



HIPAA Compliance Policy Manual

Effective Date: November 2025

Applies To: All Norman Nerds employees, contractors, vendors, and partners who create, receive, maintain, or transmit Protected Health Information (PHI).

Table of Contents

I. Introduction & Overview

1. Purpose
2. Scope
3. Definitions
4. Regulatory References
5. Governance Structure

II. Privacy Policy

1. Objectives
2. Authorized Uses and Disclosures
3. Minimum Necessary Standard
4. Procedures for Use and Disclosure
5. Retention and Destruction
6. Monitoring and Compliance

III. Security Policy

1. Administrative Safeguards
2. Technical Safeguards
3. Physical Safeguards
4. Access Control Procedures
5. System Security and Maintenance

IV. Breach Notification Policy

1. Definitions
2. Incident Response Plan
3. Notification Requirements
4. Reporting Procedures
5. Documentation

V. Workforce Training & Awareness

1. Training Requirements
2. Annual Programs
3. Specialized Training
4. Recordkeeping

VI. Sanctions Policy

1. Policy Statement
2. Classification of Violations
3. Corrective Actions
4. Enforcement Procedures

VII. Business Associate Oversight

1. BAA Execution
2. Vendor Risk Assessments
3. Ongoing Monitoring

VIII. Confidentiality Agreement

IX. Risk Management & Audit Policy

X. Retention & Documentation Policy

XI. Continuous Improvement

XII. Attestation

Appendices

- A – Business Associate Agreement Template
- B – Breach Report Form
- C – Risk Assessment Template
- D – Workforce Acknowledgment Form
- E – Annual Audit Checklist
- F – Policy Revision Log
- G – Artificial Intelligence (AI) Acceptable Use, Governance & Risk Management Policy

Norman Nerds

2

I. Introduction & Overview

1. Purpose

This manual establishes the official privacy, security, and compliance framework for Norman Nerds, an Oklahoma-based information-technology service provider that functions as a *Business Associate* under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Its purpose is to:

1. Define organizational safeguards that ensure the confidentiality, integrity, and availability of Protected Health Information (PHI).
2. Describe administrative, physical, and technical measures used to comply with 45 CFR Parts 160 and 164, Subparts A, C, and E.
3. Provide a repeatable governance model for all Norman Nerds personnel and contractors handling PHI on behalf of client Covered Entities.
4. Incorporate applicable provisions of Oklahoma Statutes Title 24 §162 (Data Breach Notification) and §76-19 et seq. (Privacy of Medical Information).

2. Scope

This manual applies to:

- All workforce members — employees, contractors, interns, and temporary staff.
- All subsidiaries or affiliates of Norman Nerds engaged in activities involving PHI.
- All computing environments including data centers, cloud services, mobile devices, removable media, and hosted client infrastructure.
- All paper, electronic, and verbal forms of PHI created, received, stored, transmitted, or disposed of by Norman Nerds.

Activities excluded from scope are strictly those with no PHI contact, such as purely administrative or marketing operations without patient data.

3. Definitions

- a. Protected Health Information (PHI): Individually identifiable health information maintained or transmitted in any medium that relates to an individual's physical or mental health, the provision of care, or payment for care.
- b. Electronic Protected Health Information (ePHI): PHI created, stored, transmitted, or received electronically.
- c. Business Associate: A person or entity that performs functions or activities on behalf of a Covered Entity involving PHI (e.g., data storage, network hosting, analytics, or technical support).
- d. Breach: The acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA that compromises its security or privacy.
- e. Minimum Necessary Standard: A principle requiring that access, use, or disclosure of PHI be limited to the minimum amount necessary to accomplish the intended purpose.
- f. Covered Entity: A health plan, healthcare clearinghouse, or healthcare provider who transmits any health information electronically in connection with HIPAA transactions.
- g. Workforce Member: Employees, volunteers, trainees, or other persons whose conduct is under the direct control of Norman Nerds.

4. Regulatory References

This program is based on the following primary authorities:

Regulation / Guidance	Reference
HIPAA Privacy Rule	45 CFR Part 164 Subpart E
HIPAA Security Rule	45 CFR Part 164 Subpart C
HIPAA Breach Notification Rule	45 CFR Part 164 Subpart D
HIPAA Enforcement Rule	45 CFR Part 160 Subpart C
HITECH Act	Public Law 111-5 §13400-13424
NIST SP 800-30 Rev 1	Guide for Conducting Risk Assessments
NIST SP 800-53 Rev 5	Security and Privacy Controls for Information Systems
HHS 405(d) Cybersecurity Performance Goals (2025)	U.S. Dept. of Health & Human Services
Oklahoma Statutes Title 24 §162	Oklahoma Breach Notification Law
Oklahoma Statutes Title 76 §19 et seq.	Medical Information Privacy Law

5. Governance Structure

a. HIPAA Compliance Officer

Responsible for overall implementation, oversight, and enforcement of this manual. Duties include annual policy review, coordinating audits, incident management, and serving as liaison with client compliance officers.

b. HIPAA Security Officer

Manages technical safeguards, access control, encryption, and monitoring systems; leads risk assessments and vulnerability remediation.

c. Legal Counsel / Privacy Advisor

Advises on contractual compliance, BAAs, and regulatory interpretations; reviews incident notifications.

d. Department Managers

Ensure workforce adherence within their operational areas; maintain training and sanction records.

e. All Workforce Members

Responsible for understanding and complying with all sections of this manual, reporting suspected breaches, and completing required training.

6. Policy Administration and Maintenance

- The Compliance Officer reviews this manual annually or after any regulatory, contractual, or operational change affecting PHI.
- Revisions are logged in Appendix F – Policy Revision Log.
- The most current approved version is maintained on the secure compliance document repository; superseded versions are archived for at least six (6) years.
- All employees must attest electronically to receipt and understanding of updates within 10 business days of publication.

II. Privacy Policy

1. Objectives

The purpose of this Privacy Policy is to ensure that Norman Nerds, as a HIPAA Business Associate operating in Oklahoma, handles Protected Health Information (PHI) only for authorized purposes and in a manner that preserves its confidentiality. This policy implements the HIPAA Privacy Rule (45 CFR Part 164 Subpart E) and Oklahoma Statutes § 76-19 et seq.

2. Authorized Uses and Disclosures

2.1 Permitted Uses

Norman Nerds may use or disclose PHI solely for the following purposes:

- 1. Performing contracted IT or data-management services for client Covered Entities under executed Business Associate Agreements (BAAs).
- 2. Providing system maintenance, data backup, hosting, or analytics in support of those services.
- 3. Complying with legal obligations such as subpoenas or court orders after consultation with Legal Counsel.
- 4. Performing internal operations necessary for compliance oversight, risk management, and auditing.

2.2 Prohibited Uses

Norman Nerds workforce members may not:

- Access or disclose PHI for personal interest or non-business reasons.
 - Sell, trade, or use PHI for marketing without explicit authorization from the Covered Entity.
 - Store PHI on personal devices or unapproved cloud storage.
 - Transmit PHI via unencrypted email or consumer messaging platforms.
-

3. Minimum Necessary Standard

All PHI access must conform to the Minimum Necessary Standard.

Procedures:

- 1. System Administrators configure user roles granting least-privilege access.
 - 2. Managers verify access lists quarterly.
 - 3. Logs of PHI queries or exports are reviewed monthly by the HIPAA Security Officer.
 - 4. Requests exceeding minimum necessity require written justification and Compliance Officer approval.
-

4. Procedures for Use and Disclosure

Step	Action	Responsible Party	Documentation Required
1	Determine if requested data contains PHI	Requestor	Data Classification Form
2	Confirm the disclosure is covered under a valid BAA	Compliance Officer	BAA Reference
3	If not, obtain client authorization	Legal Counsel	Authorization Record
4	Transfer data only via approved encrypted channels	IT Operations	Transmission Log
5	Record the disclosure in the PHI Disclosure Register	Data Owner	Disclosure Log

5. Retention and Destruction

- Electronic PHI (ePHI) is retained only as long as required by contract or legal obligation.
- Upon termination of a client relationship, all PHI must be returned or securely destroyed within 30 days, following NIST SP 800-88 Rev 1 sanitization guidelines.
- Paper records are cross-cut shredded or incinerated; destruction is witnessed and logged.
- The Compliance Officer maintains a “Certificate of Destruction” for each event.

6. Monitoring and Compliance

- Privacy audits are conducted semi-annually to verify adherence.
- Random spot-checks of email, file-sharing, and ticketing systems ensure PHI is handled appropriately.
- Non-compliance triggers corrective action under the Sanctions Policy.
- All monitoring records are retained six (6) years.

7. Patient Rights Support

Although Norman Nerds is not a Covered Entity, it supports clients in fulfilling patient rights by:

- Providing system access logs for patient-access requests.
- Assisting in correction or amendment requests to ensure data integrity.
- Ensuring timely export of PHI in electronic format upon client instruction.

Norman Nerds

III. Security Policy

1. Purpose and Objective

The purpose of this Security Policy is to ensure that Norman Nerds, as a HIPAA Business Associate, maintains administrative, physical, and technical safeguards necessary to protect the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) as required under the HIPAA Security Rule (45 CFR Part 164 Subpart C) and relevant Oklahoma data protection statutes. Norman Nerds implements a layered defense approach combining access control, encryption, system monitoring, and continuous risk management.

