Draft LLM HIPAA Audit Program - Evergreen Valley Medical Center

Conducted by Alexos security LLC

By Lazar Strulovitch

Apr, May, 2025

This document outlines an audit program for a newly implemented Large Language Model (LLM) designed to support diagnostics for practitioners at Evergreen Valley Medical Center.

We (Alexos security) have been contracted by Evergreen Valley Medical Center to perform this audit. Evergreen recognizes the critical importance of being at the forefront of technology, but also fully understands the necessity for rigorous oversight when managing highly sensitive and regulated information, such as Protected Health Information (PHI).

Executive Summary

This document outlines our planned HIPAA compliance audit of the DeepSeek R1 LLM deployment at Evergreen Valley Medical Center. Its sole purpose is to define the audit approach, methodology, procedures, and evidence-gathering steps we will follow to verify adherence to the HIPAA Privacy and Security Rules as they apply to AI systems. **This is strictly a compliance-audit plan**—it does **not** perform or replace a formal risk analysis or risk management process.

Intended Audience

This document is written for:

Executive Leadership & Board to understand high-level compliance posture and residual risks.

CISO & Security Operations to guide technical verification and monitoring activities.

Privacy & Compliance Officers to confirm HIPAA Privacy and Security Rule obligations are met in AI contexts.

IT/EHR Administrators to implement any required configuration changes and emergency procedures.

External Auditors & Regulators as evidence of the audit approach, criteria, and findings.

Our (Alexos security) involvement

Our engagement commenced in an advisory capacity, where our initial focus was on establishing a HIPAA-first architecture for the LLM implementation. This document details the work undertaken to configure and fine-tune the LLM in a manner that effectively mitigates the risk of exposing PHI.

During the initial advisory phase, we proposed several key strategies:

1. **Utilizing an advanced, open-source LLM:** Selecting a model that possesses the trust of the Free and Open-Source Software (FOSS) community and can be deployed locally.
2. **Creating a HIPAA-first architecture:** Designing the system from the ground up with HIPAA compliance as the foundational principle.

3. **Exercising heightened caution with access controls:** Given the novel nature of this technology and the absence of established official guidelines, implementing stringent access controls for both the LLM itself and the users accessing this powerful tool is essential.
4. **Developing a comprehensive training program:** Establishing a training and periodic retraining program to educate users on the technology's capabilities and limitations, specifically emphasizing the LLM's propensity for hallucination (generating incorrect or misleading information).
5. **Conducting a thorough audit:** Performing a comprehensive audit to validate the effectiveness of the implemented controls.
6. **Providing a streamlined patient opt-out mechanism:** Implementing a straightforward process for patients to easily opt out of allowing the LLM access to their data.

Evergreen Valley Medical Center, conducted a risk assessment, as mandated by the HIPAA Security Rule § 164.308(a)(1), and determined that DeepSeeK R1 was the safest and most appropriate LLM for their operational needs.

DeepSeek R1 is widely regarded as one of the best open-source reasoning models available in 2025, especially noted for its strong logical inference, mathematical problem-solving, and multi-domain reasoning capabilities. It features a large context window (128K tokens), multilingual support, and an efficient Mixture of Experts architecture, making it versatile and cost-effective compared to proprietary models like OpenAI o1.

Several critical issues were identified and addressed immediately during the initial phase:

Data for Fine-Tuning the LLM

Effective fine-tuning of an LLM, particularly in a healthcare setting, necessitates data, often involving human feedback, to make the model a genuinely useful tool for assisting physicians in patient diagnostics, asking relevant questions, and

identifying similar cases. However, in accordance with the HIPAA Privacy Rule, the use of patient data for the treatment of *other* patients is generally prohibited.

The U.S. Department of Health & Human Services (HHS) permits the disclosure of PHI without consent primarily for "Treatment, Payment, [and] Health Care Operations." To ensure compliance, our approach will involve applying tokenization or de-identification to PHI prior to model ingestion. This process ensures that the data used for training is stripped of Protected Personal Information (PPI), allowing the LLM to be trained solely on this de-identified data.

