EMRY NETWORKS
IT Solutions That Click

FREE WORKSHEET · HIPAA SECURITY RULE · EMRY NETWORKS | DEFENSIBLE IT

# HIPAA Security Risk Analysis Worksheet

A fillable, printable worksheet for medical groups, dental practices, pharmacies and therapy practices. It walks you through the risk analysis and risk management the HIPAA Security Rule requires at 45 CFR 164.308(a)(1)(ii)(A) and (B), plus the information system activity review at 164.308(a)(1)(ii)(D) and the audit controls standard at 164.312(b). Prepared by **Emry Networks** (founder Joe Tucker, CISSP) | (603) 202-3200 | Book a 30-Minute Risk Assessment

## WHAT'S INSIDE


| | | |
|---|---|---|
| ● | How to use this worksheet and assessment details | p. 2 |
| 1 | Scope and ePHI inventory | p. 3 |
| 2 | Threats, vulnerabilities, current controls and risk level | p. 4 |
| 3 | Risk management plan | p. 5 |
| 4 | Information system activity review and audit logs | p. 6 |
| 5 | Security Rule quick reference: Required vs. Addressable | p. 7 |
| 6 | What OCR keeps citing, and when to redo the analysis | p. 8 |
| 7 | Your results, summary and sign-off | p. 9 |
| ● | Sources | p. 10 |


Book a 30-Minute Risk Assessment →

## USING THE INTERACTIVE VERSION

- **Type in any shaded box.** Press Tab to move to the next one.
- **Blue-outlined boxes are drop-downs** for likelihood, impact, decisions and status.
- **Grey boxes calculate themselves:** each risk score and level, and the totals on your Results page.
- **Best in Adobe Acrobat Reader (free)** or another desktop PDF app. Browser viewers and Apple Preview let you type, but may not run the calculations; you can type those values in yourself.
- **Use the links** in the contents list, the header (Contents, Results) and the bookmarks panel to jump around.
- **Save often.** Prints on US Letter, landscape; the on-screen buttons do not print.

Print worksheet | Clear all entries

## COLOUR KEY

Scope · Assess · Plan · Monitor · Reference · Context · Results

# How to use this worksheet

45 CFR Part 164, Subpart C

**1. Set the scope.** Include every location and system that creates, receives, maintains or transmits ePHI, including acquired practices and new sites (Part 1). OCR's guidance says the scope covers all ePHI, "regardless of the particular electronic medium" or its location.

**2. Inventory the ePHI.** List each system, where it lives, who owns it and which vendor touches it (Part 1).

**3. Pair threats with vulnerabilities.** Use the starter rows in Part 2, then add your own.

**4. Record current controls.** Write down what is actually in place and working today, not what the policy says.

**5. Rate likelihood and impact.** Use the 1-3 scales in Part 2 and multiply for a risk score. HIPAA does not prescribe a scoring method; this is one simple option. In the fillable PDF, pick L and I from the drop-downs and the score and level fill in for you.

**6. Plan the fixes.** Turn every Medium and High risk into a dated, owned action in Part 3 (risk management, 164.308(a)(1)(ii)(B)).

**7. Prove you review activity.** Fill in the log-review register in Part 4 and keep the evidence.

**8. Sign, date and keep it.** Security Rule documentation must be retained for 6 years (164.316(b)(2)(i)). Update it after incidents, ownership changes, staff turnover or new technology (Part 6).

## Assessment details

| | | | |
|---|---|---|---|
| **Practice / legal entity** | | **Assessment date** | |
| **Locations in scope (all sites)** | | **Security official (164.308(a)(2))** | |
| **Prepared by** | | **Date of last risk analysis** | |
| **Method / tools used (e.g., this worksheet, HHS SRA Tool v3.7)** | | **Next scheduled review** | |

## Disclaimer

This worksheet is an educational self-assessment aid. It is not legal advice, not a certification, and not a substitute for the regulation, OCR guidance, or advice from qualified counsel. Completing it does not by itself establish HIPAA compliance. Citations reflect 45 CFR Part 164, Subpart C as published on eCFR (current as of October 29, 2026). © 2026 Emry Networks.

# 1 Scope and ePHI inventory

164.308(a)(1)(ii)(A) · 164.306(a)(1)

Rule: 164.308(a)(1)(ii)(A) requires "an accurate and thorough assessment" of risks to ePHI, and 164.306(a)(1) covers "all electronic protected health information" you create, receive, maintain or transmit. Start with locations, then systems.

## 1A. Locations and acquired practices

| Location / practice name | Date opened or acquired | Systems still separate from yours? (EHR, email, network) | Included in this analysis? | Notes / owner |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 1B. Systems and devices that hold or move ePHI

Prompts: EHR/practice management, imaging and PACS, e-prescribing, patient portal and messaging, email, fax-to-email, phone system recordings, billing/clearinghouse, cloud file storage, backups (on-site and off-site), servers, workstations, laptops, phones and tablets, networked medical devices, copiers/scanners with drives, and anything inherited from an acquired practice.

| System / device | Location | ePHI: create / receive / maintain / transmit | Vendor (if any) | BAA on file? (Y/N/NA) | System owner | Notes (where data flows in/out) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# 2 Threats, vulnerabilities, current controls and risk level

OCR Guidance on Risk Analysis

OCR's Guidance on Risk Analysis asks you to document reasonably anticipated threats, the vulnerabilities they could exploit, current security measures, likelihood, impact and a risk level for each threat and vulnerability pair. Rating scale used here: **Likelihood** 1 = Low, 2 = Medium, 3 = High. **Impact** 1 = Low, 2 = Medium, 3 = High. **Risk score** = Likelihood × Impact: 1-2 Low, 3-4 Medium, 6-9 High. This is an Emry example scale. The Security Rule does not prescribe one; NIST SP 800-30 Rev. 1 describes qualitative and quantitative approaches.

| # | Asset / system | Threat | Vulnerability | Current controls (what is in place today) | L (1-3) | I (1-3) | Score | Level | Security Rule citation |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Email / Microsoft 365 or Google Workspace | Phishing leads to account takeover | No multi-factor authentication on email or remote access | | | | | | 164.312(d)<br>164.308(a)(5)(ii)(D) |
| 2 | Workstations and servers | Ransomware encrypts EHR, imaging or file shares | Malware protection not current on every device | | | | | | 164.308(a)(5)(ii)(B)<br>164.308(a)(6)(ii) |
| 3 | Backups | Backups encrypted or deleted along with production data | Restores never tested; backups reachable with the same admin login | | | | | | 164.308(a)(7)(ii)(A), (B), (D) |
| 4 | EHR / practice management system | Misuse of access goes unnoticed | Audit logs exist but nobody reviews them on a schedule | | | | | | 164.308(a)(1)(ii)(D)<br>164.312(b) |
| 5 | Acquired practice or new location | Unknown systems hold ePHI outside your controls | Systems never inventoried or added to the risk analysis | | | | | | 164.308(a)(1)(ii)(A)<br>164.306(a)(1) |
| 6 | User accounts | Former staff or vendors still have access | No same-day account removal at termination | | | | | | 164.308(a)(3)(ii)(C)<br>164.308(a)(4)(ii)(C) |
| 7 | Front desk and shared PCs | Actions cannot be traced to a person | Shared logins; sessions left open | | | | | | 164.312(a)(2)(i)<br>164.312(a)(2)(iii) |
| 8 | Laptops, phones and tablets | Lost or stolen device exposes ePHI | Device not encrypted | | | | | | 164.312(a)(2)(iv)<br>164.310(d)(1) |
| 9 | Vendors (cloud EHR, billing, IT, imaging) | Vendor breach exposes your patients' ePHI | No signed business associate agreement on file | | | | | | 164.308(b)(1), (b)(3)<br>164.314(a) |
| 10 | Email, fax-to-email, patient messaging | ePHI intercepted in transit | No encryption for messages that contain ePHI | | | | | | 164.312(e)(1)<br>164.312(e)(2)(ii) |
| 11 | Old drives, copiers, retired PCs | ePHI recovered from discarded media | No wipe or destruction record | | | | | | 164.310(d)(2)(i), (ii) |
| 12 | Server closet / network equipment | Power loss, water or fire takes systems down | No emergency mode plan; no off-site copy | | | | | | 164.308(a)(7)(ii)(C)<br>164.310(a)(2)(i) |
| 13 | | | | | | | | | |
| 14 | | | | | | | | | |
| 15 | | | | | | | | | |

Starter rows are common examples, not a complete list. Add threats specific to your practice (for example, a vendor outage, a lost USB drive, or an employee viewing records they do not need).

# 3 Risk management plan

164.308(a)(1)(ii)(B) · 164.306(d)(3)

Rule: 164.308(a)(1)(ii)(B) (Required) says to "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." For an **Addressable** specification, 164.306(d)(3) says you must assess whether it is reasonable and appropriate, implement it if so, and if not, document why and implement an equivalent alternative measure if reasonable and appropriate. Addressable does not mean optional.

| Risk # | Planned safeguard / action | Addressable decision (Implement / Alternative / Not reasonable, documented) | Owner | Target date | Status | Date done | Evidence (ticket, screenshot, report) |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# 4 Information system activity review and audit logs

164.308(a)(1)(ii)(D) · 164.312(b)

Rules: 164.308(a)(1)(ii)(D) (Required) says to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 164.312(b) (audit controls) requires mechanisms that "record and examine activity" in systems that contain or use ePHI. 164.308(a)(5)(ii)(C) (Addressable) covers monitoring log-in attempts. The rule does not set a review frequency, so pick one, write it down, and keep proof that each review happened.

## 4A. Log source register

| System | What is logged (logins, record access, admin changes, exports) | Where logs are kept | Retention | Reviewer | Frequency | Last review | Findings / ticket # |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## 4B. Review prompts (check what you looked at; these are Emry suggestions, not rule text)

- Failed or unusual log-ins (after hours, new countries, impossible travel)
- Accounts of departed staff or vendors that are still active
- Access to records of staff, VIPs or family members
- Backup job failures and restore test results
- New or changed admin and privileged accounts
- Large exports, prints or downloads of patient records
- New mailbox forwarding rules or connected apps
- Malware / endpoint protection alerts and how each was closed

**Reviewed by:** **Date:** **Period covered:** **Issues opened:**

# 5 Security Rule quick reference: Required vs. Addressable

45 CFR 164.308-164.316

From the current text of 45 CFR Part 164, Subpart C (eCFR, current as of October 29, 2026). R = Required, A = Addressable, S = standard with no separate implementation specification (you must still meet it). Use the last column to mark your status.

| Citation | Specification / standard | | Status | Citation | Specification / standard | | Status |
|---|---|---|---|---|---|---|---|
| 164.308(a)(1)(ii)(A) | Risk analysis | R | | 164.310(a)(2)(i) | Contingency operations | A | |
| 164.308(a)(1)(ii)(B) | Risk management | R | | 164.310(a)(2)(ii) | Facility security plan | A | |
| 164.308(a)(1)(ii)(C) | Sanction policy | R | | 164.310(a)(2)(iii) | Access control and validation procedures | A | |
| 164.308(a)(1)(ii)(D) | Information system activity review | R | | 164.310(a)(2)(iv) | Maintenance records | A | |
| 164.308(a)(2) | Assigned security responsibility | S | | 164.310(b) | Workstation use | S | |
| 164.308(a)(3)(ii)(A) | Authorization and/or supervision | A | | 164.310(c) | Workstation security | S | |
| 164.308(a)(3)(ii)(B) | Workforce clearance procedure | A | | 164.310(d)(2)(i) | Disposal | R | |
| 164.308(a)(3)(ii)(C) | Termination procedures | A | | 164.310(d)(2)(ii) | Media re-use | R | |
| 164.308(a)(4)(ii)(B) | Access authorization | A | | 164.310(d)(2)(iii) | Accountability | A | |
| 164.308(a)(4)(ii)(C) | Access establishment and modification | A | | 164.310(d)(2)(iv) | Data backup and storage | A | |
| 164.308(a)(5)(ii)(A) | Security reminders | A | | 164.312(a)(2)(i) | Unique user identification | R | |
| 164.308(a)(5)(ii)(B) | Protection from malicious software | A | | 164.312(a)(2)(ii) | Emergency access procedure | R | |
| 164.308(a)(5)(ii)(C) | Log-in monitoring | A | | 164.312(a)(2)(iii) | Automatic logoff | A | |
| 164.308(a)(5)(ii)(D) | Password management | A | | 164.312(a)(2)(iv) | Encryption and decryption | A | |
| 164.308(a)(6)(ii) | Response and reporting | R | | 164.312(b) | Audit controls | S | |
| 164.308(a)(7)(ii)(A) | Data backup plan | R | | 164.312(c)(2) | Mechanism to authenticate electronic protected health information | A | |
| 164.308(a)(7)(ii)(B) | Disaster recovery plan | R | | 164.312(d) | Person or entity authentication | S | |
| 164.308(a)(7)(ii)(C) | Emergency mode operation plan | R | | 164.312(e)(2)(i) | Integrity controls | A | |
| 164.308(a)(7)(ii)(D) | Testing and revision procedures | A | | 164.312(e)(2)(ii) | Encryption | A | |
| 164.308(a)(7)(ii)(E) | Applications and data criticality analysis | A | | 164.316(b)(2)(i) | Time limit (retain documentation 6 years) | R | |
| 164.308(a)(8) | Evaluation | S | | 164.316(b)(2)(ii) | Availability | R | |
| 164.308(b)(3) | Written contract or other arrangement (business associates) | R | | 164.316(b)(2)(iii) | Updates | R | |

# 6 What OCR keeps citing, and when to redo the analysis

HHS OCR enforcement

- **Lehigh Valley Health Network (announced October 29, 2026).** $800,000 and a three-year corrective action plan after a ransomware attack that affected the PHI of 248,359 individuals. OCR found potential violations including failing to conduct an accurate and thorough risk analysis and failing to implement procedures to regularly review information system activity, such as audit logs. HHS press release
- **Regional Women's Health Group, d/b/a Axia Women's Health (announced April 23, 2026).** A network of women's health providers in five states paid $320,000 after a ransomware breach affecting 37,989 individuals; OCR found it failed to conduct an accurate and thorough risk analysis. The same release counted 13 completed investigations in OCR's Risk Analysis Initiative. HHS press release
- **Top of the World Ranch Treatment Center (announced February 19, 2026).** $103,000 and a two-year corrective action plan after a phishing attack compromised the ePHI of 1,980 patients; OCR's investigation found evidence that it failed to conduct an accurate and thorough risk analysis. HHS called it the 11th enforcement action in its Risk Analysis Initiative. HHS press release
- **MMG Fusion, LLC (announced March 5, 2026).** A business associate whose software is used to communicate with patients paid $10,000 (OCR considered its financial condition). OCR found potential violations including failing to conduct an accurate and thorough risk analysis. HHS called it the 12th Risk Analysis Initiative action. HHS press release
- **What a corrective action plan looks like.** In the Bryan County Ambulance Authority resolution agreement ($90,000), OCR required a risk analysis covering a complete inventory of electronic equipment, data systems, off-site data storage facilities and applications that contain or store ePHI, with the scope and methodology submitted to HHS within 30 calendar days. HHS resolution agreement

## When to update your risk analysis

OCR's risk analysis guidance says the process should be ongoing and that the Security Rule does not specify how often to perform it. It gives examples of when to analyze risk again: a security incident, a change in ownership, turnover in key staff or management, or plans to adopt new technology. Our recommendation: treat a newly acquired practice or a new location as one of those triggers and add it to the analysis before connecting it to your network.

## Proposed HIPAA Security Rule changes

**PROPOSED, NOT FINAL.** On January 6, 2025, HHS published a notice of proposed rulemaking (90 FR 898) to modify the Security Rule; comments closed March 7, 2025. Among other changes, it proposes removing the distinction between required and addressable specifications, requiring a written technology asset inventory and network map reviewed at least once every 12 months, encryption of ePHI at rest and in transit with limited exceptions, and multi-factor authentication. As of November 1, 2026, no final rule has been issued. The current Unified Agenda entry (RIN 0945-AA22) lists it under Long-Term Actions with final action projected for July 2027, an estimate rather than a deadline. Until a final rule takes effect, the current Security Rule text is what applies.