2. Administrative Safeguards

2.1 Security Management Process

- Risk Analysis: Conducted at least annually or after major system changes, using the methodology defined in NIST SP 800-30.
- Risk Management: Identified risks are categorized as *Low, Medium, High*, and mitigation plans are tracked in a risk register.
- Sanction Policy Enforcement: Refer to Section VI for disciplinary actions related to security violations.
- Information System Activity Review: Audit logs, access reports, and security incident tracking are reviewed monthly by the HIPAA Security Officer.

2.2 Assigned Security Responsibility

- The HIPAA Security Officer is accountable for implementing and maintaining all security measures.
- Each department designates a Security Liaison responsible for ensuring compliance at the operational level.

2.3 Workforce Security

Objective	Procedure	Responsible Role
Authorization	Verify role and access level with department manager before granting access to ePHI systems.	IT Admin
Supervision	Monitor workforce members' access logs and privilege changes.	Security Officer
Termination	Immediately disable credentials and recover all company assets upon separation.	HR & IT

2.4 Information Access Management

- Access rights are defined by job function (least privilege principle).
- User provisioning and de-provisioning follow a documented workflow and require managerial approval.
- Quarterly access reviews are mandatory for all systems storing or transmitting PHI.

2.5 Security Awareness and Training

- All workforce members complete annual HIPAA Security training (see Section V).
- Phishing simulations and email security reminders are conducted quarterly.
- IT and Compliance teams perform tabletop exercises for breach simulation twice annually.

2.6 Contingency Planning

- Data Backup: All ePHI stored in Norman Nerds systems is backed up daily, encrypted, and stored redundantly across secure cloud regions.
- Disaster Recovery: Tested semi-annually; Recovery Time Objective (RTO) = 24 hours; Recovery Point Objective (RPO) = 4 hours.
- Emergency Mode Operations: Documented procedures ensure continuity of services during natural disasters or cyber events.
- Contingency Plan Updates: Reviewed annually by the Compliance Officer.

2.7 Evaluation

Periodic technical and non-technical evaluations are conducted to ensure that security measures remain effective in light of environmental or operational changes.

3. Technical Safeguards

3.1 Access Controls

- Unique User Identification: Each user has a distinct ID; group logins are prohibited.
- Multi-Factor Authentication (MFA): Required for all remote and privileged access.
- Automatic Logoff: Workstations and systems automatically lock after 15 minutes of inactivity.
- Emergency Access Procedure: The Security Officer maintains an emergency access protocol for critical system restoration, documented and tested quarterly.

3.2 Audit Controls

- All access to ePHI is logged and timestamped.
- Logs include user ID, activity type, system, and date/time.
- Logs are retained for a minimum of six (6) years.
- SIEM tools (e.g., Microsoft Sentinel) are used for real-time anomaly detection.

3.3 Integrity Controls

- Data integrity is maintained through checksums, version control, and restricted modification rights.
- System updates are verified using cryptographic signatures.
- Unauthorized changes trigger alerts and require incident response investigation.

3.4 Authentication Controls

- Password complexity: Minimum 12 characters, upper/lowercase, number, and special character.
- Password rotation every 90 days.
- Reuse prohibited for the last five passwords.
- Account lockout after five failed login attempts.

3.5 Transmission Security

- PHI transmitted via network connections uses TLS 1.3 or higher.
 - VPN tunnels are mandatory for remote system administration.
 - Email encryption is required for all PHI content (S/MIME or equivalent).
 - Public cloud services are permitted only if compliant with HIPAA Business Associate Agreements.
-

4. Physical Safeguards

4.1 Facility Access Controls

- Server rooms and data centers are restricted to authorized personnel only.
- Access is controlled via keycard and logged electronically.
- Visitors must sign in and be escorted at all times.
- Video surveillance is maintained for a rolling period of at least 90 days.

4.2 Workstation Use and Security

- Workstations must be positioned to prevent viewing by unauthorized individuals.
-

- PHI must never be printed or displayed in open public areas.
- Devices must auto-lock after 15 minutes of inactivity.
- Only company-managed devices may be used to access PHI systems.

4.3 Device and Media Controls

Process	Procedure	Retention / Disposal
Media Disposal	Decommissioned drives sanitized using DoD 5220.22-M or NIST SP 800-88 standards.	Certificate of Destruction retained for 6 years
Media Reuse	Reformat and overwrite all PHI before reuse.	Logged by IT Security
Accountability	Maintain asset inventory of all PHI-handling devices.	Updated quarterly
Data Backup	Maintain offsite encrypted backups of all ePHI.	Daily backups retained for 30 days

5. System Security and Maintenance

5.1 Patch Management

- Critical security updates applied within 15 days of vendor release.
- Moderate updates within 30 days.
- Compliance verified through monthly vulnerability scans.

5.2 Malware Protection

- Endpoint protection software required on all servers and workstations.
- Daily automated scans and weekly full-system scans.
- Email gateways perform real-time attachment and link inspection.

5.3 Vulnerability Scanning and Penetration Testing

- Internal vulnerability scans are performed monthly.
- External third-party penetration tests conducted annually.
- Remediation actions are tracked and documented in the risk register.

5.4 Encryption Standards

- Data at rest: AES-256 encryption.
- Data in transit: TLS 1.3 minimum.
- Encryption keys stored in secure hardware modules with role-based access.

5.5 Security Incident Response Integration

- All detected anomalies feed into the incident response workflow defined in Section IV.
- Escalations are triaged within one (1) business day.
- Root cause analyses are performed post-incident and tracked for corrective action.

IV. Breach Notification Policy

1. Purpose

This policy defines the procedures for identifying, managing, documenting, and reporting any unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) or electronic PHI (ePHI) handled by Norman Nerds.

It fulfills the requirements of:

- HIPAA Breach Notification Rule (45 CFR §§164.400–414)
- HITECH Act §13402
- Oklahoma Data Breach Notification Act (Title 24 §162)

2. Definitions

Term	Definition
Security Incident	Any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.
Breach	A security incident that results in the acquisition, access, use, or disclosure of PHI in violation of HIPAA, compromising its security or privacy.
Unsecured PHI	PHI that has not been rendered unusable, unreadable, or indecipherable through encryption or destruction.
Discovery Date	The date Norman Nerds first becomes aware (or should reasonably have been aware) of the incident.
Affected Individual	A person whose PHI was involved in a breach.

3. Policy Statement

Norman Nerds must promptly detect, investigate, mitigate, and report any confirmed or suspected PHI breach. All workforce members are required to report potential incidents immediately to the HIPAA Security Officer or Compliance Officer.

Failure to report a known or suspected breach may result in disciplinary action under the Sanctions Policy.

4. Roles and Responsibilities

Role	Responsibilities
HIPAA Security Officer	Coordinates investigation, containment, and mitigation of incidents; ensures documentation and technical forensics.
Compliance Officer	Oversees legal notification requirements, coordinates communication with clients (Covered Entities) and regulators.
Legal Counsel	Advises on statutory reporting requirements and potential liabilities.
IT Operations	Implements containment measures, preserves logs, restores data integrity.
Department Managers	Ensure staff cooperation and timely completion of corrective actions.

5. Incident Response Process

5.1 Detection and Reporting

1. Any workforce member who suspects a breach must immediately notify the HIPAA Security Officer via the Incident Hotline or the internal ticketing portal.
2. Within one (1) business day, the Security Officer acknowledges receipt and begins a preliminary assessment.
3. The reporter completes a Breach Report Form (see Appendix B).

5.2 Containment

- Disconnect or disable compromised accounts or systems.
- Isolate affected network segments.
- Suspend data transmissions involving the affected systems.
- Preserve audit logs, forensic images, and access records.

5.3 Investigation and Risk Assessment

A formal risk assessment evaluates:

Factor	Example Considerations
Nature of PHI involved	Type of identifiers, sensitivity (e.g., SSN, diagnosis, treatment).
Unauthorized person	Whether recipient is subject to HIPAA or confidentiality obligations.
Acquisition or viewability	Whether PHI was actually viewed, copied, or exfiltrated.
Mitigation	Whether PHI was retrieved or adequately destroyed.

If risk is determined to be “low,” documentation of the assessment justifying non-notification is required.

5.4 Mitigation

- Reset credentials and strengthen access controls.
- Patch vulnerabilities and verify system hardening.
- Provide re-training for involved workforce members.
- Monitor for evidence of further compromise.

6. Notification Procedures

6.1 Notification to Covered Entity

- Norman Nerds notifies the client Covered Entity within ten (10) business days of discovering a breach.
- Notification includes:
 - Incident description and discovery date
 - Types of PHI involved
 - Number of individuals affected
 - Mitigation actions taken
 - Recommendations for the Covered Entity’s follow-up

6.2 Notification to Individuals

Where Norman Nerds is the party responsible for direct notice under a client agreement:

- Written notice must be provided without unreasonable delay and no later than 60 days from discovery.
- Notices may be delivered by first-class mail or email (if consented).
- If contact information is insufficient for ≥10 individuals, a substitute web or media notice must be posted for at least 90 days.

