

- Fictional — for illustration. Every name, system and finding in this report is invented.

See the deliverable *before you hire us.*

A complete synthetic security assessment report for a fictional company, "Example Health Labs". It shows the structure, scoring, risk register and remediation plan a client receives. No client data was used.

SECURITY ASSESSMENT · V1.0

Fictional — for illustration

Example Health Labs

Fictional digital-health company · 12 staff · patient app, clinician portal, cloud-hosted ePHI

Assessment period

6–31 January 2026

Interviews

3 stakeholders

Method

NIST SP 800-30r1, SP 800-66r2

Scale

Five-level qualitative
(Table I-2)

Executive summary

Two High risks need action first: ePHI exported to unencrypted laptops, and cloud administrator accounts without MFA. Three Moderate risks follow, centred on backups, vendor agreements and audit-log review. The remediation plan sequences all six within 10 weeks.

2

3

1

High

Moderate

Very low

Section 1

Scope

All systems that create, receive, maintain or transmit ePHI: the app backend, clinician portal, cloud accounts, staff laptops, email, backups, and four vendors with ePHI access. Out of scope: penetration testing; physical office beyond the visitor log.

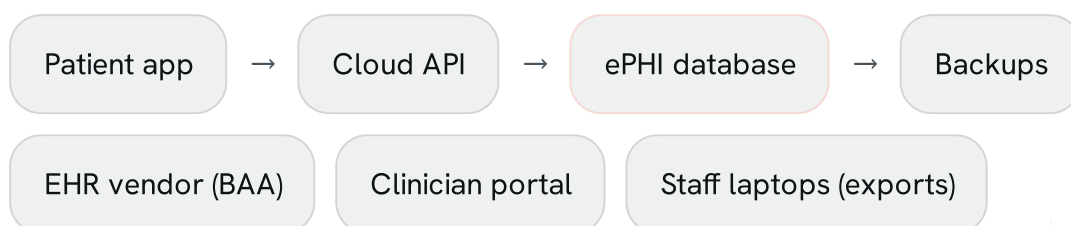
Section 2

Methodology

Prepare, conduct, communicate and maintain, per NIST SP 800-30r1, applied with SP 800-66r2. Likelihood and impact rated Very Low to Very High; level of risk taken from Table I-2. Every rating carries a rationale and evidence reference. [How NIST SP 800-30 works](#).

Section 3

Inventory and data flow



Full report: 38 assets inventoried with owners, locations and data classifications.

Section 4

Risk register (excerpt)

ID	ASSET	THREAT / VULNERABILITY	EXISTING CONTROL	LIKELIHOOD
R-01	Staff laptops	Theft or loss / ePHI exports stored locally	No full-disk encryption	High
R-02	Cloud admin accounts	Credential phishing / password only	No MFA	Moderate
R-03	Database backups	Ransomware / restore never tested	Daily backups	Moderate
R-04	Vendors with ePHI	Disclosure by vendor / BAA inventory incomplete	Two of four BAAs on file	Low
R-05	Portal audit logs	Undetected misuse / logs not reviewed	Logging enabled	Moderate
R-06	Office visitor log	Over-retention / no disposal date	Paper log	Low

Full register: 18 risks, each with rationale, owner and target date.

Section 5

Remediation plan (extract)

- 1 Enforce MFA on all cloud administrator accounts**
Addresses R-02 · Owner: CTO · Effort: low · Quick win
- 2 Enable full-disk encryption; stop local ePHI exports**
Addresses R-01 · Owner: Operations lead · Effort: low-medium
- 3 Run and document a full restore test**
Addresses R-03 · Owner: Engineering lead · Effort: medium

Section 6

Framework mapping

Each finding is mapped to HIPAA Security Rule standards and, where in scope, ISO/IEC 27001:2022 Annex A, NIST CSF 2.0 and DPDP Rule 6.
Example: R-02 → 164.312(d) · A.8.5 · PR.AA.

Section 7

Limitations

Findings reflect the systems in scope and the information disclosed during the assessment period. This report is a point-in-time assessment. It is not a certification, a penetration test or legal advice.