Mitigating Improper Access to Patient Data

A primary concern was mitigating the risk of improper access to patient data by the LLM. Given the inherent unpredictability of LLMs, ensuring that the model does not inadvertently access data belonging to other patients is paramount. A desired capability was the LLM's ability to reference pertinent prior cases.

To address this, we proposed utilizing de-identified case data for the LLM's primary reasoning processes. Full patient data will remain accessible only within the Electronic Health Record (EHR) system, contingent upon user authorization and strict access management by the EHR system itself. This approach leverages the existing access controls within the EHR system, effectively eliminating the need for redundant, specialized access controls specifically for the LLM in this context. This also facilitates the cross-referencing of patient cases by enabling the LLM to reference cases with tokenized and de-identified PHI.

(See Illustration 1.1 below)

Illustration 1.1: Proposed Data Flow

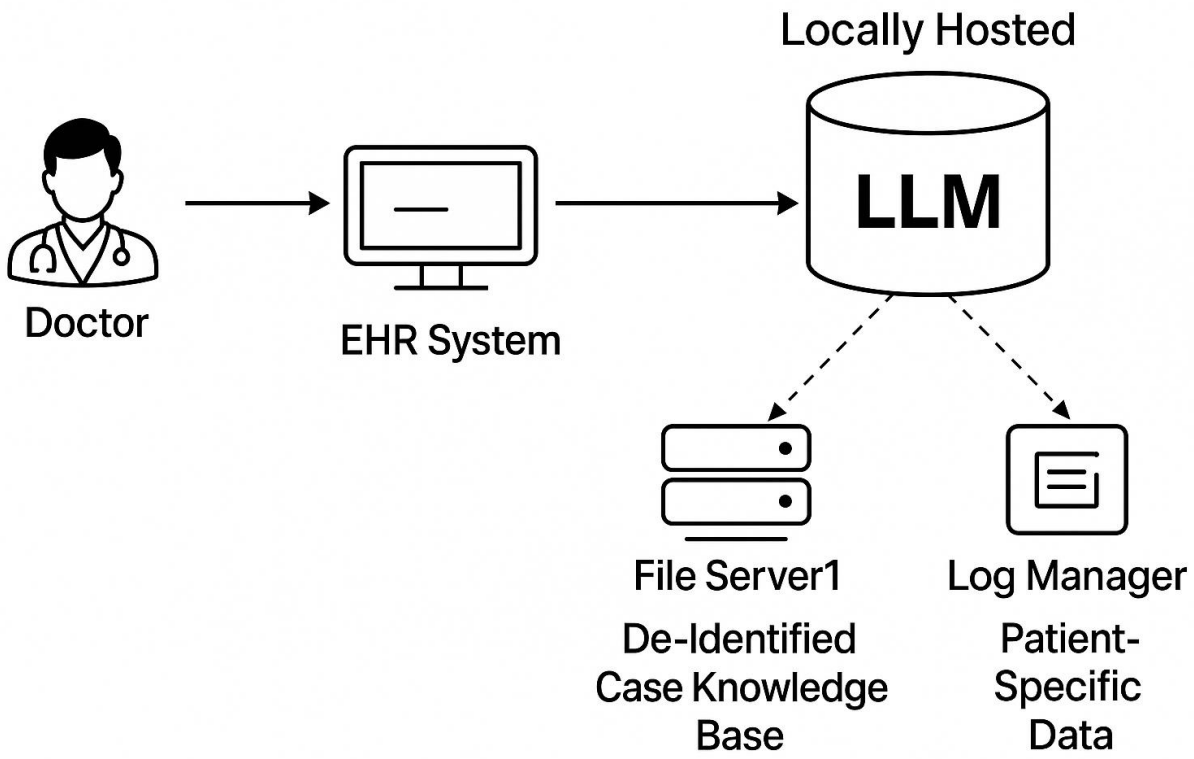


Illustration 1.1

This approach also assists with cross-referencing patient cases by bringing up cases with tokenized and de-identified PHI.

Scope of the Audit

The scope of this audit is narrowly focused on the newly implemented LLM technology. We assume that Evergreen Valley Medical Center, maintains full compliance with existing HIPAA regulations and other relevant regulatory agencies. Our specific focus is on the augmented risks introduced by the integration of this technology.