6.3 Notification to HHS and Oklahoma Authorities

- Breaches involving 500 or more individuals: report to the Secretary of HHS contemporaneously with individual notifications.
- Breaches involving fewer than 500: maintain a log and submit to HHS annually within 60 days of each calendar year-end.
- If >1,000 Oklahoma residents are affected, notify the Oklahoma Attorney General and statewide media per Title 24 §162.

6.4 Law Enforcement Delay

If law enforcement determines that notification would impede a criminal investigation, Norman Nerds will delay notification for the period specified in the official written request.

7. Documentation Requirements

All breach investigations require the following documentation, retained for six (6) years:

1. Initial Breach Report Form (Appendix B).
2. Risk Assessment and Determination Worksheet.
3. Copies of notifications sent and delivery confirmations.
4. Corrective action plans and training evidence.
5. Root-cause analysis and mitigation summary.
6. Meeting minutes from the Breach Review Committee.

8. Communication Protocols

- All public statements are handled exclusively by the Compliance Officer or authorized designee.
- Employees must not discuss breach details with external parties or media.
- Internal communications use the “Confidential — HIPAA Incident” template.
- Clients are briefed using a standardized incident summary format approved by Legal.

9. Post-Incident Review

- A post-incident meeting occurs within 15 business days of containment.
- The Breach Review Committee evaluates the response, updates procedures, and assigns corrective actions.
- Lessons learned feed into the Continuous Improvement Program (Section XI).

10. Reporting Metrics

The Compliance Officer maintains quarterly metrics, including:

- Number of incidents reported.
- Average detection-to-containment time.
- Number of confirmed breaches vs. false positives.
- Training completions following incidents.

These metrics are reviewed by executive leadership each quarter.

11. Enforcement and Sanctions

- Failure to comply with this policy or to report a suspected breach constitutes a violation of Norman Nerds policy and may result in disciplinary measures under Section VI (Sanctions).
- Severe or intentional violations are referred to legal authorities as required by HIPAA §1177.

Norman Nerds

13

V. Workforce Training and Awareness Policy

1. Purpose

This policy defines the training and awareness requirements that ensure all Norman Nerds workforce members understand their responsibilities for protecting Protected Health Information (PHI) and electronic PHI (ePHI) under HIPAA, HITECH, and Oklahoma law.

The goal is to create a culture of security and compliance by ensuring that all staff know how to identify, prevent, and report privacy and security risks.

2. Regulatory Basis

- HIPAA Privacy Rule – 45 CFR §164.530(b)(1): Mandates that workforce members be trained on policies and procedures regarding PHI.
- HIPAA Security Rule – 45 CFR §164.308(a)(5): Requires a security awareness and training program for all workforce members.
- HITECH Act §13401–13402: Expands training obligations to Business Associates.
- Oklahoma Statute Title 24 §162: Requires breach preparedness and staff awareness regarding PHI handling.

3. Scope

This policy applies to:

- All full-time, part-time, temporary, and contract employees of Norman Nerds.
- All management personnel with access to PHI systems.
- All IT, Compliance, and HR staff responsible for data handling and employee management.

4. Training Objectives

Norman Nerds' HIPAA training program ensures that workforce members can:

1. Identify PHI and understand its sensitivity.
2. Understand how PHI can be lawfully used or disclosed.
3. Follow proper procedures for access, transmission, and storage of PHI.
4. Recognize and report suspected breaches or unauthorized disclosures.
5. Apply security best practices for electronic systems, devices, and networks.

5. Training Requirements

5.1 Initial (Onboarding) Training

- Completed within ten (10) business days of hire or prior to system access.
- Covers HIPAA fundamentals, PHI handling, breach reporting, password management, and acceptable use policies.
- Employees must pass a short knowledge assessment (minimum passing score: 85%).
- Certificates of completion are stored in HR records for six years.

5.2 Annual Refresher Training

- Required for all workforce members each calendar year.
- Updates include new regulatory changes, incident trends, and revised internal policies.
- Employees receive notice at least 30 days before the due date and must complete the module within that period.
- Completion status is reported monthly to the Compliance Officer.

5.3 Role-Based Training

Role	Focus Area	Frequency
IT & Security Staff	Technical safeguards, incident response, encryption, SIEM tools	Semi-annual
Compliance & Legal	HIPAA audit readiness, breach notification law, OCR enforcement	Annual
HR & Operations	Confidentiality agreements, workforce sanctions, data retention	Annual
Executives & Managers	Risk management, policy oversight, vendor compliance	Annual

5.4 Specialized Training

Additional ad hoc training sessions are required:

- Following any significant policy change.
- After a security incident or breach.
- When new technology or system functionality involving PHI is introduced.

6. Training Content Outline

1. Overview of HIPAA & HITECH
 - Purpose, enforcement, and penalties.
 - Difference between Covered Entities and Business Associates.
2. Understanding PHI
 - Identifiers, sensitive categories, and examples.
3. Privacy Practices
 - Minimum necessary standard.
 - Disclosure procedures.
4. Security Practices
 - Passwords, encryption, MFA, workstation safety.
5. Incident Response
 - How to identify and report suspected breaches.
6. Sanctions and Enforcement
 - Disciplinary actions for non-compliance.
7. Employee Responsibilities
 - Acknowledgment of confidentiality and compliance obligations.

7. Security Awareness Program

7.1 Ongoing Awareness Activities

Norman Nerds conducts ongoing awareness efforts to reinforce compliance between annual trainings:

- Monthly email tips highlighting privacy best practices.
- Quarterly “Security Awareness Days” with interactive sessions and phishing simulations.
- Posted reminders on secure workstation practices in shared office areas.
- Cybersecurity bulletins summarizing recent threats and mitigation strategies.

7.2 Phishing Simulation Program

- Conducted quarterly using mock phishing campaigns.
- Employees who click on simulated phishing links are required to complete follow-up training within five business days.
- Aggregate simulation results are reviewed by the Security Officer and reported to executive management.

7.3 Awareness Metrics

The Compliance Officer tracks metrics such as:

- Training completion rates (target $\geq 98\%$).
 - Average quiz scores (target $\geq 90\%$).
 - Number of phishing clicks vs. prior quarters (target continuous reduction).
-

8. Training Documentation and Recordkeeping

All training activities must be documented as follows:

Record Type	Retention Period	Responsible Department
Training attendance logs	6 years	HR
Certificates of completion	6 years	HR
Course content & presentations	Current + 1 prior version	Compliance
Knowledge assessments & scores	6 years	Compliance
Phishing campaign reports	3 years	IT Security

Training documentation serves as evidence of compliance for internal audits and HHS/OCR inquiries.

9. Enforcement

- Employees failing to complete mandatory training are subject to disciplinary measures per the Sanctions Policy (Section VI).
- Intentional disregard of training or awareness programs constitutes a policy violation.
- Contractors must maintain equivalent training and provide annual compliance attestations.

10. Continuous Improvement

- Feedback from employees is solicited after each session via anonymous survey.
- Lessons learned from incidents are integrated into updated course modules.
- The Compliance Officer reviews training effectiveness annually and revises materials as needed.

VI. Sanctions Policy

1. Purpose

This policy establishes clear disciplinary standards and corrective actions for Norman Nerds workforce members who fail to comply with the company's HIPAA, HITECH, or Oklahoma privacy and security policies.

The Sanctions Policy enforces accountability, deters negligence, and ensures consistent, fair handling of violations.

2. Regulatory Basis

- HIPAA Privacy Rule: 45 CFR §164.530(e)(1) – Requires covered entities and business associates to implement and apply appropriate sanctions against workforce members who fail to comply with privacy policies.
 - HIPAA Security Rule: 45 CFR §164.308(a)(1)(ii)(C) – Mandates enforcement of workforce sanctions related to security failures.
 - Oklahoma Statutes Title 24 §162 – Requires organizations to protect personal data and report breaches; violations may result in penalties.
-

3. Scope

This policy applies to all workforce members, including:

- Full-time and part-time employees
 - Temporary staff and interns
 - Independent contractors and vendors with PHI access
 - Any person performing duties under Norman Nerds' supervision or control
-

4. Policy Statement

Norman Nerds enforces sanctions to uphold integrity, deter misconduct, and demonstrate regulatory compliance.

Sanctions are proportionate to the severity, intent, and impact of the violation.

Disciplinary actions may range from verbal counseling to termination and referral for criminal prosecution.

