PERSONAL GUIDANCE. PRACTICAL DOCUMENTATION.

Security Risk Assessment



Illustrative practice: Harborview Family Practice

Entirely fictional organization. Assessment date: October 20, 2026. Example scope: one office, a hosted EHR, staff workstations, business email, a network device and an encrypted backup service.

Executive summary

This demonstration shows how an assessment can connect the electronic protected health information environment to potential threats, vulnerabilities, existing controls and recommended actions. It illustrates documentation structure, not an actual review of any organization.

Three representative findings are shown: incomplete access-removal evidence, untested recovery procedures and an unattended workstation scenario. The example prioritizes access management and recovery verification for early action. These findings and scores are invented for demonstration.

No actual inspection, interview, technical test or independent verification occurred. This is not a comprehensive assessment, legal advice, certification or guarantee of HIPAA compliance. A customer report must reflect its agreed scope and actual evidence.

Scope, evidence & limitations

Illustrative systems and information flows

Staff access a hosted EHR through office workstations. Business email may contain ePHI. An office network supports connectivity. An external IT provider assists with account administration and backup management. A real review must inventory all relevant ePHI, including systems and locations beyond these examples.

Assessment approach

1. Define scope and identify ePHI locations and flows.
2. Gather relevant information and identify existing safeguards.
3. Connect threats and vulnerabilities to affected assets.
4. Estimate likelihood and impact with documented reasoning.
5. Record priorities, corrective actions, assumptions and next steps.

Evidence labels for a real engagement

Observed: directly inspected material or behavior, with date and reviewer.
Reported: information supplied by practice representatives.
Verified: a specific control tested or corroborated, with method and result.
Not available: an evidence gap that needs follow-up.
All evidence in this document is **fictional and unverified**.

Demonstration scoring method

Likelihood: 1 = unlikely, 2 = plausible, 3 = likely. Impact: 1 = limited, 2 = moderate, 3 = significant harm to confidentiality, integrity or availability. Illustrative score = likelihood x impact: 1-2 low, 3-4 moderate, 6-9 high. These thresholds are examples, not a government-mandated method.

Limitations

This short sample omits many potential systems, threats and safeguards. A real analysis must be accurate and thorough for its scope and should not rely solely on a questionnaire. Missing evidence may require further investigation and may affect delivery timing.

Risk register

R-01 | Administrative + technical | HIGH (6)

Access removal is not consistently documented.
Threat: access by a former worker. Vulnerability: no completed offboarding record for the fictional example. Assets: hosted EHR and email. Existing control: individual accounts and an informal manager-to-IT notification process.
Basis: Likelihood 2: the process relies on informal notification. Impact 3: unauthorized access could expose or alter ePHI. Evidence: invented scenario; no accounts were inspected.
Recommendation: Assign an owner; reconcile current accounts to authorized staff; document access removal and review its completion.

R-02 | Administrative + technical | HIGH (6)

Backup recovery has no documented restore exercise.
Threat: operational disruption after data loss or ransomware. Vulnerability: recovery capability has not been demonstrated. Existing control: a fictional encrypted backup service is reported.
Basis: Likelihood 2: recovery failure is plausible without a test. Impact 3: prolonged unavailability could disrupt access to information. Evidence: fictional report only; backups were not tested.
Recommendation: Review backup scope and recovery objectives with IT; perform a controlled restore test; retain results and resolve any gaps.

R-03 | Physical + technical | MODERATE (4)

An unattended workstation could expose information.
Threat: viewing by an unauthorized person. Vulnerability: screen visibility and an unconfirmed auto-lock setting in a shared area. Existing control: staff are instructed to lock screens.
Basis: Likelihood 2 and impact 2: exposure is plausible, with scope depending on displayed information. Evidence: fictional scenario; no workspace was inspected.
Recommendation: Evaluate positioning and access; configure appropriate automatic locking; reinforce and verify staff practices.

Corrective action roadmap

Suggested priorities for this fictional example

First: confirm facts and agree ownership. Validate the evidence behind each finding. The practice administrator and IT contact should agree on affected systems, appropriate actions and realistic target dates.

R-01 / Practice administrator + IT: reconcile accounts and document offboarding. Completion evidence: approved access list and a retained removal record. Suggested planning window: within 30 days, subject to the practice's risk decisions.

R-02 / IT contact: carry out a controlled recovery exercise. Completion evidence: restore-test record, outcome, gaps and follow-up. Suggested planning window: within 30 days, coordinated to avoid disruption.

R-03 / Office manager + IT: review screen placement and locking behavior. Completion evidence: documented configuration review and staff communication. Suggested planning window: within 60 days.

Track the work and revisit the analysis

Record an owner, target date, current status, completion evidence and residual risk for each action. Validate that changes address the concern. Update the analysis as systems, operations or threats change. The suggested windows above are illustrative planning aids, not legal deadlines.

Official reference framework

HHS, Guidance on Risk Analysis Requirements under the HIPAA Security Rule:
hhs.gov - Guidance on Risk Analysis
HHS, Summary of the HIPAA Security Rule:
hhs.gov - Summary of the HIPAA Security Rule

Prepared as a fictional marketing sample. No real practice data, customer outcomes or testimonials are included. Risk analysis is one component of a broader compliance program.