This audit and the structure of this document will adhere to the guidelines set forth in NIST SP 800-66r2, An Introductory Resource Guide for Implementing the HIPAA Security Rule. Technical security aspects will align with NIST Special Publication 800-123, Guide to General Server Security.

To clarify our role in Evergreen Valley Medical Center's governance framework, this HIPAA compliance audit sits in the **Third Line of Defence**:

1. **First Line (Operational Management)**
    - Clinical teams, IT operations, and system administrators who design, implement, and maintain controls around DeepSeek R1 (e.g., encryption, access roles, monitoring).
2. **Second Line (Risk Management & Compliance)**
    - Security, privacy, and compliance functions that define policies, perform control self-assessments, and provide guidance on HIPAA requirements for AI deployments.
3. **Third Line (Internal Audit) ← Our Audit**
    - An independent function that evaluates the effectiveness of both first- and second-line controls, conducts objective testing of administrative, physical, and technical safeguards, and reports findings directly to executive leadership and the board.

By positioning this audit in the Third Line, we ensure full independence from those who design and operate DeepSeek R1, delivering unbiased assurance on HIPAA compliance.

Understanding HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA), enacted on August 21, 1996 (Public Law 104-191), was established with the objectives of streamlining electronic healthcare transactions, combating waste and fraud, and setting national standards for the privacy and security of protected health information (PHI).

Key components of HIPAA relevant to this audit include:

- The Privacy Rule: Published in December 2000 and enforced by the Office for Civil Rights (OCR).
    - Key Provisions:
        - Notice of Privacy Practices: Covered entities are required to inform individuals regarding the uses and protections of their PHI.
        - Individual Rights: Individuals possess the right to access and obtain a copy of their PHI, request amendments, and receive an accounting of disclosures.
        - Use & Disclosure: Limits the use and disclosure of PHI to the minimum necessary for treatment, payment, or healthcare operations. Most other disclosures necessitate patient authorization.
- The Security Rule: With its final rule published in February 2003 and finalized in the 2013 Omnibus HIPAA Final Rule, this rule establishes national standards for safeguarding electronic protected health information (ePHI).
    - Covered entities must:

- Ensure the confidentiality, integrity, and availability (CIA) of all ePHI that is created, received, maintained, or transmitted.
- Implement protections against any reasonably anticipated threats and hazards to the security or integrity of ePHI.
- Guard against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.
- Ensure compliance with the Security Rule by its workforce.

The Security Rule is enforced by the Centers for Medicare & Medicaid Services (CMS). Our primary focus in this audit is the Security Rule.

A key principle of the Security Rule is the "Flexibility of Approach," which permits regulated entities to tailor the implementation of HIPAA's Security Rule requirements. The specific cybersecurity practices will vary based on an organization's size, complexity, technical infrastructure, and existing hardware, software, and security capabilities. For additional details on the Security Rule's flexibility of approach, refer to § 164.306(b) of the HIPAA Security Rule.

In complying with this section, regulated entities must be cognizant of the definitions for confidentiality, integrity, and availability as provided in § 164.304 of the Security Rule:

- Confidentiality: Defined as "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity: Defined as "the property that data or information have not been altered or destroyed in an unauthorized manner."
- Availability: Defined as "the property that data or information is accessible and useable upon demand by an authorized person." (Source: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide)

Key concepts within the Security Rule include "Flexibility of Approach," indicating that the HHS does not mandate specific technologies, allowing for substitutions, and the requirement for covered entities to assess their unique environment and risks to determine "reasonable and appropriate" security measures. This determination is highly dependent on the organization's size, resources, and risk assessments.

The Security Rule mandates the implementation of Administrative Safeguards, Physical Safeguards, and Technical Safeguards to ensure the Confidentiality, Integrity, and Availability (CIA) of ePHI.