5. General Principles

1. Consistency: All violations are investigated and addressed using standardized criteria.
 2. Fairness: The workforce member is informed of the allegation and allowed to respond.
 3. Documentation: Every sanction decision is documented and retained for a minimum of six (6) years.
 4. Confidentiality: Investigations and disciplinary proceedings are confidential to the extent permitted by law.
 5. Progressive Discipline: Sanctions escalate for repeated or intentional non-compliance.
-

6. Classification of Violations

Violations are classified into five (5) levels according to intent and impact:

Class	Description	Examples	Typical Actions
Class I – Inadvertent Violation	Unintentional, minor infraction with minimal risk to PHI.	Emailing PHI to the wrong internal recipient; failing to log out of workstation.	Verbal counseling; retraining; written warning.
Class II – Negligent Violation	Careless action causing limited PHI exposure.	Using personal cloud storage for PHI; repeated password sharing after warning.	Written reprimand; re-training; probation.
Class III – Reckless Violation	Disregard of known procedures or policy requirements.	Ignoring encryption rules; failing to report lost device.	Suspension; formal corrective action plan.
Class IV – Intentional Non-Malicious Violation	Knowingly violating policy without malicious intent.	Accessing PHI of a friend or family member out of curiosity.	Termination; possible referral to OCR.
Class V – Malicious Violation	Intentional and harmful breach or disclosure of PHI.	Selling PHI; sharing credentials to enable unauthorized access.	Immediate termination; legal referral; civil/criminal penalties.

7. Investigation Process

7.1 Reporting

- Any workforce member who observes or suspects a violation must report it to their Manager, HR, or the Compliance Hotline immediately.
- Anonymous reporting is permitted.

7.2 Preliminary Review

- The Compliance Officer and HR jointly conduct a preliminary review within five (5) business days to determine validity and classification.

7.3 Formal Investigation

- For confirmed incidents, a Sanction Review Panel (Compliance Officer, HR, Legal, and relevant management) is convened.
- The panel collects evidence, interviews witnesses, and documents findings.
- Investigations are completed within 30 days unless an extension is justified.

7.4 Determination and Disciplinary Action

- The Sanction Review Panel issues findings, recommends corrective measures, and records rationale in the Sanctions Log.
- Final disciplinary action is approved by the HR Director and Compliance Officer.
- The employee is formally notified of the decision and has the right to appeal (see Section 8).

8. Appeal Process

- The workforce member may file a written appeal within 10 business days of notification.
- Appeals are reviewed by the Chief Operating Officer (or delegate) within 15 business days.
- The decision of the reviewing officer is final.
- All appeal documentation is retained for six years.

9. Documentation and Recordkeeping

Document Type	Retention Period	Custodian
Sanctions Log	6 years	Compliance Officer
Investigation Reports	6 years	HR
Disciplinary Notices	6 years	HR
Appeal Records	6 years	HR
Training/Remediation Records	6 years	Compliance Officer

10. Coordination with Other Policies

This policy operates in conjunction with:

- Workforce Training and Awareness Policy (Section V)
- Breach Notification Policy (Section IV)
- Confidentiality Agreement (Section VIII)
- Business Associate Oversight Policy (Section VII)

A violation of any of these may trigger sanctions under this policy.

11. Reporting Obligations

- Serious or repeated violations may be reported to the client Covered Entity per contractual obligations.
 - Violations involving potential PHI breaches must also trigger the procedures in Section IV (Breach Notification).
 - Compliance reports are included in quarterly governance reviews.
-

12. Enforcement

- The Compliance Officer is responsible for ensuring consistent application of sanctions.
 - The HR Department ensures enforcement of disciplinary measures.
 - The Legal Department advises when violations require external reporting to HHS or law enforcement.
 - Managers who fail to enforce or report violations may themselves be subject to sanctions.
-

13. Policy Review

- This policy is reviewed annually or upon major updates to federal or Oklahoma law.
- Revisions are approved by executive management and recorded in Appendix F – Policy Revision Log.

VII. Business Associate Oversight Policy

1. Purpose

The purpose of this policy is to ensure that Norman Nerds, as a Business Associate under HIPAA, properly manages, monitors, and enforces compliance obligations for any subcontractors, service providers, or vendors who may create, receive, maintain, or transmit Protected Health Information (PHI) on behalf of Norman Nerds or its healthcare clients.

This policy fulfills the requirements of:

- HIPAA Privacy Rule (45 CFR §164.502(e))
- HIPAA Security Rule (45 CFR §164.308(b))
- HITECH Act §13404
- Oklahoma Statutes Title 24 §162 (Vendor Data Breach Notification Requirements)

2. Scope

This policy applies to:

- All third-party vendors, contractors, consultants, or service providers that may have access to PHI through Norman Nerds’ systems or services.
- All Norman Nerds business units engaging external vendors.
- All Business Associate Agreements (BAAs) where Norman Nerds acts as either the Business Associate or a Sub-Business Associate to a Covered Entity.

3. Policy Statement

Norman Nerds shall only share PHI with subcontractors or vendors who:

1. Have executed a written Business Associate Agreement (BAA) containing required HIPAA provisions.
2. Maintain equivalent administrative, physical, and technical safeguards to protect PHI.
3. Undergo periodic security assessments and demonstrate continued compliance.

No vendor may receive PHI until a fully executed and approved BAA is in place.

4. Definitions

Term	Definition
Business Associate (BA)	A person or entity performing services involving PHI for a Covered Entity.
Subcontractor (Sub-BA)	A third-party vendor of a Business Associate that handles PHI.
BAA (Business Associate Agreement)	A legally binding contract outlining permitted uses/disclosures of PHI and required safeguards.
Vendor Risk Assessment (VRA)	The structured evaluation process used to determine a vendor’s compliance posture.

5. Roles and Responsibilities

Role	Responsibility
Compliance Officer	Oversees vendor compliance program, reviews BAAs, ensures contractual adherence to HIPAA rules.
Legal Counsel	Drafts, negotiates, and approves all BAAs; interprets applicable state and federal laws.
Procurement Department	Ensures no vendor engagement involving PHI proceeds without prior BAA approval.

Role	Responsibility
IT Security Officer	Conducts technical due diligence and security risk assessments of vendor systems.
Vendor Manager / Project Owner	Ensures vendor activities remain within permitted scope of contract and BAA.

6. Procedures

6.1 Vendor Identification and Risk Categorization

All vendors are categorized by risk level based on PHI exposure:

Category	PHI Access Level	Examples	Assessment Frequency
High-Risk	Direct PHI access or data processing	Cloud hosting, EHR integration	Annual
Medium-Risk	Indirect PHI exposure	IT support, analytics services	Every 2 years
Low-Risk	No PHI access	Office supply vendors, cleaning services	None

6.2 Business Associate Agreement (BAA) Execution

Before engaging a vendor with potential PHI access:

1. The Project Owner submits a Vendor Request Form describing services and data flows.
2. The Compliance Officer reviews the request for HIPAA implications.
3. If PHI exposure is confirmed, a BAA is drafted or reviewed by Legal Counsel.
4. The BAA must include:
 - o Permitted uses and disclosures of PHI.
 - o Safeguard and breach notification requirements.
 - o Termination clauses for non-compliance.
 - o Subcontractor flow-down obligations.
 - o Right to audit clause.
5. Both parties execute the agreement before any PHI access is granted.
6. The signed BAA is stored in the Compliance Repository for at least six (6) years.

6.3 Vendor Risk Assessment (VRA)

Each vendor with PHI access undergoes a Vendor Risk Assessment, including:

- Review of security policies and certifications (e.g., SOC 2, ISO 27001).
- Evaluation of incident response and breach notification procedures.
- Examination of encryption, access control, and data segregation methods.
- Confirmation of background checks for vendor employees.
- Verification of cyber insurance coverage.

The IT Security Officer rates vendors on a five-point risk scale (1 = low, 5 = critical).

Remediation plans must be developed for vendors rated ≥ 3 .

6.4 Continuous Monitoring

Norman Nerds conducts ongoing vendor oversight via:

- Annual vendor compliance attestations.
- Periodic access reviews confirming least-privilege access.
- Contract renewal reviews verifying BAA validity and version control.
- Continuous security monitoring of integrated systems for abnormal activity.

All monitoring findings are logged in the Vendor Compliance Register maintained by the Compliance Office.

6.5 Breach and Incident Management

- Vendors must notify Norman Nerds within 5 business days of any actual or suspected breach involving PHI.
- Norman Nerds must notify the Covered Entity per Section IV (Breach Notification Policy).
- All vendor incidents are logged and reviewed through the standard Incident Response process.
- Failure to report a breach constitutes a material breach of the BAA.

6.6 Remediation and Termination

If a vendor is found noncompliant:

1. The Compliance Officer issues a Corrective Action Plan (CAP) with defined deadlines.
2. If remediation is successful, documentation is retained.
3. Failure to comply results in contract suspension or termination, and the vendor must return or destroy all PHI within 30 days.
4. Legal Counsel may issue a formal notice of termination per BAA provisions.

7. Documentation and Recordkeeping

Document Type	Retention Period	Custodian
Executed BAAs	6 years post-termination	Compliance Officer
Vendor Risk Assessments	6 years	IT Security
Vendor Compliance Register	Ongoing + 6 years archive	Compliance Officer
CAPs and Audit Reports	6 years	Compliance Officer
Vendor Termination Records	6 years	Legal Counsel

8. Annual Review

- The Compliance Officer reviews the vendor oversight process annually.
- Results are presented to executive leadership.
- Identified improvements feed into the Continuous Improvement Program (Section XI).

9. Enforcement

- Any Norman Nerds employee engaging a vendor without an approved BAA is subject to disciplinary action under the Sanctions Policy (Section VI).
- Noncompliant vendors may be reported to the client Covered Entity and, if applicable, the HHS Office for Civil Rights (OCR).

