# HIPAA security risk assessment worksheet

complyday.com

Risk analysis required by 45 CFR 164.308(a)(1)(ii)(A): "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." Record systems and safeguards only. Never write patient names or other patient information on this worksheet.

Office: _____ Security official: _____ Assessment done by: _____

Date: _____ Previous assessment date: _____

### Why this assessment is being done

- ☐ Scheduled review
- ☐ New system or software (name):
- ☐ Security incident or breach
- ☐ Move, new location, change in ownership or key staff

### Locations in scope

Every place that creates, receives, maintains or transmits electronic patient information: each office, any home office or remote access, and each cloud service.

| Location | Address or description | Who works there |
|---|---|---|
| | | |
| | | |
| | | |

### Step 1. Where electronic patient information lives (asset inventory)

List each system, device and service. Include practice management and charting software, imaging and X-ray sensors, intraoral scanners, workstations, laptops, phones and tablets, email, fax, backups, the network and Wi-Fi, and vendors that store or send data for you.

| System, device or service | Patient information it holds or sends | Where it is (room, cloud) | Who can access | Vendor; agreement signed? |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Step 2. Threats, vulnerabilities and risk level



For each system, write the reasonably anticipated threats and the weaknesses that would let them cause harm. Rate how likely each is and how bad the impact would be, then combine them into a risk level. HHS says the rule does not prescribe a method; this scale is one way to do it.

| Rating | Likelihood | Impact | Risk level (likelihood with impact) |
|---|---|---|---|
| Low (1) | Not expected in the next year | Minor; little data, quickly fixed | 2 to 3: low. Note it, review next time |
| Medium (2) | Could happen in the next year | Some records exposed or a day of downtime | 4: medium. Plan a fix with a date |
| High (3) | Likely, or has happened before | Many records exposed, or the office cannot see patients | 5 to 6: high. Fix first |

### Common threats to consider

- ☐ Phishing email or ransomware
- ☐ Lost or stolen laptop, phone or backup drive
- ☐ Shared or weak passwords
- ☐ Former employee's login still active
- ☐ Unpatched imaging or front desk computer
- ☐ Backup that fails or was never restored
- ☐ Records emailed or faxed to the wrong person
- ☐ Vendor breach or outage
- ☐ Open or shared Wi-Fi
- ☐ Fire, flood, power failure

| System (from step 1) | Threat | Vulnerability | Likelihood 1 to 3 | Impact 1 to 3 | Risk level |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Step 3. Current safeguards



Mark each safeguard in place, partly in place or missing. R means the rule marks it Required. A means Addressable: you must put it in place if it is reasonable and appropriate, or document why not and use an equivalent measure if reasonable (45 CFR 164.306(d)(3)). Items with no letter are standards without a separate implementation specification.

Mark: Y = in place, P = partly, N = missing:

### Administrative safeguards (164.308)

| | | |
|---|---|---|
| ____ | Security official named in writing | (a)(2) |
| ____ | Sanction policy for staff who break security policies | (a)(1)(ii)(C), R |
| ____ | Audit logs and access reports reviewed regularly | (a)(1)(ii)(D), R |
| ____ | Access removed the day someone leaves | (a)(3)(ii)(C), A |
| ____ | Each person has only the access their job needs | (a)(4)(ii)(B), A |
| ____ | Security awareness training for all staff, including the dentist owners | (a)(5) |
| ____ | Anti-malware on every computer; staff know how to report it | (a)(5)(ii)(B), A |
| ____ | Password rules written and followed | (a)(5)(ii)(D), A |
| ____ | Security incidents identified, responded to and documented | (a)(6)(ii), R |
| ____ | Backups make retrievable exact copies, and a restore has been tested | (a)(7)(ii)(A), R |
| ____ | Disaster recovery and emergency mode plans written | (a)(7)(ii)(B), (C), R |
| ____ | Business associate agreement signed with each vendor that handles patient information | (b)(3), R |

### Physical safeguards (164.310)

| | | |
|---|---|---|
| ____ | Server, network equipment and backups in a locked area | (a)(2)(ii), A |
| ____ | Screens placed or filtered so patients cannot read them | (b) |
| ____ | Workstations lock or are physically secured | (c) |
| ____ | Old drives, computers and copiers wiped or destroyed before disposal | (d)(2)(i), R |
| ____ | Devices wiped before reuse by someone else | (d)(2)(ii), R |

### Technical safeguards (164.312)

| | | |
|---|---|---|
| ____ | Every user has a unique login (no shared logins) | (a)(2)(i), R |
| ____ | Emergency access procedure for records during an outage | (a)(2)(ii), R |
| ____ | Automatic logoff or screen lock after inactivity | (a)(2)(iii), A |
| ____ | Laptops, phones and backup drives encrypted, or reason documented | (a)(2)(iv), A |
| ____ | Software records who accessed records (audit controls) | (b) |
| ____ | Email and file transfers with patient information encrypted, or reason documented | (e)(2)(ii), A |

# Step 4. Risk management plan



Risk management, 45 CFR 164.308(a)(1)(ii)(B): "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." List each medium and high risk from step 2 and each missing safeguard from step 3, starting with the highest.

| Risk or gap | Action | Owner | Due date | Done (date) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

### Addressable safeguards not used

For each addressable item you decided not to put in place, record why and what you use instead.

| Safeguard | Why not reasonable and appropriate | Equivalent measure used |
|---|---|---|
| | | |
| | | |
| | | |

### Sign-off

Security official (name and signature) _____ Date _____

Owner dentist (name and signature) _____ Next review due _____

Keep this assessment for 6 years from the date it was created or last in effect (45 CFR 164.316(b)(2)(i)). Review it periodically and when systems, locations or staff change (164.316(b)(2)(iii)). The rule sets no fixed interval. HHS says some offices repeat it annually and others as needed. The free HHS and ONC Security Risk Assessment Tool is another way to do the same work.