation to be retained for six years from the date of creation or the date it was last in effect, whichever is later. During this sample review, all sampled documentation categories were confirmed as retained within the required window; retention tracking itself, however, is performed department-by-department rather than through a single centralized schedule, which this assessment treats as a security-maturity observation rather than a compliance gap, since no retention shortfall was identified.
Condition	No instance of documentation retained short of the six-year requirement was identified in the fictional sample reviewed. Retention responsibility and destruction-eligibility tracking, however, are distributed across department-level spreadsheets rather than a single, centrally governed retention schedule.
Cause	A centralized records retention platform has not yet been extended to cover all HIPAA-related documentation categories across departments.
Risk / Business Impact	Decentralized retention tracking increases the future risk of an inadvertent early-destruction or over-retention error as institutional knowledge of department-level spreadsheets changes over time, even though no current shortfall was observed.
Evidence Reference	*EV-001 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Extend the centralized records retention platform to cover all HIPAA-related documentation categories and formally retire department-level retention tracking spreadsheets.
Management Response	*Agreed. HIPAA-related documentation retention will be consolidated into the centralized records retention platform.*
Owner / Target Date / Status	**Records Management Lead** | 31 Dec 2026 | **Open**

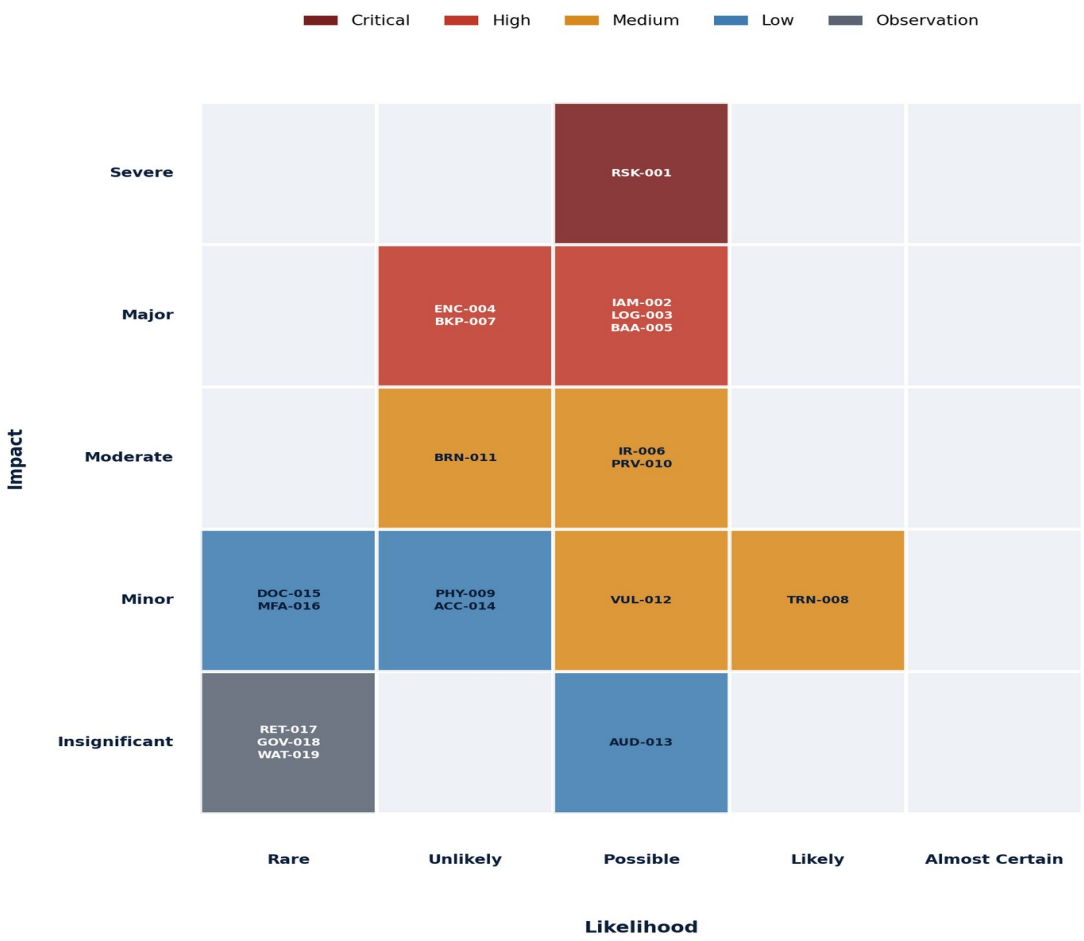
HIPAA-GOV-018 — Assigned Security Responsibility Documentation Not Current	**OBSERVATION**
HIPAA Reference: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	A security official responsible for the development and implementation of NovaCura's Security Rule policies and procedures is formally identified and documented, consistent with §164.308(a)(2).
Criteria	45 CFR §164.308(a)(2) requires identification of the security official responsible for developing and implementing the required security policies and procedures. NovaCura has formally identified its Chief Information Security Officer as the designated security official; this item concerns the currency of the supporting documentation rather than the designation itself, so it is reported as an internal governance observation.