VIII. Confidentiality Agreement

1. Purpose

The purpose of this policy and agreement is to establish the confidentiality obligations of all Norman Nerds workforce members, contractors, and third-party affiliates who have access to Protected Health Information (PHI) or other confidential business data.

This section fulfills requirements under:

- HIPAA Privacy Rule – 45 CFR §164.530(a)(1)
- HIPAA Security Rule – 45 CFR §164.308(a)(3)(ii)(A)
- Oklahoma Statutes Title 76 §19–§19.2 (Confidentiality of Medical Information)

2. Scope

This agreement applies to:

- All employees, contractors, and volunteers of Norman Nerds.
- All third parties performing services involving access to PHI or confidential information.
- All forms of PHI—electronic, paper, or verbal—created, received, or maintained by Norman Nerds or its client Covered Entities.

3. Policy Statement

All workforce members must maintain strict confidentiality regarding PHI and other sensitive business information.

Information obtained in the course of employment or service shall be used solely for authorized business purposes and never disclosed to unauthorized persons.

Breaches of confidentiality, whether intentional or inadvertent, will result in disciplinary action under the Sanctions Policy (Section VI) and may lead to termination or legal penalties under federal and state law.

4. Definitions

Term	Definition
Confidential Information	Includes PHI, ePHI, business data, trade secrets, proprietary technology, customer lists, or any data designated confidential by Norman Nerds or its clients.
Need to Know	Access principle that allows use or disclosure only when necessary to perform assigned duties.
Unauthorized Disclosure	Any access, use, or release of information not permitted under policy or law.

5. Responsibilities

Each workforce member must:

1. Access PHI only as necessary for legitimate job duties.
2. Protect all forms of PHI and confidential data from unauthorized viewing, copying, or removal.
3. Avoid discussing PHI in public or unsecured areas (e.g., hallways, elevators, public calls).
4. Immediately report any suspected breach, unauthorized disclosure, or security incident.
5. Refrain from using PHI for personal, educational, or research purposes without explicit written authorization.
6. Continue to protect confidential information even after employment or contractual engagement ends.

6. Access Control and Security Obligations

- Each user is assigned a unique login credential; sharing credentials is strictly prohibited.
- Workstations must be locked when unattended.
- PHI or confidential documents must be stored in encrypted drives or secured cabinets.
- Printed materials must be disposed of using approved shredding processes.
- Portable storage devices (e.g., USB drives) may not contain PHI unless specifically authorized and encrypted.

7. Non-Disclosure Agreement (NDA) Acknowledgment

All workforce members must sign a Confidentiality and Non-Disclosure Agreement as a condition of access to PHI or company systems.

The NDA must include:

- Acknowledgment of the legal definition of PHI under HIPAA.
- Agreement to maintain confidentiality indefinitely, including post-employment.
- Consent to monitoring of system activity for compliance verification.
- Acknowledgment that violations may result in civil and criminal penalties under HIPAA §1177 and Oklahoma Statutes Title 76 §19.1.
- Authorization for Norman Nerds to enforce this agreement through disciplinary or legal action.

8. Workforce Confidentiality Statement

I acknowledge that in the performance of my duties at Norman Nerds, I may have access to Protected Health Information (PHI) and other confidential data.

I understand that such information is protected by federal and state laws, including HIPAA and Oklahoma privacy statutes.

I agree to use this information solely for authorized business purposes and to maintain its confidentiality at all times.

I understand that unauthorized disclosure or misuse of PHI may result in disciplinary action, including termination of employment, civil liability, or criminal prosecution.

I further understand that my obligation to maintain confidentiality continues indefinitely after my employment or contract ends.

Employee/Contractor Name: _____

Signature: _____

Date: _____

Supervisor/Manager: _____

9. Retention and Documentation

Document Type	Retention Period	Custodian
Signed Confidentiality Agreements	6 years post-separation	HR Department
NDA Master Templates	Current + 1 prior version	Legal Department
Confidentiality Training Records	6 years	Compliance Officer

10. Violations and Enforcement

Violations of this policy, including failure to sign or comply with the confidentiality agreement, will result in disciplinary action under Section VI (Sanctions Policy) and may be reported to the appropriate regulatory bodies (HHS/OCR or state authorities).

11. Policy Review

This policy and agreement are reviewed annually by the Compliance Officer and Legal Counsel to ensure compliance with HIPAA, HITECH, and Oklahoma law.

Norman Nerds

25

IX. Risk Management and Audit Policy

1. Purpose

This policy establishes the structured framework by which Norman Nerds identifies, evaluates, mitigates, and monitors risks to the confidentiality, integrity, and availability of Protected Health Information (PHI) and electronic PHI (ePHI).

It also defines the internal auditing process used to ensure continued compliance with HIPAA, HITECH, and Oklahoma data protection laws.

This section fulfills requirements under:

- HIPAA Security Rule – 45 CFR §164.308(a)(1)(ii)(A)-(B)
- HITECH Act §13401
- NIST SP 800-30 Rev.1 (Risk Assessment Guide)
- NIST SP 800-53 Rev.5 (Security and Privacy Controls)
- Oklahoma Title 24 §162 (Data Breach and Security Standards)

2. Scope

This policy applies to:

- All systems, applications, and data storage environments containing PHI.
- All Norman Nerds business units, data centers, and cloud service providers.
- All workforce members and subcontractors participating in system operations or compliance activities.

3. Policy Statement

Norman Nerds shall maintain a continuous, enterprise-wide risk management and audit program to ensure:

1. Identification and prioritization of risks affecting PHI.
2. Implementation of appropriate safeguards to mitigate identified risks.
3. Regular auditing of administrative, technical, and physical controls.
4. Documentation and retention of all assessments, results, and mitigation plans for at least six (6) years.

4. Risk Assessment Framework

4.1 Methodology

Norman Nerds follows a structured 5-step risk assessment process consistent with NIST SP 800-30:

Step	Description	Outcome
1. Identify Assets	Catalog all systems, devices, applications, and data flows involving PHI.	Asset inventory
2. Identify Threats and Vulnerabilities	Evaluate environmental, human, technical, and process-based risks.	Threat inventory
3. Assess Likelihood and Impact	Assign quantitative or qualitative risk ratings (Low, Medium, High).	Risk matrix
4. Determine Risk Level	Multiply likelihood × impact to determine overall risk exposure.	Prioritized risk register
5. Recommend Controls	Specify mitigations, controls, or acceptance rationale.	Risk Treatment Plan

Risk assessments are conducted annually and upon any major system, operational, or regulatory change.

5. Risk Categorization

Risk Category	Examples	Potential Impact
Technical Risks	Unpatched systems, weak encryption, misconfigured firewalls	Data exposure or integrity loss
Administrative Risks	Inadequate training, poor documentation, missing BAAs	Regulatory non-compliance
Physical Risks	Unauthorized server room access, theft, natural disasters	PHI loss or downtime
Third-Party Risks	Vendor breaches, subcontractor negligence	Shared liability or breach propagation
Human Risks	Insider threats, negligence, phishing	Unauthorized disclosure

6. Risk Evaluation and Rating

6.1 Risk Matrix

Likelihood Impact: Low (1) Medium (2) High (3)

Low (1) 1 2 3

Medium (2) 2 4 6

High (3) 3 6 9

- Risk Score = Likelihood × Impact
- Thresholds:
 - 1–2 = Low (Acceptable)
 - 3–4 = Moderate (Mitigation Required)
 - 6–9 = High (Immediate Action Required)

6.2 Documentation

Results are recorded in the Risk Register, which includes:

- Asset or process name
- Risk description
- Likelihood and impact scores
- Mitigation strategy
- Assigned owner and target completion date

7. Risk Mitigation

- Controls selected must be cost-effective and aligned with risk severity.
- Mitigation actions are prioritized based on residual risk after control implementation.
- Examples of mitigation strategies include:
 - Implementing multi-factor authentication.
 - Encrypting all PHI storage and transmissions.
 - Conducting staff re-training.
 - Deploying intrusion detection and endpoint protection.
 - Enforcing vendor compliance through BAAs and audits.

Each mitigation plan is documented in a Risk Treatment Plan (RTP), approved by the Compliance Officer and IT Security Officer.

8. Risk Monitoring and Review

- The Risk Register is reviewed quarterly by the Risk Management Committee (Compliance, Security, Legal, and IT).
- High and critical risks remain on active review until resolved or accepted by executive leadership.
- The Compliance Officer provides quarterly risk summaries to executive management.
- Updated assessments are conducted following any:
 - Security incident or breach
 - Technology infrastructure change
 - New client engagement involving PHI
 - Major organizational restructuring

9. Audit Program Overview

9.1 Objectives

The Internal Audit Program ensures:

1. Controls are designed and operating effectively.
2. Gaps or non-compliance are identified early.
3. Compliance evidence is available for clients, regulators, or auditors.

