Security Risk Assessment

Assessment Date: [ASSESSMENT DATE] (HIPAA Security Rule risk analysis · 45 C.F.R. § 164.308(a)(1)(ii)(A))

This Security Risk Assessment ("SRA") documents the risk analysis performed by **SecureLynx, LLC** for [CLIENT LEGAL NAME] ("Client"), identifying threats and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI), assessing current safeguards, and prioritizing remediation. The methodology is consistent with NIST SP 800-30 and guidance from the HHS Office for Civil Rights. This SRA is performed at onboarding and kept current as the environment changes.

SAMPLE · NOT FOR EXECUTION

1. Assessment Overview

Field	Detail
Client	[CLIENT LEGAL NAME]
Locations in Scope	[ADDRESSES / SITES]
Assessor	SecureLynx, LLC
Assessment Type	[Initial (onboarding) / Annual review / Triggered by change]
Prior SRA Date	[DATE or N/A]
Next Scheduled Review	[DATE]

2. Scope and Methodology

This assessment covers all systems, applications, devices, media, and facilities where the Client creates, receives, maintains, or transmits ePHI. The methodology consists of:

- Inventory of ePHI systems and data flows, including third-party and cloud services.
- Identification of reasonably anticipated threats and vulnerabilities.
- Review of existing administrative, physical, and technical safeguards.
- Risk determination based on likelihood and impact, using the matrix in Section 6.
- Documented findings, a prioritized risk register, and a remediation roadmap.

3. ePHI System Inventory

System / Service	ePHI Function	Location / Vendor
EHR / Practice Management	[Create / Receive / Maintain / Transmit]	[SYSTEM, VENDOR, HOSTING]
Imaging / PACS	[C / R / M / T or N/A]	[SYSTEM, VENDOR]
Email and messaging	[C / R / M / T]	[PLATFORM]
File storage / servers	[C / R / M / T]	[ON-PREM / CLOUD]
Backups	[Maintain]	[SOLUTION, OFFSITE LOCATION]

System / Service	ePHI Function	Location / Vendor
Workstations and mobile devices	[C / R / M / T]	[COUNT, MANAGEMENT STATUS]
Third-party billing / clearinghouse	[Transmit or N/A]	[VENDOR, BAA STATUS]

Every system listed above that is operated by a vendor should have a signed Business Associate Agreement in place; note any gaps in the risk register.

4. Current Safeguards Review

Status key: **In place · Partial · Not in place · N/A**

- **Administrative:** risk management process, workforce security training, sanction policy, access authorization procedures, incident response plan, contingency/disaster-recovery plan, periodic review. [STATUS PER ITEM]
- **Physical:** facility access controls, workstation placement and security, device and media controls, disposal and re-use procedures. [STATUS PER ITEM]
- **Technical:** unique user IDs, multi-factor authentication, automatic logoff, encryption at rest and in transit, audit logging, integrity controls, endpoint detection and response, patch and vulnerability management. [STATUS PER ITEM]

5. Threats and Vulnerabilities Considered

- **External:** ransomware and malware, phishing and credential theft, business email compromise, exploitation of unpatched systems, vendor or supply-chain compromise.
- **Internal:** inadvertent disclosure, misdirected communications, excessive access rights, departed-user accounts left active, unauthorized software or devices.
- **Environmental:** hardware failure, power loss, fire or water damage, loss or theft of devices and media, natural disaster affecting the facility.

6. Risk Determination Methodology

Each finding is rated for likelihood and impact, and the combination determines the risk level and remediation priority:

	Low Impact	Medium Impact	High Impact
High Likelihood	Medium	High	Critical
Medium Likelihood	Low	Medium	High
Low Likelihood	Low	Low	Medium

Critical and High findings are addressed during onboarding remediation; Medium findings are scheduled on the roadmap; Low findings are documented and monitored.

SAMPLE · NOT FOR EXECUTION

7. Risk Register

ID	Finding (threat / vulnerability)	Likelihood	Impact	Risk Level
R-01	[FINDING]	[H/M/L]	[H/M/L]	[Critical/High/Medium/Low]
R-02	[FINDING]	[H/M/L]	[H/M/L]	[LEVEL]
R-03	[FINDING]	[H/M/L]	[H/M/L]	[LEVEL]

8. Remediation Roadmap

ID	Remediation Action	Priority	Owner	Target Date
R-01	[ACTION]	[P1/P2/P3]	[SecureLynx / Client]	[DATE]
R-02	[ACTION]	[P1/P2/P3]	[OWNER]	[DATE]
R-03	[ACTION]	[P1/P2/P3]	[OWNER]	[DATE]

Remediation to the SecureLynx security baseline is included in onboarding per the SLA; items outside that baseline or requiring Client purchases are noted with the Client as owner.

9. Review and Maintenance

- This SRA is reviewed and updated at least annually, and upon any material change to the environment (new systems, locations, vendors, or a security incident).
- Completed remediation items are recorded with the completion date, keeping the register current as evidence of an ongoing risk management process.
- The Client retains this document and its updates as part of its HIPAA compliance records.

10. Limitations

This assessment supports the Client's compliance obligations under the HIPAA Security Rule. SecureLynx is not an auditor or certifying body, and this document is not a certification of HIPAA compliance, a legal opinion, or a guarantee that a security incident will not occur. The Client, as the Covered Entity, remains responsible for its own regulatory obligations.

11. Acknowledgment and Signatures

By signing below, the parties acknowledge the findings and the remediation roadmap in this assessment.

SecureLynx, LLC	Client
Authorized Signature	Authorized Signature
Printed Name	Printed Name
Date	Date

SAMPLE - NOT FOR EXECUTION