ePHIShield

SECURITY RISK ANALYSIS REPORT

Security Risk Analysis

Sunny Meadows Pediatrics

Single-location pediatric practice · synthetic demonstration engagement

PREPARED FOR

Sunny Meadows Pediatrics
Practice owner and management

ASSESSMENT DATE

November 2, 2026
45 CFR §164.308(a)(1)(ii)(A)

EDITION

Complete report · synthetic demonstration
Draft · not approved for release

Contains no patient information. This sample describes an invented practice created for demonstration and does not describe any real organization.

SYNTHETIC

About this report

This Security Risk Analysis Report documents ePHIShield's assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of Sunny Meadows Pediatrics (SYNTHETIC)'s electronic protected health information, the analysis 45 CFR 164.308(a)(1)(ii)(A) requires. It identifies the threats a practice of this kind can reasonably anticipate, the vulnerabilities through which each could occur, the safeguards each depends on and how far they were established, and rates each risk by likelihood and impact. It can be read on its own. How far it is accurate and thorough rests on the scope set out in Part B, the record and evidence described in Parts E and F, and the quality review and professional approval shown in its document control.

> This is a risk analysis, not a full assessment of compliance with every Security Rule requirement. Requirements are examined here as safeguards that bear on the risks. Where a requirement was examined only in part, or not at all, the report says so; nothing is concluded about what was not examined, and nothing in this report should be read as a statement that the practice meets or fails a requirement it does not evaluate.

Document control

Synthetic demonstration	This report was produced from a synthetic demonstration record. Every professional determination in it is part of the demonstration and is not an ePHIShield determination about any practice. It cannot be approved or delivered.
Practice	Sunny Meadows Pediatrics (SYNTHETIC)
Report	Security Risk Analysis Report
Report version	v78.19 (LISA-ENGINE-1.14.14), synthetic rehearsal
Engagement	Security risk analysis (45 CFR 164.308(a)(1)(ii)(A)); not a full Security Rule compliance assessment

Assessment scope	The practice's single location and the systems, vendors, remote access paths and external flows of ePHI recorded in this engagement, wherever they are (cloud services, devices and any remote work included). Limitations, assessed by ePHIShield's reviewer as not invalidating this risk analysis: Whether Old laptops in storage closet (2) holds or reaches patient information is not established (SYNTHETIC REHEARSAL. Two retired pre-2019 laptops whose contents nobody knows; they are analyzed under the disposal and lost-device threats and carried by the closet-laptop risk, whose step establishes what they hold. Evidence: On-site observation: two laptops in the unlocked storage closet, Office manager: used before athena, contents unknown). Based on the systems and information identified and reconciled during this engagement, no known in-scope environment was excluded. Reconciliation cannot establish that no unidentified system exists.
Assessment date	November 2, 2026 (information recorded through this date)
Site visit	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC): visited, October 21, 2026, ePHIShield analyst
Regulatory reference date	45 CFR Part 164 as revised October 1, 2025; HHS commentary from the 2003 Security Rule preamble (68 FR 8334) and the 2013 amendments (78 FR 5566)
Proposed rule status	The proposed amendment to the Security Rule (90 FR 898, Jan. 6, 2025) was still a proposed rule, with no final rule or withdrawal published and a final-action target of July 2027 in the most recent Unified Agenda entry, as verified against the Federal Register (document 2024-30983) and reginfo.gov (Unified Agenda, RIN 0945-AA22) on October 16, 2026. This report assesses current law only.
Professional review and approval	Not yet approved. This version is a draft for professional review and may not be released to the practice.
Explanation library	Threat library: 14 threat explanations (14 approved). Risk analysis narrative and methodology text: eight entries, eight approved. A report may be released only when every entry it uses has been reviewed and approved by ePHIShield for its current text.
Assessment engine	LISA-ENGINE-1.14.14. Engine release checks (the engine's internal consistency only; not a review of this report or an approval): none blocking. This report's QA result is in the next row; its approval is under Professional review and approval above.
Quality assurance	Automated QA at composition: one blocking finding (NQ-34: not a synthetic demonstration record); one pending professional review (NQ-19S: reviewer approval sealed with the engagement and still valid, and every threat explanation and risk analysis text used is approved for its current text). The check of the printed layout (NQ-50) runs on the finished PDF and is bound to that file's SHA-256; the QA record classifies each finding as blocking, review required (held until a reviewer records a disposition) or informational, and states the release eligibility. Presentation review is separate from the final professional approval. Release is not permitted while any finding is blocking or pending.