9.2 Audit Frequency

Audit Type	Frequency	Conducted By
Privacy Audit	Semi-annually	Compliance Officer
Security Audit	Quarterly	IT Security
Vendor Audit	Annually	Compliance & Procurement
Physical Security Review	Annually	Facilities & Security
System Access Review	Quarterly	IT Administrator

9.3 Audit Procedures

1. Review policies, logs, and configurations for compliance.
2. Interview key personnel and inspect system settings.
3. Test selected controls through sampling and observation.
4. Document findings, classify risk severity, and assign corrective actions.
5. Track remediation progress until closure.

10. Reporting and Corrective Action

10.1 Audit Reporting

- Draft audit reports are prepared within 10 business days of completion.
- Reports include:
 - Audit scope and methodology
 - Findings and observations
 - Risk ranking and corrective action recommendations
- Final reports are reviewed by the Compliance Officer and distributed to department heads.

10.2 Corrective Action Plans (CAPs)

- Each finding is assigned a CAP with due dates, responsible owners, and milestones.
- Progress is tracked monthly.
- Unresolved findings >90 days are escalated to executive leadership.

11. Metrics and Performance Indicators

Key metrics tracked by Compliance and Security:

- % of risks mitigated within target dates
- % of audits completed on schedule
- Average time to close corrective actions
- Number of repeat audit findings
- Trend analysis on incident frequency

Reports are summarized quarterly for management review.

12. Documentation and Retention

Document Type	Retention Period	Custodian
Risk Register	6 years	Compliance Officer
Risk Assessment Reports	6 years	IT Security Officer
Audit Reports	6 years	Compliance Officer
Corrective Action Plans	6 years	Department Managers
Committee Meeting Minutes	6 years	Compliance Office

13. Enforcement

- Failure to comply with this policy may result in disciplinary actions under the Sanctions Policy (Section VI).
- Serious or willful violations may be reported to client entities or regulatory authorities.

14. Policy Review

This policy is reviewed annually by the Compliance Officer and IT Security Officer, or more frequently as regulations or business conditions change.

X. Retention and Documentation Policy

1. Purpose

The purpose of this policy is to define the documentation and record retention standards for Norman Nerds as a HIPAA Business Associate, ensuring that all compliance-related materials, operational records, and Protected Health Information (PHI) are created, maintained, retained, and destroyed in accordance with applicable federal and state requirements.

This section satisfies the following requirements:

- HIPAA Privacy Rule – 45 CFR §164.530(j) (Retention of documentation for six years).
- HIPAA Security Rule – 45 CFR §164.316(b)(1) (Maintenance of policies, procedures, and actions).
- HITECH Act §13411 (Audit and compliance evidence).
- Oklahoma Title 24 §162 (Retention of breach and notification documentation).

2. Scope

This policy applies to all:

- Business units and departments of Norman Nerds.
- Employees, contractors, and vendors managing or storing PHI or compliance records.
- All forms of documentation, including electronic, paper, and cloud-based systems.

3. Policy Statement

Norman Nerds will maintain all required HIPAA and organizational documentation for a minimum of six (6) years from the date of creation or the date when it last was in effect—whichever is later.

Records will be stored securely and accessible only to authorized personnel. Destruction of records will be completed in a manner that ensures data confidentiality and integrity.

4. Types of Documentation Covered

Category	Examples	Retention Period
Policies and Procedures	HIPAA manual, security standards, SOPs	6 years from last effective date
Training and Awareness Records	Attendance logs, training materials, certifications	6 years
Risk Assessments and Audits	Risk analysis reports, audit logs, CAPs	6 years
Breach and Incident Reports	Incident forms, investigation notes, notifications	6 years
BAA's and Legal Contracts	Business Associate Agreements, NDAs	6 years post-termination
Access Logs and System Activity Reports	Authentication records, change logs	6 years
Employee Sanction and Disciplinary Records	Violation reports, corrective actions	6 years
Compliance Committee Records	Meeting minutes, review notes	6 years
Retention and Disposal Certificates	Certificates of destruction	6 years

5. Record Creation and Control

5.1 Record Creation

- All departments must ensure that records are created at the time of relevant events (e.g., audits, incidents, policy approvals).
- Documentation must be complete, dated, and signed (physical or digital signature).

5.2 Version Control

- All controlled documents must have version numbers, revision dates, and approval records.
- Superseded versions are archived with revision history.
- The Compliance Officer maintains a Master Document Index for tracking current and historical versions.

6. Storage and Security Requirements

Storage Type	Security Requirements
--------------	-----------------------

Electronic Records	Encrypted at rest (AES-256) and in transit (TLS 1.3); access restricted via role-based permissions; backups performed daily.
--------------------	--

Paper Records	Stored in locked, fire-resistant cabinets in secure areas with controlled key access.
---------------	---

Cloud Records	Hosted only in HIPAA-compliant environments under Business Associate Agreements.
---------------	--

Access to records is limited to authorized personnel designated by the Compliance Officer, HR, or Legal Counsel.

7. Retrieval and Access

- Authorized users may request access through the Compliance Document Request Form.
- The Compliance Officer approves all requests and logs retrievals for audit tracking.
- All accesses are logged electronically and reviewed quarterly.
- Requests for PHI-related records follow Minimum Necessary standards.

8. Retention Periods and Destruction Schedule

8.1 Minimum Retention Period

All HIPAA-related records are retained for at least six (6) years from the later of:

- The date of creation, or
- The date when the record last was in effect.

8.2 Early Destruction Prohibition

No record may be destroyed before the retention period ends, except under written authorization from Legal Counsel and the Compliance Officer.

8.3 Destruction Procedures

When records reach end-of-life:

1. Electronic Media – Sanitized using NIST SP 800-88 Rev.1 standards (e.g., cryptographic wipe, degaussing).
2. Paper Records – Cross-cut shredded or incinerated; destruction witnessed by an authorized employee.
3. Certification – A Certificate of Destruction is generated and logged with the record's metadata.

8.4 Suspension of Destruction

If a record is subject to litigation, investigation, or audit, destruction is suspended under a Legal Hold Notice until written clearance is granted by Legal Counsel.

9. Backup and Archiving

- Daily encrypted backups of all compliance records are maintained offsite or in secure cloud storage.
 - Backups are verified weekly and tested quarterly for recoverability.
 - Archived data is labeled and indexed by retention period and destruction date.
-

10. Auditing and Monitoring

- The Compliance Officer conducts semi-annual record retention audits to verify completeness, integrity, and accessibility.
 - Random sampling ensures proper classification, versioning, and protection of sensitive data.
 - Non-compliance is reported under the Sanctions Policy (Section VI).
-

11. Responsibilities

Role	Responsibilities
Compliance Officer	Oversees retention program, authorizes destruction, manages audit readiness.
Legal Counsel	Reviews legal holds, approves destruction of legally sensitive documents.
Department Managers	Ensure staff compliance with record creation and storage requirements.
IT Security Officer	Maintains secure backups and encryption for electronic records.
HR Department	Retains personnel and training documentation.

12. Enforcement

Failure to adhere to this policy may result in disciplinary action, up to and including termination, and potential reporting to regulatory agencies if PHI-related records are improperly destroyed or disclosed.

13. Policy Review

This policy is reviewed annually by the Compliance Officer, Legal Counsel, and IT Security Officer. All updates are documented in Appendix F – Policy Revision Log.

XI. Continuous Improvement Policy

1. Purpose

The purpose of this policy is to ensure that Norman Nerds maintains a living, adaptive HIPAA compliance program through systematic evaluation, improvement, and documentation of its privacy and security controls. Continuous improvement ensures the organization remains compliant with evolving HIPAA, HITECH, and Oklahoma state privacy requirements, and keeps pace with technological and organizational changes.

2. Scope

This policy applies to:

- All Norman Nerds departments handling Protected Health Information (PHI).
- All employees, contractors, and business partners responsible for compliance-related activities.
- All components of the HIPAA Compliance Program, including privacy, security, training, incident response, vendor management, and risk assessments.

3. Policy Statement

Norman Nerds is committed to continuous improvement of its HIPAA Compliance Program by:

1. Conducting periodic reviews of policies and procedures to ensure effectiveness and regulatory alignment.
2. Using lessons learned from incidents, audits, and risk assessments to strengthen safeguards.
3. Encouraging employee feedback and innovation in compliance processes.
4. Documenting and tracking all improvement initiatives to demonstrate an active compliance lifecycle.

4. Regulatory Basis

This policy fulfills obligations under:

- HIPAA Security Rule (45 CFR §164.308(a)(8)) – Evaluation of security measures.
- HIPAA Privacy Rule (45 CFR §164.530(i)) – Review and modification of policies as needed.
- HITECH Act §13411 – Continuous compliance improvement and audit preparedness.
- Oklahoma Title 24 §162 – Periodic review of data protection measures.

5. Program Objectives

The Continuous Improvement Program seeks to:

- Identify opportunities to enhance compliance performance.
- Maintain an agile, proactive compliance posture.
- Integrate feedback from employees, clients, and auditors.
- Ensure rapid adaptation to new regulatory or technological developments.

6. Continuous Improvement Framework

Norman Nerds follows a Plan–Do–Check–Act (PDCA) cycle to maintain compliance maturity.

Phase Description		Deliverables
Plan	Identify gaps, risks, or new requirements; set improvement goals.	Improvement Plan, Policy Update Proposal
Do	Implement new or revised controls, training, or processes.	Updated procedures, documentation
Check	Audit and measure effectiveness of implemented changes.	Audit Reports, Metrics Dashboard
Act	Adjust and standardize improvements across the organization.	Revised policies, Compliance Officer sign-off

7. Improvement Sources

Continuous improvement actions may be initiated by:

- Results of internal audits or risk assessments.
- Findings from incident or breach reviews.
- OCR or HHS regulatory guidance updates.
- Employee or client feedback.
- Technology changes introducing new vulnerabilities or efficiencies.
- Lessons learned from industry peer benchmarks or security advisories.

8. Annual Compliance Review

- The Compliance Officer conducts a comprehensive annual compliance review assessing all HIPAA-related functions.
- Each department must submit a self-assessment report addressing:
 - Compliance achievements and gaps.
 - Completed corrective actions.
 - Planned improvements for the upcoming year.
- Findings are summarized in the Annual Compliance Review Report, presented to executive leadership and retained for six (6) years.

9. Change Management and Policy Updates

9.1 Change Identification

Changes may originate from:

- Regulatory or contractual updates.
- Security incidents or audit findings.
- New systems or data workflows involving PHI.

9.2 Approval and Implementation

1. Proposed changes are submitted to the Compliance Officer.
2. Legal Counsel reviews for regulatory impact.
3. Approved changes are incorporated into relevant policies and procedures.
4. Revisions are recorded in Appendix F – Policy Revision Log.
5. Updated versions are distributed to affected departments with acknowledgment tracking.

9.3 Communication

- All affected workforce members receive notification of updates via email or intranet portal.
- Significant policy changes trigger mandatory refresher training within 30 days of issuance.

10. Performance Measurement

Compliance effectiveness is monitored using Key Performance Indicators (KPIs):

Category	Metric	Target
Training & Awareness	Annual completion rate	≥ 98%
Incident Management	Average breach response time	≤ 5 business days
Risk Mitigation	% of mitigations closed within deadline	≥ 95%
Audit Compliance	% of findings resolved within 90 days	≥ 90%
Vendor Oversight	% of active BAAs reviewed annually	100%

Performance results are discussed during quarterly Compliance Committee meetings.

11. Feedback and Employee Participation

- Employees are encouraged to provide feedback through the Compliance Feedback Form or via direct email to the Compliance Officer.
- Anonymous suggestions are permitted and reviewed quarterly.
- Valid recommendations are documented as Improvement Initiatives and assigned to responsible departments.
- Recognition programs acknowledge employees who contribute to compliance innovation.

12. Documentation and Recordkeeping

Record Type	Retention Period	Custodian
Improvement Action Plans	6 years	Compliance Officer
Annual Compliance Review Reports	6 years	Compliance Officer
Policy Revision Logs	Permanent archive	Legal Department
KPI Metrics Dashboards	6 years	Compliance & IT Security
Employee Feedback Records	3 years	HR / Compliance

13. Roles and Responsibilities

Role	Responsibilities
Compliance Officer	Oversees continuous improvement program, approves policy updates, monitors KPIs.
IT Security Officer	Implements technical control improvements; validates effectiveness through scans and audits.
Legal Counsel	Ensures updated policies align with federal and Oklahoma statutes.
Department Managers	Integrate updates into workflows; ensure staff compliance.
All Workforce Members	Provide feedback and adhere to updated policies and procedures.

14. Review and Reporting

- The Compliance Officer prepares a Quarterly Compliance Performance Report summarizing metrics, improvements, and pending actions.
- The Executive Management Team reviews this report to prioritize resources and corrective initiatives.
- Significant compliance enhancements are logged for audit demonstration and regulatory readiness.

15. Enforcement

Failure to adhere to updated policies or to participate in improvement programs may result in disciplinary action under the Sanctions Policy (Section VI).

XII. Attestation

1. Purpose

This section serves as the formal attestation that Norman Nerds has reviewed, approved, and implemented the policies, procedures, and safeguards described within this HIPAA Compliance Policy Manual (2025 Edition). It affirms that Norman Nerds, as a Business Associate under HIPAA, is committed to maintaining full compliance with the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and all applicable provisions of the HITECH Act and Oklahoma privacy and data protection laws.

2. Organizational Commitment

Norman Nerds recognizes the importance of safeguarding Protected Health Information (PHI) and ensuring that privacy and security standards are integrated into all aspects of its operations.

Through this attestation, the company acknowledges its responsibility to:

1. Uphold the confidentiality, integrity, and availability of PHI.
2. Enforce the policies and procedures detailed in this manual.
3. Provide regular training, risk assessments, and audits to sustain compliance.
4. Promptly report and mitigate any data breaches or unauthorized disclosures.
5. Maintain documentation and evidence of compliance activities for at least six (6) years.

3. Executive Certification

The undersigned officers of Norman Nerds certify that they have reviewed and approved the HIPAA Compliance Policy Manual as of the effective date below.

They attest that the policies contained herein reflect the company's official procedures and that all workforce members are required to comply with them.

Authorized by:

Name: _____

Title: Chief Executive Officer / Managing Partner

Signature: _____

Date: _____

Name: _____

Title: Compliance Officer

Signature: _____

Date: _____

4. Employee Acknowledgment

Each employee, contractor, and volunteer with access to PHI or ePHI must sign this acknowledgment to confirm understanding and compliance with this manual.

I acknowledge that I have received, read, and understood the Norman Nerds HIPAA Compliance Policy Manual (2025 Edition).

I understand my responsibilities to protect PHI and comply with all applicable federal and state privacy and security regulations.

I agree to adhere to all policies, procedures, and reporting obligations described in this manual.

I understand that violations of these policies may result in disciplinary action, termination, or legal penalties.

I also acknowledge that my confidentiality obligations continue indefinitely after my employment or engagement with Norman Nerds ends.

Employee Name: _____

Position/Department: _____

Signature: _____

Date: _____

Supervisor Signature: _____

5. Distribution and Version Control

Version Date		Change Summary	Approved By	Effective Date
1.0	November 2025	Initial publication of Norman Nerds HIPAA Compliance Policy Manual	Compliance Officer	11/15/2025
1.1	Pending	Future updates and amendments	TBD	TBD

All current and historical versions of this manual are maintained in the Compliance Repository and governed under Appendix F – Policy Revision Log.

Each department is responsible for maintaining the most recent version accessible to all staff.

6. Certification Statement

This HIPAA Compliance Policy Manual and all supporting procedures are officially adopted by Norman Nerds as of the date below.

The manual supersedes all prior HIPAA or data protection policies.

It shall remain in effect until modified or replaced by an updated version approved by the

Compliance Officer and Executive Management.

Effective Date: _____

Authorized Signature (Compliance Officer): _____

Authorized Signature (CEO/Managing Partner): _____

Appendices

Appendix A — Business Associate Agreement (BAA) Template

1. Purpose

This template establishes the required contractual relationship between Norman Nerds (“Business Associate”) and a client healthcare provider (“Covered Entity”) or subcontractor (“Sub-Business Associate”), ensuring compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

2. Agreement Sections

A. Definitions

Terms used in this Agreement have the same meanings as in HIPAA and the HITECH Act, including *PHI*, *Breach*, *Business Associate*, and *Covered Entity*.

B. Obligations of the Business Associate

1. Implement administrative, physical, and technical safeguards to protect PHI.
2. Use and disclose PHI only as permitted by the Agreement or required by law.
3. Report any Breach or security incident to the Covered Entity within 10 business days.
4. Ensure all subcontractors with PHI access agree to equivalent restrictions via written BAAs.
5. Make available PHI as necessary to allow Covered Entity compliance with patient rights.
6. Maintain documentation for at least six (6) years.
7. Return or destroy all PHI upon termination of the Agreement.

C. Permitted Uses and Disclosures

Business Associate may use PHI solely to perform services defined in the underlying Service Agreement.

D. Termination

- Covered Entity may terminate for cause upon knowledge of material noncompliance.
- Upon termination, Business Associate must return or securely destroy all PHI within 30 days.

E. Indemnification

Each party agrees to indemnify and hold harmless the other from losses due to its own noncompliance.

F. Miscellaneous

- Agreement is governed by U.S. federal and Oklahoma law.
- Survival: Privacy and confidentiality obligations survive termination.

Signatures:

Covered Entity	Business Associate (Norman Nerds)
Name: _____	Name: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Appendix B — Breach Report Form

Purpose:

Used by any workforce member to report a suspected or confirmed breach involving PHI or ePHI.

Field	Details / Instructions
Reporter Name / Title	
Department	
Date / Time of Discovery	
Description of Incident	Describe what happened and how it was discovered.
Systems or Data Affected	Identify databases, servers, or applications.
Type of PHI Involved	e.g., names, SSNs, medical records, billing info
Approximate Number of Records	
Individuals Potentially Affected	
Containment Actions Taken	e.g., disabled account, isolated server
Date / Time Reported to Compliance Officer	
Follow-Up Required	Yes / No
Root Cause (if known)	
Signatures (Reporter / Compliance Officer)	

- Instructions:
- Submit immediately upon discovery to the HIPAA Security Officer.
 - Attach screenshots, logs, or evidence.
 - Retain completed form for six (6) years.