## Free government resources

- **Security Risk Assessment (SRA) Tool v3.7**, developed by ONC with HHS OCR: available at no cost as a Windows application or an Excel workbook, aimed at small and medium-sized providers. Information you enter is stored locally; HHS says it does not collect it. Version 3.7 added an assessment-scope question so the analysis accounts for every location that handles ePHI. https://healthit.gov/privacy-security/security-risk-assessment-tool/
- **OCR Guidance on Risk Analysis:** the elements a risk analysis must include. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
- **NIST SP 800-66 Rev. 2** (February 2024), Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide. https://csrc.nist.gov/pubs/sp/800/66/r2/final
- **NIST SP 800-30 Rev. 1** (September 2012), Guide for Conducting Risk Assessments. https://csrc.nist.gov/pubs/sp/800/30/r1/final

# 7 Your results, summary and sign-off

Calculated from Parts 2-5

These totals fill in automatically from your answers in Adobe Acrobat Reader and most desktop PDF apps. If a box stays blank in your viewer, count from Parts 2-5 and type or write the number in. Coverage figures are your own self-assessment, not a compliance determination.

## Risk register (Part 2)

| Risks rated High | Risks rated Medium | Risks rated Low | Rows not yet rated | Highest risk score |
|---|---|---|---|---|
| | | | | |

**High risks to fix first (calculated, highest score first)**

## Risk management plan and log review (Parts 3-4)

| Actions planned | Actions done | Plan complete | Review prompts |
|---|---|---|---|
| | | | |

## Security Rule quick reference (Part 5)

| In place | Partial | Gap | Required specs Partial/Gap | Coverage (self-rated) | Not yet marked |
|---|---|---|---|---|---|
| | | | | | |

Coverage = specifications marked In place ÷ specifications you have marked, excluding N/A. Specifications marked N/A:

## Sign-off

| | |
|---|---|
| **Risk management plan approved by (name, title)** | |
| **Security official signature / date** | |
| **Date of next review (and trigger events to watch)** | |

Keep this worksheet, the risk management plan and your log-review evidence for at least 6 years from creation or the date last in effect, whichever is later (164.316(b)(2)(i)).

## Sources

45 CFR 164.308 Administrative safeguards (eCFR): https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.306 General rules, incl. addressable (eCFR): https://www.ecfr.gov/current/title-45/section-164.306
45 CFR 164.310 Physical safeguards (eCFR): https://www.ecfr.gov/current/title-45/section-164.310
45 CFR 164.312 Technical safeguards (eCFR): https://www.ecfr.gov/current/title-45/section-164.312
45 CFR 164.316 Documentation (eCFR): https://www.ecfr.gov/current/title-45/section-164.316
HHS OCR Guidance on Risk Analysis: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
HHS/ONC Security Risk Assessment Tool: https://healthit.gov/privacy-security/security-risk-assessment-tool/
SRA Tool v3.7 User Guide: https://healthit.gov/wp-content/uploads/2026/09/SRA_Tool_User_Guide_Version_3.7.pdf
NIST SP 800-66 Rev. 2: https://csrc.nist.gov/pubs/sp/800/66/r2/final
NIST SP 800-30 Rev. 1: https://csrc.nist.gov/pubs/sp/800/30/r1/final
HHS: Lehigh Valley Health Network settlement (Oct 29, 2026): https://www.hhs.gov/press-room/hhs-ocr-settles-ransomware-investigation-lehigh-valley-health-network.html
HHS: Four ransomware settlements (Apr 23, 2026): https://www.hhs.gov/press-room/ocr-settles-four-ransomware-investigations.html
HHS: Top of the World Ranch Treatment Center (Feb 19, 2026): https://www.hhs.gov/press-room/ocr-settles-hipaa-security-rule-investigation-twrtc.html
HHS: MMG Fusion (Mar 5, 2026): https://www.hhs.gov/press-room/ocr-mmg-fusion-hipaa-agreement.html
HHS: Bryan County Ambulance Authority resolution agreement: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bcaa-ra-cap/index.html
Federal Register: Proposed Security Rule (Jan 6, 2025):
https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
Unified Agenda: RIN 0945-AA22: https://www.reginfo.gov/public/do/eAgendaViewRule?RIN=0945-AA22&pubId=202510

## Want a second set of eyes on your risk analysis?

Emry Networks helps medical groups, dental practices, pharmacies and therapy practices build risk analyses that hold up, with evidence for every control. Call (603) 202-3200 or Book a 30-Minute Risk Assessment.

Book a 30-Minute Risk Assessment →

Print worksheet Clear all entries