Our audit will be organized in accordance with the following six sections outlined in NIST SP 800-66r2:

- Security Standards: General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

(See Charts 2.1 and 2.2 below)

Standard	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R)

Standard	Sections	Implementation Specifications (R) = Required, (A) = Addressable
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

Chart 2.2 from NIST SP 800-66r2

Risk Assessment and Risk Management

Within the framework of the HIPAA Security Rule, protecting Electronic Protected Health Information (ePHI) is fundamentally a process of **Risk Management**. This involves a cyclical approach to understanding and addressing potential threats and vulnerabilities.

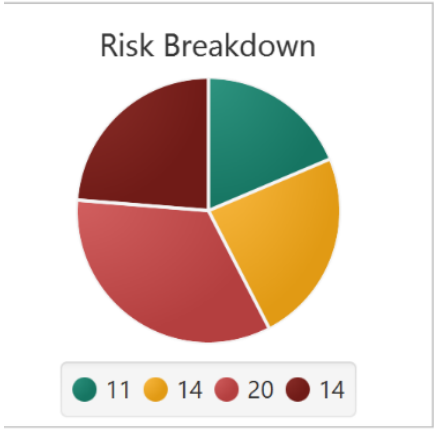
1. **Risk Assessment:** The initial step in Risk Management is the **Risk Assessment**. This is the process of identifying potential threats and vulnerabilities to ePHI within an organization's specific environment, determining the likelihood of a harmful event occurring, and estimating the potential impact of such an event on the confidentiality, integrity, and availability of ePHI. The output of a Risk Assessment is a comprehensive understanding of the risks faced, often documented and prioritized. Evergreen Hospital completed this crucial step, utilizing the HHS Security Risk Assessment (SRA) tool, and determined that DeepSeeK R1 was the appropriate choice after assessing potential risks associated with implementing an LLM. The detailed risk assessment report serves as a foundational document and will be appended to this report.
2. **Risk Management:** Building upon the findings of the Risk Assessment, **Risk Management** encompasses the ongoing processes and controls implemented to mitigate, transfer, accept, or avoid the identified risks. This includes selecting and implementing appropriate security measures, establishing policies and procedures, training the workforce, and

continuously monitoring the environment. The HIPAA Security Rule's required safeguards (Administrative, Physical, and Technical) are examples of the types of controls implemented as part of Risk Management to address identified risks.

Our Role: A Regulatory Compliance Audit as part of Risk Management

Our engagement constitutes a **HIPAA Compliance Audit**, which is a specific activity performed *within* Evergreen Hospital's broader Risk Management program. The objective of this audit is not to conduct a new, comprehensive vulnerability assessment or to provide a granular listing of every potential technical vulnerability and its corresponding mitigation control, as might be found in a detailed technical risk assessment report.

Instead, this audit focuses on assessing whether the **HIPAA Security Rule safeguards** – the mandatory controls required by the regulation as part of a compliant risk management strategy – have been appropriately selected, implemented, and are operating effectively in relation to the newly introduced LLM technology. We will systematically review the implementation of these safeguards as outlined in NIST SP 800-66r2, verifying compliance with the regulatory requirements. This process provides assurance to Evergreen Hospital that their risk management efforts, specifically concerning the LLM, align with federal mandates for protecting ePHI.



Risk Assessment Rating Key		Impact		
		Acceptable little to no effect	**Tolerable** moderate effect	**Intolerable** critical effect
Likelihood	**Improbable** risk unlikely to occur	Low	Medium	High
	Possible risk likely to occur	Low	Medium	Critical
	Probable risk will occur	Medium	High	Critical

This matrix is your single-page view of how our DeepSeek R1 AI system aligns with each HIPAA Security Rule requirement. It shows, in plain language, what we intend to safeguard patient data in this novel LLM deployment—and how we can be confident that each control is working.

Column	What It Means
Cat	Safeguard type: **AD** = Administrative, **PH** = Physical, **TH** = Technical.
Standard & Section	The exact HIPAA citation (e.g. §164.308(a)(1)) tied to each control.
Implementation Spec.	Whether the control is **Required (R)** or **Addressable (A)** under HIPAA, plus its name.
Specific Control	How DeepSeek R1 meets that HIPAA requirement—using language and examples specific to our AI architecture.
Sub-Controls	1–3 concrete "best practice" options that strengthen the core control (e.g. MFA choices, cache-purge settings, enclave use).
Verification Method	Exactly how the auditor can confirm the control is in place—logs to review, tests to run, documents to inspect.
Residual Risk	After applying the control, the remaining risk level: **Low**, **Medium**, or **High**.