> **Findings and implementation.** This report records what ePHIShield found as of the assessment date. Implementing the corrective actions, deciding how to implement them, and maintaining the practice's security program remain the practice's responsibility. The

> urgency, timeframes and priorities stated here are ePHIShield's professional recommendations; they do not change what the regulation requires, and completing an action does not by itself establish compliance, which is confirmed at the next assessment.

How evidence is characterized

Term	Meaning
Documented	A document was provided and reviewed for the fact.
Observed	ePHIShield saw it during the site visit.
Reported	The practice stated it. It was not verified by document or observation.
Unresolved	The record does not establish it: not answered, answered "not sure," or a question the review could not close.

Two measures appear throughout and are kept apart. The level of risk combines likelihood and impact. The remediation priority says how soon to act and can be higher than the risk alone suggests, for example where the Rule requires a safeguard regardless of risk.

Summary for the practice owner

In plain words: what the analysis found, what to do, and what you need to decide. Each point names the Part of the report where it is set out in full.

The most serious exposures

- Unattended personal remote-access tool on the office PC: High risk. What could happen: An outsider who obtains the helper's TeamViewer credentials, or the helper's own compromised computer, takes control of the office manager's PC and reaches athena and locally saved scans. Why: a personal-edition TeamViewer allows unattended access at any time with a fixed password and no second factor. (Part D)
- Password-only remote access to athena and Gmail: High risk. What could happen: Someone who phishes or guesses a physician's password signs in to athenaOne or Gmail from anywhere and reads or changes patient records. Why: athena MFA is on only for the office manager's admin account. (Part D)
- Waiting-room tablet signed in to the EHR all day: High risk. What could happen: A parent or visitor using the check-in tablet navigates out of check-in and views or changes other patients' information. Why: the tablet stays signed in to athenaOne under a front-desk staff account with full front-desk access, unattended in the waiting room. (Part D)
- Texts and the practice Gmail app on unmanaged personal phones: High risk. What could happen: Appointment texts naming a child, and the practice mailbox reached through the Gmail app, stay on personal phones the practice does not manage, including the phones of staff who have left. Why: staff text parents from personal phones with no MDM and no remote wipe, and the inventory records the practice Gmail app on the same phones. (Part D)
- Lost or stolen device: High risk. What could happen: Laptop, tablet, phone, or portable drive containing ePHI is lost or stolen. Why: the safeguards it depends on that are not in place include encryption and decryption, device and media controls, accountability, and workstation security. (Part D)
- Disposal or reuse of equipment and media: High risk. What could happen: ePHI is disclosed through improperly disposed or reused hardware, media, or leased copiers. Why: the safeguards it depends on that are not in place include disposal and media re-use. (Part D)

21 exposures were assessed in all; the other 15 are listed with their levels in Part A. Each exposure is counted once, even where two records describe it.

What to do today

- Immediately disable any active account belonging to a former workforce member and review access logs for that account (Item 1, Part G).
- Accept Google's Workspace business associate agreement in the admin console (a same-day administrator action) (Item 2, Part G).
- Turn off TeamViewer's unattended access on the office manager PC, so no session can start without someone at the PC accepting it (Item 3, Part G).
- Sign the front-desk account out of the check-in tablet and change that account's password, which is on the sticky note (Item 4, Part G).
- Lock the storage closet, or move both retired laptops to a locked cabinet, and note who holds the key (Item 5, Part G).

- Write down what the office manager knows of the 2025 misdirected fax (what the form held, when it was learned of, who received it and what they said) and open the assessment with counsel (Item 6, Part G).
- Take down the sticky note and the whiteboard password, and change the posted Windows password, the Wi-Fi password and the alarm code (Item 7, Part G).
- Designate a named security official in writing with defined responsibility, authority, and allocated time for the HIPAA security program (Item 8, Part G).

What to do within 30 days

- Define access levels by job role, document the role-to-permission mapping, and reconcile system user lists against current staff at least quarterly (Item 9, Part G).
- One access-review routine, with each obligation kept (Item 10, Part G).
- Adjust and document system access at every role change, and perform a periodic documented review of all user rights (Item 11, Part G).
- Close the gaps in the existing endpoint protection (Windows Defender (built-in)) (Item 12, Part G).
- Confirm whether the existing endpoint protection (Windows Defender (built-in)) includes behavior-based detection and response on every practice machine, and add it only where it does not (Item 13, Part G).
- Ensure every system holding ePHI enforces authenticated, individually attributable access, and retire or isolate any system that cannot (Item 14, Part G).

12 further 30-day items are in Part G.

> The timeframes are ePHIShield's recommended targets, not deadlines set by law, except where Part G says a deadline is the law's.

What you need to decide or find out

15 open questions could change a rating once answered. Each is in Schedule H-7 with who settles it and the evidence that settles it:

- Whether Windows Defender is running and current on every practice PC.
- The patch state of the PCs other than the Windows 10 front-desk PC, and of the gateway.
- Whether the physicians' personal laptops hold downloaded ePHI and are encrypted.
- What the two retired closet laptops hold.
- What credential and image cache the leased copier holds, and how its drive is handled at lease return.
- Whether athenaOne and Gmail keep audit logs, and for how long.

Nine more are in Schedule H-7.

A. Summary of risks

Threat	Likelihood	Impact	Risk	Treatment
Unattended personal remote-access tool on the office PC (reviewer-recorded)	High	High	High	Item 3, Item 47
Front-desk PC running Windows 10 past end of support (reviewer-recorded) (included in: exploited unpatched or unsupported systems)	High	High	High	Item 48
Password-only remote access to athena and Gmail (reviewer-recorded)	High	High	High	Item 19
Waiting-room tablet signed in to the EHR all day (reviewer-recorded)	High	High	High	Item 4, Item 49
Texts and the practice Gmail app on unmanaged personal phones (reviewer-recorded)	High	High	High	Item 50
Two retired unencrypted laptops in an unlocked closet (reviewer-recorded) (included in: disposal or reuse of equipment and media)	High	High	High	Item 5, Item 38, Item 39, Item 51, Item 55, Item 56
Lost or stolen device	Very High	High	High	Item 16, Item 38, Item 41, Item 42
Disposal or reuse of equipment and media	Very High	High	High	Item 39, Item 40, Item 5, Item 38, Item 51, Item 55, Item 56
Inappropriate access by a staff member	High	High	High	Item 9, Item 15, Item 27, Item 28, Item E2
Access retained after someone leaves	Very High	High	High	Item 1, Item 10, Item 11, Item 28
Phishing and stolen email credentials	Very High	High	High	Item 17, Item 18, Item 29, Item 30, Item 31, Item 70

Threat	Likelihood	Impact	Risk	Treatment
Ransomware	Very High	High	High	Item 12, Item 13, Item 17, Item 18, Item 29, Item 32, Item 33, Item 34, Item 35, Item 36, Item 37, Item 46
Shared sign-in without individual attribution	Very High	High	High	Item 15, Item 28, Item E2
Interception or misdirection in transit	High	High	High	Item 43, Item 45
Exploited unpatched or unsupported systems	High	High	High	Item 12, Item 13, Item 14, Item 28, Item 46, Item 63, Item 71, Item 48
Shared physical and network secrets never changed (reviewer-recorded)	Moderate	High	Moderate	Item 7, Item 52, Item 53, Item 55, Item 56, Item 61, Item 72
Patient information kept by services with no agreement on record (reviewer-recorded) (included in: vendor compromise)	Moderate	High	Moderate	Item 2, Item 24
Fire, flood, storm or power loss	Moderate	High	Moderate	Item 33, Item 34, Item 35, Item 54, Item 77
Unauthorized physical access	Moderate	High	Moderate	Item 55, Item 56, Item 58, Item 72, Item 73
Vendor compromise	Moderate	High	Moderate	Item 20, Item 21, Item 22, Item 23, Item 2, Item 24
Misdirected fax never assessed; no working incident procedure (reviewer-recorded)	High	Moderate	Moderate	Item 6, Item 60, Item 64, Item 65, Item 66, Item 67, Item 68
Policy binder states controls that do not exist (reviewer-recorded)	Moderate	Moderate	Moderate	Item 75
Permanent data loss	High	Moderate	Moderate	Item 34, Item 35, Item 36, Item 37, Item 74
Visible or unattended screens	Very High	Moderate	Moderate	Item 57, Item 58, Item 59

Every risk assessed, highest first. A risk marked 'included in' describes part of the same current exposure as the risk named, and is counted once, there.