Condition	The CISO's designation as security official was confirmed as accurate and current. The formal designation memorandum on file, however, still referenced the organization's prior security team structure predating a fictional 2025 reorganization, and had not been reissued to reflect current reporting lines and delegated responsibilities.
Cause	Updating the designation memorandum was not included as a required step in the 2025 security team reorganization project plan.
Risk / Business Impact	An outdated designation memorandum does not affect the validity of the current designation but represents a documentation-currency gap that could create ambiguity if referenced during a future review or investigation.
Evidence Reference	*EV-001 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Reissue the security official designation memorandum to reflect current reporting lines and delegated responsibilities, and add a documentation-currency checkpoint to future organizational changes affecting the security function.
Management Response	*Agreed. The designation memorandum will be reissued to reflect the current organizational structure.*
Owner / Target Date / Status	**Security Governance Lead** | 31 Dec 2026 | **Open**

HIPAA-WAT-019 — Technology Asset Inventory Maturity Gap — Future Regulatory Readiness Observation	**OBSERVATION**
HIPAA Reference: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	NovaCura maintains a current, complete technology asset inventory sufficient to support its risk analysis and to position the organization for anticipated future HIPAA Security Rule expectations regarding asset inventory and network mapping.
Criteria	The current HIPAA Security Rule does not mandate a specific technology asset inventory or network-mapping deliverable as a standalone requirement; an accurate risk analysis under §164.308(a)(1)(ii)(A) nonetheless depends on knowing what systems exist. HHS/OCR's December 2024 proposed Security Rule modernization (see Section 34, Regulatory Watch) would introduce more explicit asset inventory and network mapping expectations; those proposed provisions are not current mandatory requirements and are not scored as a compliance gap here.
Condition	NovaCura maintains an asset inventory covering core infrastructure and centrally managed endpoints. A fictional sample comparison against the cloud environment's resource tagging found a small number of analytics-environment resources not yet reflected in the central asset inventory, though they were confirmed as within existing network security monitoring.
Cause	Cloud resource provisioning for the analytics environment does not currently trigger an automatic asset-inventory registration step.
Risk / Business Impact	This gap did not result in an unmonitored or unprotected asset in this fictional sample, but reduces the completeness of the asset inventory that underpins the enterprise risk analysis, and represents an area of proactive readiness relative to the proposed 2024 Security Rule modernization's asset inventory and network mapping concepts.
Evidence Reference	*EV-004 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement automated asset-inventory registration for newly provisioned cloud resources, and periodically reconcile the central asset inventory against cloud resource tagging as a forward-looking readiness measure.
Management Response	*Agreed. Automated asset registration will be implemented for the cloud environment and periodic reconciliation performed.*
Owner / Target Date / Status	**IT Asset Management Lead** | 31 Dec 2026 | **Open**

27 RISK HEATMAP

The 5×5 risk matrix below maps all 19 fictional findings and observations from this sample assessment by Likelihood and Impact, consistent with the rating methodology introduced in Section 17. Likelihood ranges from Rare to Almost Certain; Impact ranges from Insignificant to Severe. Cell shading reflects the highest severity finding mapped to that cell.



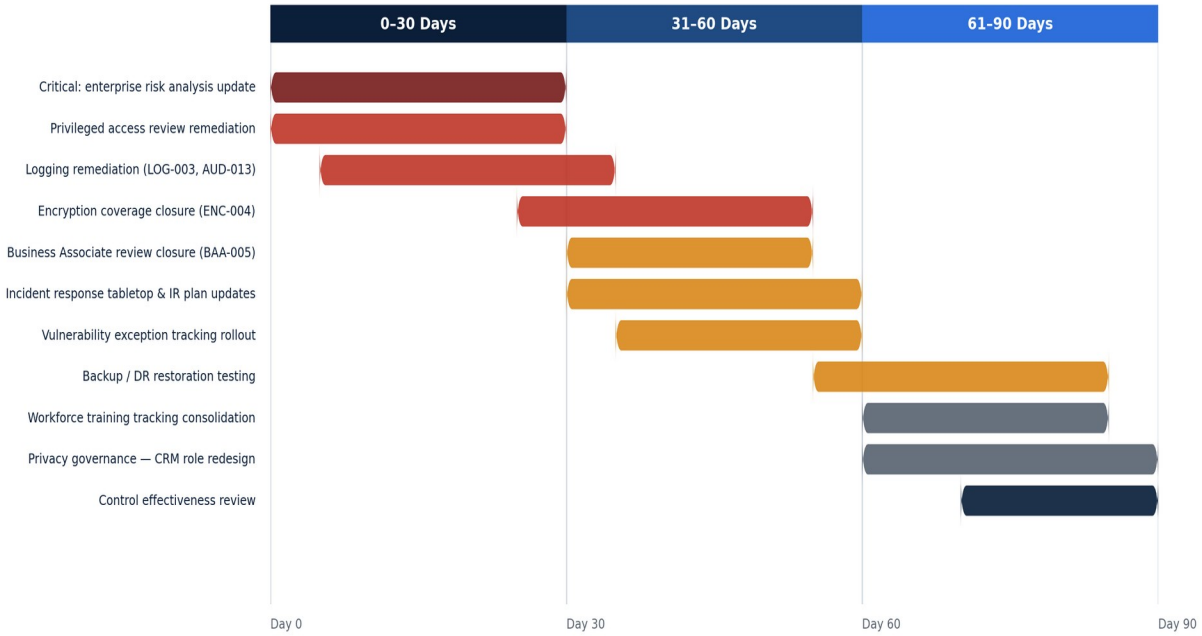
Illustrative 5×5 Risk Heatmap — Fictional Findings, Mapped by Likelihood × Impact

How to Read the Heatmap

- Upper-right cells (higher likelihood, higher impact) represent the fictional findings warranting the most urgent remediation attention, led by HIPAA-RSK-001 in the Possible / Severe cell.
- Lower-left cells represent lower-urgency observations, several of which are reported as internal security-maturity observations rather than direct compliance gaps.
- The heatmap is a visualization aid; the authoritative severity rating for each finding is presented in Section 26 (Detailed Findings) and Section 32 (Finding Register).

28 90-DAY REMEDIATION ROADMAP

The fictional remediation roadmap below sequences remediation activity across a 90-day window, prioritizing the critical- and high-severity sample findings for early closure. All dates and timelines shown are illustrative.



Illustrative 90-Day Remediation Roadmap — Fictional Timeline

0–30 Days

- Address the critical-severity finding: begin the enterprise-wide ePHI risk analysis update (HIPAA-RSK-001).
- Complete the privileged access review remediation and centralize recertification tracking (HIPAA-IAM-002).
- Close the high-risk logging remediation: assign backup reviewer and restore CRM audit review cadence (HIPAA-LOG-003, HIPAA-AUD-013).

31–60 Days

- Close the portable-device encryption coverage gap (HIPAA-ENC-004).
- Complete overdue Business Associate security reviews (HIPAA-BAA-005).
- Deliver incident response tabletop exercise and Contingency Plan improvements (HIPAA-IR-006, HIPAA-BKP-007).
- Complete vulnerability remediation exception tracking rollout (HIPAA-VUL-012).

61–90 Days

- Complete disaster recovery / backup restoration testing across all in-scope systems (HIPAA-BKP-007).
- Deliver workforce training tracking consolidation and completion closure (HIPAA-TRN-008).
- Complete privacy governance remediation: CRM minimum-necessary role redesign (HIPAA-PRV-010).
- Complete control effectiveness review across remaining low-severity findings and observations.

29 MANAGEMENT ACTION PLAN

NovaCura's fictional management team has reviewed and formally accepted each sample finding below, with defined ownership and target remediation dates. This table is synchronized with the Detailed Findings section (Section 26) and the Finding Register (Section 32).

Finding ID	Management Response	Owner	Target Date	Priority	Status
HIPAA-RSK-001	Agreed. NovaCura will commission an updated enterprise-wide risk analysis covering all current ePHI systems and will formalize a recurring refresh trigger tied to the change management process.	Chief Information Security Officer	15 Oct 2026	Priority 0	Open
HIPAA-IAM-002	Agreed. NovaCura will implement centralized recertification tracking	IAM Program Manager	30 Oct 2026	Priority 1	Open

Finding ID	Management Response	Owner	Target Date	Priority	Status
	and require documented sign-off for all in-scope systems beginning with the next semi-annual cycle.				
HIPAA-LOG-003	Agreed. A backup reviewer will be assigned and checklist completion will be tracked automatically within the SIEM platform going forward.	SOC Manager	15 Oct 2026	Priority 1	Open
HIPAA-ENC-004	Agreed. All legacy field devices will be re-enrolled in MDM and encryption status verified and remediated where required.	IT Endpoint Security Lead	30 Oct 2026	Priority 1	Open
HIPAA-BAA-005	Agreed. Overdue reviews will be completed and business associate review tracking will move to the centralized GRC platform with automated scheduling.	Third-Party Risk Manager	30 Nov 2026	Priority 1	Open
HIPAA-IR-006	Agreed. Ownership has been assigned and the next tabletop exercise will be scheduled within 60 days.	Incident Response Manager	15 Nov 2026	Priority 2	Open
HIPAA-BKP-007	Agreed. Restoration testing will be scheduled and completed for all in-scope systems, including coordination with the managed-hosting business associate for the CRM platform.	Backup & Infrastructure Manager	15 Nov 2026	Priority 2	Open
HIPAA-TRN-008	Agreed. Supplemental training tracking will be consolidated into the central learning management system and completion gaps closed.	Training & Awareness Lead	15 Nov 2026	Priority 2	Open
HIPAA-PRV-010	Agreed. The CRM role model will be redesigned around minimum-necessary principles for each sub-team and affected users re-provisioned accordingly.	Data Governance Lead	15 Dec 2026	Priority 2	Open
HIPAA-BRN-011	Agreed. All PHI-involving events, including lower-severity events, will be routed through the documented breach risk assessment workflow going forward.	Privacy Officer	30 Nov 2026	Priority 2	Open
HIPAA-VUL-012	Agreed. Mandatory exception workflow will be enforced for all SLA-exceeding vulnerabilities on ePHI-relevant systems.	Vulnerability Management Lead	15 Dec 2026	Priority 2	Open
HIPAA-PHY-009	Agreed. Privacy screens will be issued by default with remote-work equipment for all ePHI-accessing personnel.	Facilities & IT Asset Manager	15 Dec 2026	Priority 3	Open
HIPAA-AUD-013	Agreed. CRM audit log review ownership will be fixed and automated reminders configured to enforce the bi-weekly cadence.	Security Operations Manager	15 Dec 2026	Priority 3	Open
HIPAA-ACC-014	Agreed. The clinical coordination application's timeout configuration will be updated and the standard reconfirmed with all application owners.	Application Security Lead	15 Dec 2026	Priority 3	Open
HIPAA-DOC-015	Agreed. Outstanding policy reviews will be completed and a centralized policy governance calendar implemented.	Policy & Documentation Manager	15 Dec 2026	Priority 3	Open
HIPAA-MFA-016	Agreed. The legacy scheduling tool's remote-access path will be migrated behind the primary SSO/MFA gateway.	Identity & Access Engineering Lead	15 Dec 2026	Priority 4	Open
HIPAA-RET-017	Agreed. HIPAA-related documentation retention will be consolidated into the centralized records retention platform.	Records Management Lead	31 Dec 2026	Priority 4	Open
HIPAA-GOV-018	Agreed. The designation memorandum will be reissued to reflect the current organizational structure.	Security Governance Lead	31 Dec 2026	Priority 4	Open
HIPAA-WAT-019	Agreed. Automated asset registration will be implemented for the cloud environment and periodic reconciliation performed.	IT Asset Management Lead	31 Dec 2026	Priority 4	Open

30 FINAL ASSESSMENT & CONCLUSION

Based on the fictional evidence and simulated procedures described in this report, NovaCura Health & Pharmaceuticals, Inc.'s environment is presented with an overall Illustrative Assessment Status of PARTIALLY IN PLACE for demonstration purposes.

This status is illustrative only. It is not an official HIPAA compliance determination, OCR audit outcome, certification, or attestation of any kind.

Executive Conclusion

This fictional assessment demonstrates that NovaCura maintains a reasonable baseline HIPAA compliance and security program: documented Administrative, Physical, and Technical Safeguards policies, a mature Privacy Rule program, a well-designed Breach Notification workflow, and executed Business Associate Agreements across all sampled third-party relationships. Material fictional improvement opportunities exist around the completeness of the enterprise-wide ePHI risk analysis, the consistency of access governance and audit control evidence, third-party security review currency, incident response exercising, and ePHI protection on legacy portable devices.

None of the fictional findings in this report indicate an absent HIPAA safeguards program; rather, they reflect documentation, consistency, and coverage gaps within an otherwise-designed program — the pattern TMG Security

most frequently identifies in real-world HIPAA readiness engagements. NovaCura is not represented as HIPAA certified as a result of this report; HIPAA does not provide for a formal government-issued certification, and this document does not constitute or substitute for an OCR audit, investigation, or compliance determination.

This conclusion, and every element of this report, is fictional and produced solely to demonstrate TMG Security's assessment methodology and reporting standards. It does not describe the actual security or compliance posture of any real organization.

31 EVIDENCE REGISTER

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

The register below lists every fictional evidence reference (EV-xxx) cited throughout this sample report. Each item is an illustrative placeholder used solely to demonstrate TMG Security's evidence referencing convention; no actual NovaCura documents, configurations, or artifacts were collected, reviewed, or retained.

Reference	Evidence Description	Type	Illustrative Owner
EV-001	HIPAA Security Policies	Policy	Compliance Officer
EV-002	Enterprise Risk Analysis	Risk Assessment	Chief Information Security Officer
EV-003	ePHI Data Flow Diagram	Diagram	Security Governance Lead
EV-004	Asset Inventory	Register	IT Asset Management Lead
EV-005	IAM Access Review	Access Records	IAM Program Manager
EV-006	MFA Configuration	Configuration Export	Identity & Access Engineering Lead
EV-007	SIEM Configuration	Configuration Export	SOC Manager
EV-008	EDR Configuration	Configuration Export	Security Operations Manager
EV-009	Encryption Standards	Standard / Configuration Export	IT Endpoint Security Lead
EV-010	Business Associate Register	Register	Third-Party Risk Manager
EV-011	BAA Samples	Contract Records	Third-Party Risk Manager
EV-012	Incident Response Plan	Program Records	Incident Response Manager
EV-013	Backup / Recovery Records	Operational Records	Backup & Infrastructure Manager
EV-014	Workforce Training Records	Training Records	Training & Awareness Lead
EV-015	Privacy Policies	Policy	Privacy Officer
EV-016	Breach Response Procedure	Procedure	Privacy Officer
EV-017	Vulnerability Reports	Scan Report	Vulnerability Management Lead
EV-018	Physical Security Procedures	Procedure	Facilities & IT Asset Manager
EV-019	Disaster Recovery Test	Test Report	Backup & Infrastructure Manager
EV-020	Privacy Complaint Records	Program Records	Privacy Officer

32 FINDING REGISTER

Illustrative Assessment Status reflects the sampled control condition underlying each finding; Remediation Status reflects fictional tracking of the corrective action itself. Both are synchronized with Section 25, Section 26, and Section 29.

ID	Title	Severity	HIPAA Reference	Illustrative Assessment Status	Remediation Status
HIPAA-RSK-001	Incomplete Enterprise-Wide ePHI Risk Analysis	CRITICAL	45 CFR §164.308(a)(1)(ii)(A)	Not In Place	Open
HIPAA-IAM-002	Privileged Access Review Evidence Incomplete	HIGH	45 CFR §164.308(a)(4)(ii)(C)	Partially In Place	Open
HIPAA-LOG-003	Information System Activity Review Not Consistently Documented	HIGH	45 CFR §164.308(a)(1)(ii)(D)	Partially In Place	Open
HIPAA-ENC-004	Encryption Coverage Gap on Selected Portable Devices	HIGH	45 CFR §164.312(a)(2)(iv)	Partially In Place	Open
HIPAA-BAA-005	Business Associate Security Review Evidence Incomplete	HIGH	45 CFR §164.308(b)(1) / §164.314(a)(1)	Partially In Place	Open
HIPAA-IR-006	Security Incident Response Testing Not Consistently Documented	MEDIUM	45 CFR §164.308(a)(6)(i)-(ii)	Partially In Place	Open
HIPAA-BKP-007	Backup Restoration Testing Not Performed	MEDIUM	45 CFR §164.308(a)(7)(ii)(A)/(D)	Partially In Place	Open

ID	Title	Severity	HIPAA Reference	Illustrative Assessment Status	Remediation Status
	on Defined Cycle				
HIPAA-TRN-008	Workforce HIPAA Training Completion Not Fully Tracked	MEDIUM	45 CFR §164.308(a)(5)(i)	Partially In Place	Open
HIPAA-PRV-010	Minimum Necessary Standard Not Consistently Applied in CRM Access Provisioning	MEDIUM	45 CFR §164.502(b) / §164.514(d)	Partially In Place	Open
HIPAA-BRN-011	Breach Risk Assessment Documentation Incomplete for Sampled Security Events	MEDIUM	45 CFR §164.402 / §164.404–408	Partially In Place	Open
HIPAA-VUL-012	Vulnerability Remediation Exceptions Not Formally Tracked	MEDIUM	45 CFR §164.308(a)(1)(ii)(B)	Partially In Place	Open
HIPAA-PHY-009	Workstation Physical Safeguard Gaps at Remote / Field-Based Sites	LOW	45 CFR §164.310(b) / §164.310(c)	Partially In Place	Open
HIPAA-AUD-013	Audit Log Review Cadence Inconsistent Across ePHI Systems	LOW	45 CFR §164.312(b)	Partially In Place	Open
HIPAA-ACC-014	Automatic Logoff Configuration Inconsistent Across Clinical Applications	LOW	45 CFR §164.312(a)(2)(iii)	Partially In Place	Open
HIPAA-DOC-015	Policy Review and Update Documentation Gaps	LOW	45 CFR §164.316(a) / §164.316(b)(1)	Partially In Place	Open
HIPAA-MFA-016	Multi-Factor Authentication Not Enforced on All Remote Access Paths	OBSERVATION	Not directly applicable — Informational	Observation	Open
HIPAA-RET-017	Documentation Retention Tracking Not Centralized	OBSERVATION	Not directly applicable — Informational	Observation	Open
HIPAA-GOV-018	Assigned Security Responsibility Documentation Not Current	OBSERVATION	Not directly applicable — Informational	Observation	Open
HIPAA-WAT-019	Technology Asset Inventory Maturity Gap — Future Regulatory Readiness Observation	OBSERVATION	Not directly applicable — Informational	Observation	Open

33 HIPAA CONTROL MATRIX

The matrix below maps every Administrative, Physical, Technical, Organizational, and Policies/Documentation standard under 45 CFR §§164.308, 164.310, 164.312, 164.314, and 164.316, together with applicable Privacy Rule and Breach Notification Rule areas, to NovaCura's fictional illustrative status, supporting evidence, and any related finding.

Citation	Control Area	Control Objective	Illustrative Status	Evid.	Finding	Recommended Action
§164.308(a)(1)	Security Management Process	Risk Analysis	Not In Place	EV-002	HIPAA-RSK-001	Update enterprise risk analysis; add refresh trigger to onboarding.
§164.308(a)(1)	Security Management Process	Risk Management	Partially In Place	EV-017	HIPAA-VUL-012	Enforce mandatory exception workflow for overdue vulnerabilities.
§164.308(a)(1)	Security Management Process	Sanction Policy	In Place	EV-001	—	Maintain current sanction policy and enforcement records.
§164.308(a)(1)	Security Management Process	Information System Activity Review	Partially In Place	EV-007	HIPAA-LOG-003	Assign backup reviewer; automate checklist tracking.
§164.308(a)(2)	Assigned Security Responsibility	Security Official Designation	Partially In Place	EV-001	HIPAA-GOV-018	Reissue designation memorandum to reflect current structure.
§164.308(a)(3)	Workforce Security	Authorization / Supervision, Clearance, Termination	In Place	EV-005	—	Maintain current workforce security procedures.
§164.308(a)(4)	Information Access Management	Access Authorization / Establishment & Modification	Partially In Place	EV-005	HIPAA-IAM-002	Centralize privileged access recertification tracking.
§164.308(a)(5)	Security Awareness and Training	Training Program & Completion Tracking	Partially In Place	EV-014	HIPAA-TRN-008	Consolidate role-based training tracking into central LMS.
§164.308(a)(6)	Security Incident Procedures	Identification, Response, Mitigation, Documentation	Partially In Place	EV-012	HIPAA-IR-006	Schedule and evidence the annual IR tabletop exercise.
§164.308(a)(7)	Contingency Plan	Data Backup, DR, Emergency Mode, Testing	Partially In Place	EV-013	HIPAA-BKP-007	Complete outstanding restoration test cycles.
§164.308(a)(8)	Evaluation	Periodic Technical & Non-Technical Evaluation	In Place	EV-002	—	Continue periodic evaluation aligned to this assessment cycle.
§164.308(b)(1)	Business Associate Contracts	BAA Execution & Security Oversight	Partially In Place	EV-010	HIPAA-BAA-005	Complete overdue BA security reviews; centralize tracking.
§164.310(a)(1)	Facility Access Controls	Facility Security Plan, Access Control & Validation	In Place	EV-018	—	Maintain current facility access control procedures.
§164.310(b)	Workstation Use	Proper Functions & Workstation Context	Partially In Place	EV-018	HIPAA-PHY-009	Default privacy screens for remote ePHI-accessing personnel.
§164.310(c)	Workstation Security	Physical Safeguards for Workstations	Partially In Place	EV-018	HIPAA-PHY-009	Close identified gaps for sampled home-office workstations.
§164.310(d)(1)	Device and Media Controls	Disposal, Media Re-Use, Accountability, Backup/Storage	In Place	EV-018	—	Maintain current device and media control procedures.
§164.312(a)(1)	Access Control	Unique User ID, Emergency Access, Automatic Logoff, Encryption	Partially In Place	EV-006	HIPAA-ACC-014	Align clinical coordination app timeout to 15-minute standard.
§164.312(b)	Audit Controls	Recording & Examining Activity	Partially In Place	EV-007	HIPAA-AUD-013	Fix CRM audit log review ownership and cadence.
§164.312(c)(1)	Integrity	Mechanisms to Authenticate ePHI	In Place	EV-007	—	Maintain current integrity monitoring controls.
§164.312(d)	Person or Entity Authentication	Verification of User/Entity Identity	Partially In Place	EV-006	HIPAA-MFA-016	Migrate legacy scheduling tool behind SSO/MFA gateway.
§164.312(e)(1)	Transmission Security	Integrity Controls & Encryption in Transit	In Place	EV-009	—	Maintain current transmission security controls.
§164.314(a)(1)	Organizational Requirements	Business Associate Contracts	Partially In Place	EV-011	HIPAA-BAA-005	See Business Associate Contracts and Other Arrangements above.
§164.314(b)	Organizational Requirements	Requirements for Group Health Plans	Not Applicable	—	—	NovaCura does not sponsor a group health plan subject to this provision.
§164.316(a)	Policies and Procedures	Reasonable and Appropriate Policies	Partially In Place	EV-001	HIPAA-DOC-015	Complete outstanding policy reviews; centralize governance calendar.
§164.316(b)(1)	Documentation	Documentation, Retention, Availability,	Observation	EV-001	HIPAA-RET-	Centralize documentation

Citation	Control Area	Control Objective	Illustrative Status	Evid.	Finding	Recommended Action
		Updates			017	retention tracking platform-wide.
§164.520	Privacy Rule	Notice of Privacy Practices	In Place	EV-015	—	Maintain current Notice of Privacy Practices distribution.
§164.502(b) / §164.514(d)	Privacy Rule	Minimum Necessary	Partially In Place	EV-015	HIPAA-PRV-010	Redesign CRM role model around minimum-necessary access.
§164.502	Privacy Rule	Permitted Uses and Disclosures	In Place	EV-015	—	Maintain current uses-and-disclosures controls.
§164.524	Privacy Rule	Individual Right of Access	In Place	EV-020	—	Maintain current individual access request process.
§164.526	Privacy Rule	Individual Right to Request Amendment	In Place	EV-020	—	Maintain current amendment request process.
§164.528	Privacy Rule	Accounting of Disclosures	In Place	EV-020	—	Maintain current accounting-of-disclosures process.
§164.402 / §164.404	Breach Notification Rule	Breach Definition & Risk Assessment	Partially In Place	EV-016	HIPAA-BRN-011	Route all PHI-involving events through documented risk assessment.
§164.404	Breach Notification Rule	Individual Notification	In Place	EV-016	—	Maintain current individual notification workflow and timing.
§164.408	Breach Notification Rule	HHS Notification	In Place	EV-016	—	Maintain current HHS notification workflow and timing.
§164.410	Breach Notification Rule	Business Associate Notification to Covered Entity	In Place	EV-011	—	Maintain current BA-to-covered-entity notification terms.

34 REGULATORY WATCH — 2026

PROPOSED / REGULATORY-WATCH ITEMS — NOT CURRENT MANDATORY HIPAA SECURITY RULE REQUIREMENTS

2026 HIPAA Cybersecurity Regulatory Watch

In December 2024, HHS/OCR published a Notice of Proposed Rulemaking (NPRM) proposing significant cybersecurity-focused modifications to the HIPAA Security Rule. As of this report's date, the NPRM has not been finalized and does not constitute a current, legally effective requirement. This section presents the proposed concepts separately, for regulatory awareness and future-readiness purposes only. None of the items below were scored as part of the current-state assessment in Sections 11 through 33 of this report, and none are treated as a current mandatory HIPAA Security Rule requirement.

Proposed Concepts Under the 2024 NPRM

Technology Asset Inventory	A more explicit requirement to maintain a written inventory of technology assets that create, receive, maintain, or transmit ePHI.
Network Mapping	A requirement to maintain a network map illustrating the movement of ePHI throughout the organization's electronic information systems.
More Specific Written Risk Analysis	More prescriptive documentation requirements for the risk analysis required under §164.308(a)(1)(ii)(A).
Multi-Factor Authentication (MFA)	A proposal to require MFA for access to systems containing ePHI, subject to defined exceptions.
Encryption	A proposal to make encryption of ePHI at rest and in transit a required (rather than addressable) specification, subject to defined exceptions.
Vulnerability Scanning	A proposal to require vulnerability scanning at least every six months.
Penetration Testing	A proposal to require penetration testing at least once every twelve months.
Network Segmentation	A proposal to require network segmentation to limit the spread of a security incident.
Incident Response Planning	More prescriptive incident response planning and testing requirements.
Backup / Recovery Objectives	A proposal to require written procedures restoring the loss of certain relevant electronic information systems and data within 72 hours.
Annual Compliance Audits	A proposal requiring an annual audit or evaluation of compliance with the Security Rule.

These proposed modifications are presented for regulatory awareness and future-readiness purposes only and are NOT scored as current mandatory HIPAA Security Rule requirements in this sample assessment.

Future-Readiness Observations

Several fictional findings and observations in this report — particularly HIPAA-RSK-001 (enterprise risk analysis completeness), HIPAA-WAT-019 (technology asset inventory maturity), HIPAA-MFA-016 (MFA coverage), HIPAA-ENC-004 (encryption coverage), HIPAA-VUL-012 (vulnerability remediation), and HIPAA-BKP-007 (backup/recovery testing) — happen to also represent areas of alignment with the proposed 2024 NPRM concepts above. This alignment is presented for informational context only; each of those findings is scored in this report solely against the current, legally effective HIPAA Security Rule, not against the proposed rule.

35 ASSESSMENT LIMITATIONS

This entire report — including its scope, methodology, evidence, findings, and conclusions — is a fictional construct created solely to demonstrate TMG Security's report structure, methodology, and reporting standards. The following limitations apply specifically to this sample document and distinguish it from an actual HIPAA engagement deliverable:

- NovaCura Health & Pharmaceuticals, Inc. is a fictional organization. It does not correspond to any real company, and no real entity was assessed in the production of this document.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report.
- No real PHI or ePHI was accessed at any point in the production of this document.
- No actual policies or evidence were collected. All evidence references (EV-xxx) are illustrative placeholders only.
- No actual penetration testing was performed.
- No actual vulnerability scanning was performed.
- No actual interviews occurred; all interviews and control walkthroughs referenced in this report are simulated.
- No actual breach occurred; the incident scenario in Section 15 is entirely fictional.
- No actual OCR investigation, audit, or enforcement action occurred.
- Findings, evidence references, dates, and management responses are fictional and illustrative.
- Risk ratings are illustrative and do not reflect any actual risk assessment outcome.
- This document does not constitute HIPAA certification. HIPAA does not provide for a formal government-issued certification of compliance.
- This document does not constitute an OCR audit, investigation, or enforcement determination.
- This document does not constitute legal advice.
- This document does not establish actual HIPAA compliance for any organization.
- Actual HIPAA compliance depends on the organization's specific facts, scope, legal obligations, risk analysis, and implemented safeguards, and should be evaluated with qualified legal and compliance counsel.

36 GLOSSARY

PHI	Protected Health Information — individually identifiable health information held or transmitted by a covered entity or business associate.
ePHI	Electronic Protected Health Information — PHI that is created, received, maintained, or transmitted in electronic form.
Covered Entity	A health plan, healthcare clearinghouse, or healthcare provider that transmits health information electronically in connection with a covered transaction.
Business Associate	A person or entity that performs functions or services on behalf of a covered entity involving the use or disclosure of PHI.
BAA	Business Associate Agreement — the contract required between a covered entity and a business associate under §164.314(a).
Security Rule	The HIPAA Security Rule (45 CFR Part 164, Subpart C), establishing administrative, physical, and technical safeguards for ePHI.

Privacy Rule	The HIPAA Privacy Rule (45 CFR Part 164, Subpart E), governing permitted uses and disclosures of PHI and individual rights.
Breach Notification Rule	The HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D), governing notification obligations following a breach of unsecured PHI.
HITECH	Health Information Technology for Economic and Clinical Health Act — extends certain HIPAA obligations to business associates and strengthens enforcement.
OCR	HHS Office for Civil Rights — the federal agency responsible for enforcing HIPAA.
Minimum Necessary	The Privacy Rule standard requiring reasonable efforts to limit PHI use, access, and disclosure to the minimum necessary for the intended purpose.
Risk Analysis	The Security Rule–required assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
Addressable Specification	A Security Rule implementation specification that must be implemented as specified, replaced with an equivalent alternative, or documented as not reasonable and appropriate — but which cannot simply be omitted.
MFA	Multi-Factor Authentication — authentication requiring two or more independent verification factors.
SIEM	Security Information and Event Management — a platform for centralized log aggregation, correlation, and alerting.
EDR	Endpoint Detection and Response — technology that monitors and responds to threats on endpoint devices.
MDM	Mobile Device Management — a platform used to enforce configuration and security policy on managed devices.
NPRM	Notice of Proposed Rulemaking — the December 2024 HHS/OCR proposal to modernize the HIPAA Security Rule, not yet final as of this report's date.
CRM	Customer/Patient Relationship Management platform — used in this report to refer to NovaCura's patient-support case management system.
GRC	Governance, Risk, and Compliance — the discipline and tooling used to manage organizational risk and regulatory compliance.

37 CONTACT & DISCLAIMER

TMG ..SECURITY..

Cybersecurity | SOC | VAPT | GRC | MDR | Compliance Solutions | Corporate Trainings

Web: www.tmgsec.com **Email:** security@tmgsec.com
USA Office: 117 South Lexington Street, STE 100, Harrisonville, MO 64701
Support: support@tmgsec.com | **Phone:** +1 (816) 793-1929
WhatsApp: +1 (480) 680-0342

Final Disclaimer

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL HIPAA ASSESSMENT OR CERTIFICATION

This document was created by TMG Security solely to demonstrate assessment methodology, cybersecurity analysis, and professional reporting standards. NovaCura Health & Pharmaceuticals, Inc. is fictional. No actual HIPAA assessment, OCR audit, certification, attestation, or compliance determination was performed or issued.