Appendix C — Risk Assessment Template

Purpose:

Used to evaluate vulnerabilities and determine the likelihood and impact of risks to PHI.

Asset / Process	Threat or Vulnerability	Likelihood (1–5)	Impact (1–5)	Risk Score (L×I)	Existing Controls	Additional Safeguards Needed	Responsible Party	Target Date
EHR Cloud Storage	Misconfiguration or unauthorized access	3	5	15	MFA, encryption	Quarterly access review	IT Security	Q1 2026
Vendor API Integration	Weak token authentication	4	4	16	Token rotation policy	Implement signed JWTs	DevOps	Q2 2026
Employee Email	Phishing and credential theft	4	5	20	Email filtering, MFA	Phishing simulations	Security Officer	Ongoing

Risk Rating Key:
1–5 = Low; 6–10 = Moderate; 11–20 = High; >20 = Critical
Review Frequency: Annually or after significant changes.

Appendix D — Workforce Acknowledgment Form

I, the undersigned, acknowledge that I have received, read, and understand the Norman Nerds HIPAA Compliance Policy Manual (2025 Edition).
I agree to abide by all policies, procedures, and responsibilities related to the protection of PHI and ePHI. I understand that any violation of these policies may result in disciplinary action, termination, and potential civil or criminal penalties.
Employee/Contractor Name: _____
Title/Department: _____
Signature: _____
Date: _____
Supervisor/Manager Signature: _____
Retention: 6 years from employee separation.

Appendix E — Annual Audit Checklist

Purpose:
To verify compliance with HIPAA Privacy, Security, and Breach Notification Rules.

Audit Category	Verification Items	Compliant (Y/N)	Findings / Notes	Responsible Person
Administrative Safeguards	Risk assessment conducted within 12 months; policies reviewed; training logs up to date			Compliance Officer
Technical Safeguards	Access control, encryption, and audit logs functioning properly			IT Security
Physical Safeguards	Facility access logs maintained; device disposal documented			Facilities
Vendor Oversight	Active BAAs current; vendor assessments reviewed			Procurement
Breach Response	Incident logs complete; response times within limits			Compliance Officer

Completion Date: _____
Auditor Name: _____
Next Review Due: _____

Appendix F — Policy Revision Log

Purpose:
To maintain documentation of revisions, version history, and approvals for all HIPAA policies.

Version Date		Policy or Section Revised	Summary of Changes	Approved By	Effective Date
1.0	Nov 2025	Full Manual	Initial release for Norman Nerds HIPAA Compliance Program	Compliance Officer	11/15/2025
1.1	TBD	All Sections	Annual review and updates per HHS guidance	Compliance Officer & Legal Counsel	TBD
1.2	TBD	Appendix B, D	Revised forms for new breach reporting standards	Compliance Officer	TBD

Retention: Permanent record.
Custodian: Compliance Officer.

Appendix G — Artificial Intelligence (AI) Acceptable Use, Governance & Risk Management Policy

1. Purpose
This policy establishes governance standards for the secure, compliant, and risk-managed use of Artificial Intelligence (AI) technologies within Norman Nerds ProActive CyberSecurity MSP IT Services and in services provided to healthcare clients. This policy is designed to:

- Protect Protected Health Information (PHI)
- Maintain compliance with HIPAA and HITECH
- Meet cybersecurity insurance underwriting requirements
- Reduce regulatory, legal, and operational risk
- Prevent data leakage into unauthorized AI systems
- Establish documented AI governance controls

2. Scope
This policy applies to:

- All employees, contractors, and consultants
- All AI-enabled platforms and software
- Generative AI systems (e.g., ChatGPT, Microsoft Copilot, Gemini, etc.)
- AI-integrated cybersecurity platforms
- AI tools used in healthcare client environments
- Any AI tool capable of processing, analyzing, generating, or storing sensitive data

3. Definitions

Artificial Intelligence (AI): Software systems that simulate human intelligence processes including content generation, pattern recognition, or automated decision-making.

Generative AI: AI capable of creating text, code, images, summaries, or other outputs.

Protected Health Information (PHI): Individually identifiable health information as defined under HIPAA (45 CFR §160.103).

De-Identified Data: Health information stripped of identifiers in accordance with HIPAA Safe Harbor or Expert Determination standards.

Sensitive Data: PHI, PII, financial data, authentication credentials, security configurations, client documentation, insurance materials, and proprietary data.

4. AI Use in Healthcare Client Environments

Norman Nerds recognizes that healthcare environments require heightened regulatory controls.

4.1 PHI Restrictions

AI tools may not process PHI unless:

- A signed Business Associate Agreement (BAA) is executed with the AI vendor
- The vendor provides documented HIPAA compliance controls
- Encryption is enforced in transit and at rest
- Access is protected by Multi-Factor Authentication (MFA)
- Logging and audit capabilities are enabled

Public/free AI platforms are considered non-HIPAA compliant unless documented otherwise.

4.2 De-Identification Requirement

If AI tools are used for:

- Documentation drafting
- Policy development
- Clinical workflow assistance
- Reporting templates
- Training materials

All PHI must be de-identified prior to input unless a compliant BAA exists.

4.3 Healthcare-Specific Prohibited Uses

The following are strictly prohibited:

- Entering patient names or identifiers into public AI tools
- Uploading medical records to generative AI systems
- Using AI to independently generate medical diagnoses or treatment decisions
- Using AI outputs as a substitute for licensed clinical judgment
- Uploading EHR exports into non-approved AI platforms

4.4 Clinical Decision Safeguards

AI tools used in healthcare environments:

- Must function as support tools only
- May not replace licensed medical judgment
- Must undergo validation before integration into clinical workflows
- Must not be used for autonomous treatment recommendations

5. Approved AI Tool Requirements

All AI tools must meet the following minimum security standards:

- Documented security architecture
- Encryption (TLS 1.2+ minimum)
- MFA enforcement
- Administrative oversight capability
- Logging and monitoring support
- Data retention transparency
- Explicit disclosure of model training practices
- Ability to opt out of data used for model training (when applicable)

Shadow AI is strictly prohibited.

6. Cybersecurity Insurance Compliance Controls

To maintain insurability and meet underwriting requirements:

- AI platforms must not allow regulated data to enter public training datasets.
- Enterprise-grade AI subscriptions must be used instead of consumer/free plans.
- Data-sharing and model training opt-in features must be disabled when possible.
- Administrative logging must be enabled.
- AI-generated content must undergo human review prior to distribution.
- AI usage must align with the organization's Incident Response Plan.
- Access to AI tools must be role-based and least privilege.

7. AI Risk Assessment Framework (For Insurance & Audit Purposes)

Norman Nerds maintains a documented AI Risk Assessment process that includes:

7.1 Risk Identification

Each AI system is evaluated for:

- PHI exposure risk
- Data leakage potential
- Third-party data processing risks
- Vendor financial stability
- Regulatory compliance gaps
- Reputational impact
- Operational dependency risks

7.2 Risk Classification

AI systems are categorized as:

- **Low Risk:** No sensitive data exposure
 - **Moderate Risk:** Internal business data exposure
 - **High Risk:** PHI or regulated data exposure
 - **Prohibited:** Uncontrolled public AI with no security assurances
-

7.3 Vendor Due Diligence Review

Before approval, vendors must provide:

- SOC 2 Type II (preferred)
- Security whitepaper
- Data retention policy
- Incident response documentation
- Subprocessor disclosures
- BAA (if PHI involved)

7.4 Technical Control Review

Security team verifies:

- MFA enforcement
- Encryption standards
- Admin controls
- Logging capability
- Data isolation architecture
- Access control configuration

7.5 Ongoing Monitoring

Approved AI tools are:

- Reviewed annually
- Re-evaluated upon major vendor changes
- Audited if regulatory updates occur
- Reassessed after security incidents

8. Human Oversight & Validation

AI-generated outputs:

- Must be reviewed by a qualified human prior to client delivery
- May not be relied upon for compliance determinations without verification
- Must be validated before inclusion in healthcare documentation
- Must not replace professional cybersecurity, legal, or medical review

9. Incident Reporting & Breach Response

Any suspected exposure of PHI or sensitive data through AI tools must be reported immediately to:

Eric Crawford

Owner

Norman Nerds ProActive CyberSecurity MSP IT Services

Phone: 405-203-9358

Incidents will be evaluated under:

- The HIPAA Breach Notification Rule
 - The organization's Incident Response Plan
 - Cybersecurity insurance reporting requirements
-

10. Training Requirements

All staff must:

- Complete annual HIPAA training (if servicing healthcare clients)
- Complete cybersecurity awareness training
- Receive AI governance training before accessing AI tools
- Acknowledge this policy in writing

11. Policy Violations

Violations may result in:

- Immediate suspension of AI access
- Disciplinary action
- Termination
- Regulatory reporting (if required)
- Insurance carrier notification (if required)

12. Policy Review & Governance

This policy will be reviewed:

- Annually
- Upon regulatory change
- Upon cybersecurity insurance renewal
- After any AI-related security incident

Norman Nerds