Cat	Standard	Section	Implementation Specification	Specific Control	Sub-Controls	Verification Method	Residual Risk
AD	Security Management Process	Â§164.308(a)(1)	Risk Analysis (R)	Conduct a comprehensive risk analysis focusing on DeepSeek R1s use of ePHI (prompt injection, memory leaks, training-data exposure); update annually or with major changes	Include LLM-specific threat modeling; perform red-team PHI-leak tests; reevaluate risks after retraining	Review risk analysis document for LLM sections; interview LLM security officer	Low
AD	Security Management Process	Â§164.308(a)(1)	Risk Management (R)	Implement a risk management plan that mitigates DeepSeek R1 risks (restrict training to tokenized data, enhanced monitoring); track status regularly	Allow fine-tuning only on de-identified data; require change control for model updates; maintain an LLM risk register	Examine LLM risk plan and mitigation evidence; verify action items closed	Low
AD	Security Management Process	Â§164.308(a)(1)	Sanction Policy (R)	Include DeepSeek R1 misuse (unauthorized PHI prompts, use of external LLMs) in sanction policy; publicize consequences	Add AI-misuse examples; monitor LLM usage; involve HR on violations	Confirm policy update; review any LLM-related sanctions	Low

AD	Security Management Process	Â§164.308(a)(1)	Information System Activity Review (R)	Review DeepSeek R1 logs weekly/monthly for anomalies (bulk queries, off-hours access, PHI in outputs)	Integrate logs into SIEM; alert on abnormal patterns; sample manual review of LLM outputs	Check SIEM alert reports; inspect log-review tickets	Low
AD	Assigned Security Responsibility	Â§164.308(a)(2)	Assigned Security Responsibility (R)	Assign a dedicated LLM Security Officer for DeepSeek R1 oversight; schedule regular compliance reviews	Document LLM security role; hold quarterly LLM status meetings	Verify org chart and role description; interview the LLM Security Officer	Low
AD	Workforce Security	Â§164.308(a)(3)	Authorization and/or Supervision (A)	Grant DeepSeek R1 access by role (clinician vs. non-clinical); supervise initial PHI queries	Configure DeepSeek R1 roles; require managerial approval; monitor first sessions	Review access requests; verify supervised onboarding	Medium
AD	Workforce Security	Â§164.308(a)(3)	Workforce Clearance Procedure (A)	Ensure DeepSeek R1 users complete HIPAA & LLM-specific training before access	Use checklist verifying training & background; require dept-head sign-off	Audit training records for active LLM users	Medium

AD	Workforce Security	Â§164.308(a)(3)	Termination Procedures (A)	Automatically revoke DeepSeek R1 access on HR offboarding via IAM integration; quarterly audits	Link to EHR system; audit accounts	Cross-check terminated users vs. LLM accounts; inspect deprovision logs	Low
AD	Information Access Management	Â§164.308(a)(4)	Isolating Health Care Clearinghouse Function (R)	Ensure DeepSeek R1 only accesses treatment/operations data; block clearinghouse systems	Enforce network segmentation; policy restricting LLM to EHR modules	non-applicable	Low
AD	Information Access Management	Â§164.308(a)(4)	Access Authorization (A)	Inherit EHR role-based AC DeepSeek R1 only accepts EHR-authenticated requests	Leverage EHR ACLs; disable standalone LLM accounts	Attempt LLM login without EHR token; review ACL export	Low
AD	Information Access Management	Â§164.308(a)(4)	Access Establishment and Modification (A)	Mirror EHR provisioning DeepSeek R1 grants/revokes access on EHR user-change events	Subscribe to EHR event stream; synchronize user directory	Inspect event logs; compare LLM vs. EHR user lists	Low
AD	Security Awareness and Training	Â§164.308(a)(5)	Security Reminders (A)	Distribute periodic LLM-focused security tips (PHI-leak avoidance, AI-hallucination handling)	Include LLM topics in newsletter; use login-popup reminders	Review communications; survey users for awareness	Medium

AD	Security Awareness and Training	Â§164.308(a)(5)	Protection from Malicious Software (A)	Harden DeepSeek R1 hosts in isolated containers/VMs; warn against executing LLM-suggested code unvetted	Apply network isolation; includes malware-caution in training	Verify container configs; inspect training slides	Medium
AD	Security Awareness and Training	Â§164.308(a)(5)	Log-in Monitoring (A)	Alert on LLM login anomalies (failed attempts, off-hours) via SIEM	Enable SIEM alerts for auth failures; monitor trends	Check SIEM logs; test alert on failed login	Medium
AD	Security Awareness and Training	Â§164.308(a)(5)	Password Management (A)	Enforce SSO/MFA for DeepSeek R1 via EHR; vault service-account keys	Require push-MFA; rotate service keys	Attempt login without MFA; review SSO config	Medium
AD	Security Incident Procedures	Â§164.308(a)(6)	Response and Reporting (R)	Include LLM breach scenarios (PHI leakage, prompt injection) in IR plan; train team	Develop AI-incident playbook; conduct breach drills	Review IR plan; inspect drill after-action reports	Low
AD	Contingency Plan	Â§164.308(a)(7)	Data Backup Plan (R)	Backup DeepSeek R1 data (model state, logs, embeddings) daily to encrypted offsite storage	Automate encrypted backups; maintain checksums; retain versions	Verify backup logs; confirm recent restore test	Low

AD	Contingency Plan	Â§164.308(a)(7)	Disaster Recovery Plan (R)	Maintain a standby environment for DeepSeek R1; document failover steps; test annually	Provision alternate environment; run DR test	Review DR plan; inspect DR-test report	Low
AD	Contingency Plan	Â§164.308(a)(7)	Emergency Mode Operation Plan (R)	Define LLM emergency mode. Its not a tool we need in a Emergency	Provide offline dataset; train fallback procedures	Examine emergency-ops doc; interview staff	Low
AD	Contingency Plan	Â§164.308(a)(7)	Testing and Revision Procedure (A)	Test LLM contingency (backup/DR/emergency) annually; update plans post-test	Schedule annual drills; revise plan based on findings	Review test records; compare plan versions	Medium
AD	Contingency Plan	Â§164.308(a)(7)	Applications and Data Criticality Analysis (A)	Rank DeepSeek R1 and its data by clinical criticality to prioritize recovery	Assign criticality tiers; revisit upon scope changes	Review criticality analysis; verify priority list	Medium
AD	Evaluation	Â§164.308(a)(8)	Evaluation (R)	Conduct annual HIPAA evaluation covering DeepSeek R1 controls and architecture; perform pen tests	Engage external auditor; quarterly self-assessment	Check evaluation reports; confirm remediation	Low

AD	Business Associate Contracts and Other Arrangements	Â§164.308(b)(1)	Written Contract or Other Arrangement (R)	Maintain BAAs with all DeepSeek R1 vendors (cloud, integrators) including HIPAA-AI terms	Inventory vendors; store signed BAAs; include right-to-audit clauses	Review BAA repository; inspect sample contracts	Low
PH	Facility Access Controls	Â§164.310(a)(1)	Contingency Operations (A)	Authorize emergency badge access to LLM server room with logged override	Issue emergency keycards; log usage	Verify access list; inspect logs	Low
PH	Facility Access Controls	Â§164.310(a)(1)	Facility Security Plan (A)	Document physical safeguards for LLM hardware (locks, CCTV, climate control);	Map server area; schedule quarterly walkthroughs	Review plan; Test controls in place	Medium
PH	Facility Access Controls	Â§164.310(a)(1)	Access Control and Validation Procedures (A)	Enforce multi-factor door access (badge + biometric) for LLM area; escort visitors	Implement MFA doors; log visitor entries	Inspect door system; review visitor logs	Medium
PH	Facility Access Controls	Â§164.310(a)(1)	Maintenance Records (A)	Log all LLM hardware maintenance (drive swaps, lock repairs) with chain of custody	Use ticketing system; supervise hardware changes	Examine logs; verify chain-of-custody records	Medium
PH	Workstation Use	Â§164.310(b)	Workstation Use (R)	Restrict LLM use to hospital-approved secure devices; forbid public/personal devices for PHI	Update use policy; require annual user attestations	Check attestations; perform spot-checks	Low

PH	Workstation Security	Â§164.310(c)	Workstation Security (R)	Enforce auto-lock (5 min), privacy screens, and software controls on LLM workstations	Configure group policy; install cable locks	Observe settings; inspect policy config	Low
PH	Device and Media Controls	Â§164.310(d)(1)	Disposal (R)	Sanitize or destroy media containing LLM PHI (SSD: crypto-erase; HDD: degauss; paper: cross-cut shred)	Use certified vendor; retain destruction certificates	Review certificates; inspect storage area	Low
PH	Device and Media Controls	Â§164.310(d)(1)	Media Re-use (R)	Wipe or cryptographically erase LLM drives before reuse; label cleared media	Automate wipe with audit report;	Inspect wipe logs; verify cryptographic erase	Low
PH	Device and Media Controls	Â§164.310(d)(1)	Accountability (A)	Maintain inventory of all LLM hardware and media; log custody and transfers	Use asset-management system; perform annual audits	Reconcile inventory; spot-check devices	Medium
PH	Device and Media Controls	Â§164.310(d)(1)	Data Backup and Storage (A)	Store backup media in locked safe offsite or encrypted cloud with access controls	Safe + offsite vault; HIPAA-compliant cloud	Inspect storage site; review compliance report	Medium
TH	Access Control	Â§164.312(a)(1)	Unique User Identification (R)	Use EHR SSO DeepSeek R1 sessions require valid EHR tokens; no standalone credentials	Enforce EHR token validation; disable generic accounts	Attempt login without token; review SSO config	Low

TH	Access Control	Â§164.312(a)(1)	Emergency Access Procedure (R)	Implement break-glass LLM account activated by admin in emergencies; alert on use	Store disabled account; audit break-glass events	Simulate break-glass; check alert logs	Low
TH	Access Control	Â§164.312(a)(1)	Automatic Logoff (A)	Expire LLM sessions after 5 min inactivity; flush context on logout	Set timeout in portal; clear session memory	Test idle timeout; verify context purge	Low
TH	Access Control	Â§164.312(a)(3)	Encryption & Decryption (A)	Encrypt LLM data at rest (AES-256) bit locker and in use via SGX enclave; manage keys securely	Enable full-disk encryption; leverage Intel SGX	Review encryption configs; inspect key-vault policies	Medium
TH	Audit Controls	Â§164.312(b)	Audit Controls (R)	Log all LLM events (auth, queries, config changes) to append-only store; forward to SIEM; retain 6 yrs	Integrate with SIEM; enable WORM storage	Review log completeness; test tamper detection: teat how long logs are seved	Medium
TH	Integrity	Â§164.312(c)(1)	Mechanism to Authenticate ePHI (A)	Hash or sign LLM inputs/outputs containing PHI; validate on read/write	Apply HMAC to payloads; verify before use	Inspect hash logs; test tamper detection	Medium
TH	Person or Entity Authenticatio n	Â§164.312(d)	Person or Entity Authentication (R)	Enforce MFA for DeepSeek R1 users; require signed OAuth2 JWTs for APIs	Enable push-MFA; issue signed tokens	Attempt login/API call without token	Low

TH	Transmission Security	Â§164.312(e)(1)	Integrity Controls (A)	Use TLS 1.2+ with strong ciphers for all LLM communications; apply message HMAC	Enforce HTTPS; implement HMAC	Capture traffic; test tampered payload	Low
TH	Transmission Security	Â§164.312(e)(2)	Encryption (A)	Require HTTPS/VPN for all remote LLM access; enforce HSTS and certificate pinning	Configure HSTS; disable HTTP	Attempt HTTP connection; review cert settings	Low