21 current exposures were assessed (14 from ePHIShield's threat catalog and seven recorded by the reviewer): 13 High and eight Moderate. Three further records (front-desk PC running Windows 10 past end of support, in exploited unpatched or unsupported systems, two retired unencrypted laptops in an unlocked closet, in disposal or reuse of equipment and media, and patient information kept by services with no agreement on record, in vendor compromise) are counted inside the exposure named, not twice. The highest assessed level is High, for unattended personal remote-access tool on the office PC, password-only remote access to athena and Gmail, waiting-room tablet signed in to the EHR all day, texts and the practice Gmail app on unmanaged personal phones, lost or stolen device, disposal or reuse of equipment and media, inappropriate access by a staff member, access retained after someone

leaves, phishing and stolen email credentials, ransomware, shared sign-in without individual attribution, interception or misdirection in transit, and exploited unpatched or unsupported systems.

> **What to do first.** Immediate containment, before anything else: Item 1, Immediately disable any active account belonging to a former workforce member and review access logs for that account; Item 2, Accept Google's Workspace business associate agreement in the admin console (a same-day administrator action); Item 3, Today: turn off TeamViewer's unattended access on the office manager PC, so no session can start without someone at the PC accepting it; Item 4, Today: sign the front-desk account out of the check-in tablet and change that account's password, which is on the sticky note; Item 5, Today: lock the storage closet, or move both retired laptops to a locked cabinet, and note who holds the key; Item 6, Today: write down what the office manager knows of the 2025 misdirected fax (what the form held, when it was learned of, who received it and what they said) and open the §164.402 assessment with counsel; Item 7, Today: take down the sticky note and the whiteboard password, and change the posted Windows password, the Wi-Fi password and the alarm code; give staff the new ones in person; Item 8, Designate a named security official in writing with defined responsibility, authority, and allocated time for the HIPAA security program.

> **What is not yet established.** One safeguard that the risk ratings depend on is not yet established, so those ratings rest partly on what is unknown: §164.312(b) Audit controls (unable to determine). Three steps to establish the facts are listed in Part G. Until they are settled, these safeguards are not evaluated as in place.

> **Material items still open.** 15 material items are still open. Each bears on the ratings above and is listed with the same identifier in Schedule H-7, the one register of what is unresolved, with its owner and the evidence that settles it.

- Open item 1 (material question (reviewer); Front desk PCs 1 and 2, Exam room PCs (4), Office manager PC): Whether Windows Defender is running and current on every practice PC. Bears on: ransomware, exploited unpatched or unsupported systems, §164.308(a)(5)(ii)(B).
- Open item 2 (material question (reviewer); Front desk PC 1, Exam room PCs (4), Office manager PC, Comcast Business gateway and Wi-Fi): The patch state of the PCs other than the Windows 10 front-desk PC, and of the gateway. Bears on: exploited unpatched or unsupported systems.
- Open item 3 (material question (reviewer); Physicians' personal laptops): Whether the physicians' personal laptops hold downloaded ePHI and are encrypted. Bears on: lost or stolen device, ransomware, password-only remote access to athena and Gmail.
- Open item 4 (material question (reviewer); Old laptops in storage closet (2)): What the two retired closet laptops hold. Bears on: two retired unencrypted laptops in an unlocked closet, disposal or reuse of equipment and media, permanent data loss.
- Open item 5 (material question (reviewer); Canon multifunction copier): What credential and image cache the leased copier holds, and how its drive is handled at lease return.

Bears on: shared physical and network secrets never changed, disposal or reuse of equipment and media.

- Open item 6 (material question (reviewer); athenaOne; Google Workspace email): Whether athenaOne and Gmail keep audit logs, and for how long. Bears on: §164.312(b), inappropriate access by a staff member, shared sign-in without individual attribution.
- Open item 7 (material question (reviewer); eFax Corporate): The facts of the 2025 misdirected fax needed for the breach assessment. Bears on: misdirected fax never assessed; no working incident procedure, interception or misdirection in transit.
- Open item 8 (material question (reviewer); Staff personal phones): Whether staff phones are encrypted and passcode-locked, and whether departed staff still hold parent text threads. Bears on: texts and the practice Gmail app on unmanaged personal phones, lost or stolen device.
- Open item 9 (material question (reviewer); eFax Corporate; Valley After-Hours Answering (SYNTHETIC)): Whether an agreement exists with eFax and with Valley After-Hours Answering (none was produced when requested on site). Bears on: vendor compromise, patient information kept by services with no agreement on record, §164.308(b)(1).
- Open item 10 (material question (reviewer); Office manager PC; TeamViewer (personal edition)): Whether the TeamViewer access was used by anyone other than the helper. Bears on: unattended personal remote-access tool on the office PC.
- Open item 11 (material question (reviewer); Staff personal phones; Google Workspace email): How staff confirm a number or address belongs to the child's parent or guardian before texting or emailing. Bears on: texts and the practice Gmail app on unmanaged personal phones, interception or misdirection in transit.
- Open item 12 (material question (reviewer); athenaOne): Whether the departed MA's athenaOne account was used after August 2025. Bears on: access retained after someone leaves, inappropriate access by a staff member.
- Open item 13 (verification requested; practice-wide): Requested once (round 2); no document was received. The answer stands as reported, not verified. Bears on: inappropriate access by a staff member.
- Open item 15 (not answered; practice-wide): Not established after 2 attempt(s), first with the practice administrator and then by another route (ask the HIPAA security official instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established. Bears on: phishing and stolen email credentials, ransomware.
- Open item 16 (not answered; practice-wide): Not established after 3 attempt(s), first with the IT provider and then by another route (ask the practice administrator, for the vendor's documentation or a vendor contact who can answer instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established. Bears on: ransomware, fire, flood, storm or power loss, permanent data loss.

53 safeguards were examined (Part E); 14 requirements belonging to a full Security Rule assessment were not examined and nothing is concluded about them.

Contents

About this report 2

Summary for the practice owner 5

A. Summary of risks 7

B. Scope and environment 12

C. Methodology 14

D. Risk analysis by threat 19

- Unattended personal remote-access tool on the office PC 19
- Front-desk PC running Windows 10 past end of support 21
- Password-only remote access to athena and Gmail 22
- Waiting-room tablet signed in to the EHR all day 24
- Texts and the practice Gmail app on unmanaged personal phones 25
- Two retired unencrypted laptops in an unlocked closet 27
- Lost or stolen device 28
- Disposal or reuse of equipment and media 31
- Inappropriate access by a staff member 33
- Access retained after someone leaves 35
- Phishing and stolen email credentials 37
- Ransomware 40
- Shared sign-in without individual attribution 43
- Interception or misdirection in transit 46
- Exploited unpatched or unsupported systems 48
- Shared physical and network secrets never changed 50
- Patient information kept by services with no agreement on record 52
- Fire, flood, storm or power loss 53
- Unauthorized physical access 55
- Vendor compromise 57
- Misdirected fax never assessed; no working incident procedure 61
- Policy binder states controls that do not exist 62
- Permanent data loss 64
- Visible or unattended screens 66

E. Current safeguards and evidence 68

F. Professional determinations and limitations 88

G. Risk treatment plan 97

H. Schedules 133

Technical schedules (H-9, H-10, H-11) 157

B. Scope and environment

Scope. The practice's single location and the systems, vendors, remote access paths and external flows of ePHI recorded in this engagement, wherever they are (cloud services, devices and any remote work included). Limitations, assessed by ePHIShield's reviewer as not invalidating this risk analysis: Whether Old laptops in storage closet (2) holds or reaches patient information is not established (SYNTHETIC REHEARSAL. Two retired pre-2019 laptops whose contents nobody knows; they are analyzed under the disposal and lost-device threats and carried by the closet-laptop risk, whose step establishes what they hold. Evidence: On-site observation: two laptops in the unlocked storage closet, Office manager: used before athena, contents unknown). Based on the systems and information identified and reconciled during this engagement, no known in-scope environment was excluded. Reconciliation cannot establish that no unidentified system exists.

> **Site visit and places not visited.** ePHIShield visited 2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (October 21, 2026, ePHIShield analyst). These places were neither visited nor evaluated remotely: Physicians' homes (remote access to athenaOne from personal laptops) (Physicians' personal laptops); Computer helper's home (remote support from his own computer). Nothing there was observed; what the analysis records about them rests on the answers of the practice and its vendors, and it makes no statement about physical conditions there (who else is in the room, who else uses the device, what can be seen or overheard). This is a limitation of the analysis (Part F).

Fact	Recorded	Source
Practice	Sunny Meadows Pediatrics (SYNTHETIC)	Profile
Specialty	Pediatrics	Profile
Locations	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC)	Profile

Fact	Recorded	Source
People with access to patient information	7	Profile
Systems named at setup	athenaOne, Google Workspace email, eFax Corporate, LabCorp lab interface, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet, Staff personal phones, Physicians' personal laptops, Old laptops in storage closet (2), and Canon multifunction copier	Profile
Recorded as holding or reaching patient information	athenaOne, Google Workspace email, eFax Corporate, LabCorp lab interface, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet, Staff personal phones, Physicians' personal laptops, Canon multifunction copier, and TeamViewer (personal edition)	Inventory
Recorded as holding none (with the basis)	Comcast Business gateway and Wi-Fi (Seen on site, confirmed by the computer helper: the gateway routes internet traffic and serves staff and guest Wi-Fi; no files, scans or mail are stored on it. Patient information passes through it (transit), and is not kept there.)	Inventory
Holding not established	Old laptops in storage closet (2)	Inventory
Hosting of the main record system	Vendor-hosted (cloud)	Record
Patient information held on practice equipment	Yes: Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet, and Canon multifunction copier (recorded system inventory)	Record
Remote access	Yes	Record
IT support	As answered: “My nephew Kyle (SYNTHETIC) helps a few hours a month; athena handles the EHR” (category chosen: a staff member who is good with computers)	Intake answer
Patient volume	3,200	Profile
Site visit	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC): visited, October 21, 2026, ePHIShield analyst	Location review

Facts that set the scope and adjust ratings. 'Not established' means the record does not settle it; such a fact neither raises nor lowers a rating.

Each system, location and recorded flow of patient information, with how each is known and a diagram, is in Schedule H-1 of this report.

C. Methodology

What comes from NIST SP 800-30

The analysis follows the structure of NIST Special Publication 800-30 Rev. 1, which HHS guidance on risk analysis draws on. From it come the concepts used throughout: a threat source initiates a threat event, which exploits a vulnerability, with a likelihood of occurring and an impact if it does; the five-level qualitative scales (Very Low to Very High); and Table I-2, which combines likelihood and impact into a level of risk.[1]

The elements HHS's Office for Civil Rights describes for a risk analysis are addressed as follows: the scope is the electronic patient information the practice creates, receives, maintains or transmits, in the environments listed in Part B; threats and vulnerabilities are identified per threat (Part D), including risks recorded by ePHIShield's reviewer outside the catalog; current security measures are summarized with their evidence in Part E; likelihood, impact and the level of risk are rated per threat; and the analysis is documented in this report and reviewed at each assessment.[2]

Likelihood \ Impact	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

NIST SP 800-30 Rev. 1, Appendix I, Table I-2: level of risk as a combination of likelihood and impact.

1. Methodology. NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments (Sept. 2012), Appendix G (likelihood), Appendix H (impact) and Appendix I, Table I-2 (level of risk). Methodology, not regulatory text.
2. Guidance. HHS Office for Civil Rights, Guidance on Risk Analysis Requirements under the HIPAA Security Rule: elements of a risk analysis. Guidance, not regulatory text.

What is L.I.S.A.'s own scoring

NIST SP 800-30 does not say how likely a given threat is for a given practice, or how much a safeguard should move that likelihood. Those values are ePHIShield's, implemented in L.I.S.A., and are stated here so they can be examined. They are not attributed to NIST.[3]

- Starting points. Each threat in ePHIShield's catalog has a starting likelihood and impact for a small medical practice, shown in each analysis.
- Safeguard weights. Each safeguard the threat depends on is weighted by its status in Part E (table below). The weights are averaged.
- Scaling. The average is multiplied by 1.6 and rounded; the result is the number of steps likelihood moves from its starting point, down where safeguards are in place, up where they are absent or unverified.
- Adjustments. Only these recorded facts adjust a likelihood, each because it is an exposure mechanism the threat's safeguards do not already weigh: the likelihood of fire, flood, storm or power loss -1 where the record establishes, with its basis, that no patient information is held on practice equipment (Where the practice keeps no patient information on its own equipment, loss of the premises does not destroy the data; the record vendor carries site risk. Not a safeguard the threat weighs). An unrecorded fact adjusts nothing. These conditions do not adjust a likelihood: the likelihood of inappropriate access by a staff member where the recorded number of people with access is above 25 (a fixed cutoff at 25 is a scoring cliff that establishes nothing about user privileges, reachable records, monitoring or insider exposure. Workforce size stays as assessment context; an established insider exposure is rated by a documented threat-specific professional judgment); the likelihood of lost or stolen device where remote access is established and device encryption (§164.312(a)(2)(iv)) is not established as implemented (remote access does not by itself make a device more likely to be lost or stolen, and encryption (§164.312(a)(2)(iv)) is already a safeguard the lost-device threat weighs); the likelihood of phishing and stolen email credentials where remote access is established and person or entity authentication (§164.312(d)) is not established as implemented (the authentication defect is already weighed through §164.312(d), a safeguard of the phishing threat; adding a step counts it twice).
- Limits on how far a rating moves. Where the record establishes the threat's own precondition (active log-ins of people who no longer work here, for access retained after departure; an established shared log-in, for shared sign-in), safeguards may not lower likelihood below the starting point. Unknown never triggers it. Vendor assurance lowers the likelihood of vendor compromise by one step at most, and not at all unless every material vendor is assessed as supporting. A reviewer's incident disposition whose attack path remains may raise likelihood (one level, more only with heightened review), never lower it. A current, documented reviewer impact determination sets impact. A safeguard an established incident shows did not operate as credited is capped at Partially Implemented once (documented implementation); for the threat weight it is weighed as

3. ePHIShield. L.I.S.A. scoring, ePHIShield's own method: the starting points, safeguard weights, scaling and adjustments are not taken from NIST SP 800-30, which sets no such values.

partly in place only for the threats the incident's recorded attack path is an instance of, and its credit stands for other threats and where a corrective measure since the incident is on record. The same failure never moves both the weight and the likelihood.

- System scoping. Where a shared sign-in is established on a particular system, that threat's safeguards are judged on that system: unique identification counts as absent, and audit controls and activity review earn no credit, because there they record the account rather than the person.
- Evidence. A safeguard rated Implemented counts fully only where its operation is shown; on the practice's report alone, or on a documented addressable decision without evidence that the measure operates, it counts as partly in place (table below).
- Standards and their specifications. Where a standard's own safeguards are in place but a specification beneath it is an established deficiency, the standard is weighed as partly in place for each threat that specification bears on, and in full for the others; its status in Part E is unchanged.
- Vendor compromise. The business associate agreements are assessed as contractual assurances and do not move this rating. Each in-scope vendor counts by what ePHIShield's reviewer concluded about its own security evidence (supports −1, partly supports −0.4, does not support or not assessed 0), averaged and scaled the same way.
- Risks outside the catalog. A questionnaire and a fixed catalog cannot surface every risk a practice has. Where ePHIShield's reviewer identified a risk the catalog does not rate, it is recorded with the threat event, the affected asset, location or flow, the vulnerability, the existing safeguards, the evidence, a likelihood and an impact on the same scales, the rationale, the reviewer and the date. Its level of risk comes from the same table (Table I-2). Its treatment is chosen on the same facts, as for any identified risk: corrective action, monitoring, or a documented decision by the practice to accept the risk. Where corrective action is recorded, it is in the plan.

Status in Part E	Weight	Meaning
Implemented with its operation shown (observed, or a document recording it), or a reviewed adequate alternative	−1	counts fully as in place
Implemented with operation shown for some parts or systems and reported for others	−1	counts fully as in place, unless ePHIShield's reviewer judges the evidence does not support the protection credited; then as partly in place (where the credit changes a likelihood or a risk level, the reviewer must judge)
Implemented on the practice's report only, on a documented addressable decision, or on a written policy or procedure where the requirement is to apply it (sanctions, ending access), without evidence that it operates	−0.4	counts as partly in place; for a written procedure, ePHIShield's reviewer may judge it functioning on what was reasonably assessed, which counts it fully
Partially Implemented, Partly Established, or Reported, Not Verified	−0.4	counts as partly in place
Unable to Determine, or an alternative awaiting review	+0.5	cannot be credited, and the uncertainty counts against
Not Implemented	+1	counts as absent

L.I.S.A. safeguard weights (ePHIShield's method).

> Unknown, absent and reported are kept apart. A safeguard the record shows is not in place counts as absent. A safeguard that could not be established is Unknown: it is neither assumed absent nor credited as in place; it counts against the rating as uncertain (Part C), and the open question is listed with what would settle it. An answer the practice gave is reported as its statement unless a document or an observation verified it. A safeguard rated Implemented counts fully only where its operation was shown; resting on the practice's report alone, on a documented decision, or on a written policy where the requirement is to apply it, without evidence that it operates, it counts as partly in place, unless ePHIShield's reviewer judges a documented procedure to be functioning on what was reasonably assessed. Where operation was shown for some parts or systems and only reported for others, it counts fully unless the reviewer judged that the evidence does not support the protection credited; where that credit changes a likelihood or a level, the reviewer must judge (Part F). The ratings are qualitative judgments made consistently, not statistical probabilities.

> Where the practice reports that an addressable specification is met by an alternative, the analysis credits the alternative only as far as reviewed evidence shows it operates and protects the information. The practice's obligation to document its decision for each addressable specification, and why, remains in force (45 CFR 164.306(d)(3) and 164.316); this report does not make that decision for the practice.

Impact review. ePHIShield's reviewer considered each threat's impact against the sensitivity facts the record establishes: Most of the practice's patients are minors: school and daycare forms and shot records are held in Gmail (inventory, computer helper). SYNTHETIC REHEARSAL. Every catalog threat's impact was considered against the systems in the inventory and what they hold. Minors' records are protected health information like any other

under the Security Rule; no recorded fact (such as a state confidentiality rule) supports a higher impact for any threat on that ground. The same reach judgment is applied to data loss and ransomware: athenahealth holds the chart, so neither threat makes the chart unavailable from the practice's side; ransomware keeps a disclosure consequence that data loss does not, and is set one level lower only. Shared sign-in is set one level higher: the shared accounts are not confined to a workstation but reach athena's front-desk role for every patient (the kiosk), the frontdesk@ mailbox and the eFax archive. The reviewer set the impact of three threats (permanent data loss; ransomware; shared sign-in without individual attribution); each is explained in that threat's analysis. The others stay at their starting points. (A. Reviewer (SYNTHETIC), October 21, 2026.)

Incident review. ePHIShield's reviewer recorded a disposition for each prior incident the record establishes. A past incident never raises a rating by itself; a reviewer may raise a threat's likelihood only where the attack path remains and the safeguards' credit overstates protection. (A. Reviewer (SYNTHETIC), October 21, 2026.)

- Spring 2025: a school form was faxed to a wrong number, one digit off; the business that received it called and said it was shredded; the form was re-faxed to the right number and nothing was written up: the attack path remains. Path: Misdirected transmission: a fax number was keyed wrongly in the shared eFax account and the form went to an outside recipient, with no check of the number before sending and no incident handling afterwards. Evidence: Intake prior-incidents (office manager, round 1): the spring 2025 misfax; Intake incident-detail (office manager, round 1): re-faxed, nothing written up; Inventory eFax Corporate (office manager): one shared login, still used for referrals and records requests; No fax-number check or working incident procedure is recorded; the binder's template procedure was rejected as not adopted. Corrective action: Item 6, Item 60, Item 64, Item 65, Item 66, Item 67, and Item 68, the treatment of the risk that carries this incident (each set out in full once, in Part G). Carried as the reviewer-recorded risk “Misdirected fax never assessed; no working incident procedure”. Likelihood of interception or misdirection in transit reviewed against it (shown in that threat's analysis).

D. Risk analysis by threat

One analysis for each of the 24 risks, highest first. Each describes what could go wrong, the recorded data environment, the safeguards the threat depends on, how the rating was reached, related risks and the treatment. 24 risk records are analyzed; three of them are counted inside another record's exposure, so Part A counts 21 current exposures.

Unattended personal remote-access tool on the office PC (recorded by ePHIShield's reviewer)

Threat source: Adversarial: external, through a third-party remote tool · Assessed risk: High (likelihood High, impact High)

Threat event	An outsider who obtains the helper's TeamViewer credentials, or the helper's own compromised computer, takes control of the office manager's PC and reaches athena and locally saved scans.
Asset, location or flow	Remote control of the administrator PC; Office manager PC
Vulnerability	A personal-edition TeamViewer allows unattended access at any time with a fixed password and no second factor; the helper has no written agreement or BAA, and no one reviews its sign-ins.
Existing safeguards	TeamViewer password set by the helper (fixed, no 2FA).
Evidence	Computer helper (round 2), inventory TeamViewer (personal edition): unattended access with a fixed password, no 2FA; