Risk Register -Amanda Onumah 12-2025

Risk ID	Risk Description	Control Effectiveness	Impact	Likelihood	Risk Score	Risk Response	Action Items	Risk Owner	Target Date	HIPAA Requirment/Impact
Sequential number (1, 2, 3...)	*Brief explanation in cause-effect format: "If X occurs, then Y happens"*	*How effective are current controls?*	*Potential impact if this risk occurs*	*How likely is this risk to occur?*	*Auto-calculated based on Impact × Likelihood*	*Select response strategy*	*Specific actions to address risk*	*Person responsible for managing this risk*	*Date for completion/review*	*Additional context or updates*
1	**BYOD Remote Access:** If staff access PHI on personal devices without encryption or MDM, then patient data could be exposed if a device is lost, stolen, or compromised	Open	High	Medium	**Red**	Enhance/Mitigate	Implement MDM solution; Require device encryption; Create BYOD security policy	IT Security Manager	[60 days before audit]	Critical for HIPAA compliance. Affects 45 staff members accessing PHI remotely. Controls reduce the chance and blast radius of device loss/theft and man-in-the-middle attacks; big reduction in confidentiality risk.
2	**Training & Awareness:** If staff lack cybersecurity awareness training, then they may fall victim to phishing attacks leading to credential compromise and unauthorized EHR access	Open	High	High	**Red**	Enhance/Mitigate	Deploy mandatory HIPAA security awareness training; Implement phishing simulation program; Create incident reporting procedure	Compliance Officer	https://goproofly.com/templ	HIPAA requires documented security training. High priority given recent healthcare phishing campaigns. Training lowers likelihood of social-engineering success and speeds reporting, reducing overall risk exposure.
3	**Shared EHR credentials** — If nurses share accounts, then untraceable access occurs, resulting in HIPAA violations/audit gaps.	Open	High	High	**Red**	Enhance/Mitigate	MDM, encryption, lock; managed-device only; VPN + posture checks; BYOD policy & attestation.	IT Security Manager & Nursing Lead	[30 days]	HIPAA requires individual user IDs and usable audit trails. Sharing logins makes it impossible to prove who looked at a patient's record and will almost certainly lead to an audit finding.
4	**Third-party (MediCloud) risk** — If vendor is breached, then TechHealth data exposed, resulting in penalties/trust loss.	Open	High	High	**Red**	Enhance/Mitigate	Confirm Business Associate Agreement (BAA); complete vendor risk review (independent audit reports, penetration test, incident Service Level Agreements); require MFA; add 72-hour incident notice	Vendor Risk Lead & Legal Counsel	[60 days before audit]	Per HIPAA, you must have a signed BAA and oversight of the vendor's safeguards. If the vendor leaks PHI, the clinic still has to notify patients and regulators. No BAA = non-compliance.
5	**Incident response gaps** — If no practiced plan, then delayed containment/notice, resulting in higher impact/non-compliance.	Open	High	High	**Red**	Enhance/Mitigate	Create and test an Incident Response Plan; define roles and on-call rotation; joint playbooks with MediCloud; run a tabletop (ransomware + misdirected email).	GRC and Operations	[60 days]	HIPAA requires having and following security-incident procedures and sending timely breach notices (no later than 60 days). Delays can lead to fines.
6	**Data classification / minimum necessary** — If staff unclear on PHI, then oversharing/misdirected emails → disclosure.	Open	Medium	Medium	**Yellow**	Enhance/Mitigate	Publish a clear data-classification policy; label PHI in systems; Data Loss Prevention (DLP) rules for Social Security numbers and clinical terms; require email encryption; block auto-forwarding.	Compliance Officer	[30 days]	HIPAA expects you to share only what is needed. Sending PHI to the wrong person or sharing more than necessary is an unauthorized disclosure and may require patient notification.
7	**Logging & auditability** — If logs incomplete, investigations/audit evidence fail → findings/CAPs	Open	Medium	Medium	**Yellow**	Enhance/Mitigate	Turn on immutable audit logs in the EHR; forward to a Security Information and Event Management (SIEM) tool; keep logs accessible; weekly reviews; alert on unusual access.	IT Security Manager	[30 days]	HIPAA requires monitoring system activity. If you cannot show who accessed what and when, you cannot demonstrate compliance during an audit.
8	**Backups & ransomware resilience** — If backups not isolated/tested, ransomware hits backups → downtime/data loss.	Open	Medium	Medium	**Yellow**	Enhance/Mitigate	"3-2-1" backups with one offline/immutable copy; daily backup checks; monthly restore tests; define recovery time and recovery point targets	IT Operations Manager	[30 days]	HIPAA expects working backups and disaster-recovery plans. If ransomware hits and you cannot recover, patient care suffers and the event will likely be treated as a breach unless you can show low ris
9	**Payment card handling (PCI DSS)** — If clinic systems store card data, scope/risk increase → fines.	Open	Low	Low	**Green**	Accept	Outsource payments to a validated processor; use tokenization; network-segment payment devices; complete the right Self-Assessment Questionnaire; quarterly scans if needed	Revenue Cycle Lead & IT Network Lead	[30 days]	Not a direct HIPAA requirement, but separating card data from health data reduces the chance that PHI is swept up in a payment-system incident and makes HIPAA compliance easier to prove.
10	**Patient trust & communications** — If concerns go unanswered, complaints/churn rise → reputational damage.	Open	Low	Low	**Green**	Accept	Publish a plain-English privacy and security FAQ or SBAR; add a portal banner about new protections (MFA, device checks); train front desk on approved talking points etc.	Communications Manager & Compliance Officer	[30 days]	Clear communication supports the required Notice of Privacy Practices and prepares the team to deliver accurate breach notices if ever needed.

NIST Requirement
Additional context or updates per NIST 800-53 Rev. 5 framework
Remote Access (AC-17); Mobile Device Access (AC-19); Identification and Authentication (IA-2); Cryptographic Protection (SC-12/SC-13); Boundary Protection (SC-7).
Security Awareness and Training (AT-2); Role-Based Training (AT-3); Incident Reporting (IR-6).
Access Control, Account Management (AC-2); Identification and Authentication, Multifactor (IA-2, IA-2(1)); Audit Logging (AU-2); Audit Review (AU-6); Least Privilege (AC-6
External System Services (SA-9); Supply Chain Risk Management (SR-3, SR-5); System Interconnections (CA-3); Planning, Rules for External Parties (PL-8).
Incident Response Policy and Procedures (IR-1); Incident Handling (IR-4); Incident Reporting (IR-6); Contingency Planning (CP-2).
Security Categorization (RA-2); System and Communications Protection, Information Flow Enforcement (AC-4 / SC-7); Least Privilege (AC-6); Planning, Security and Privacy Plans (PL-2).
Event Logging (AU-2, AU-12); Audit Review, Analysis, and Reporting (AU-6); Time Stamps (AU-8); Security Monitoring (SI-4).
Information System Backup (CP-9); System Recovery (CP-10); Contingency Plan (CP-2); Configuration Management, Least Functionality (CM-7).
Boundary Protection and Segmentation (SC-7); Information Flow Enforcement (AC-4); External System Services (SA-9); System Interconnections (CA-3).
Transparency (TR-1, privacy control family); Security and Privacy Training (AT-2); Planning, Rules of Behavior (PL-4).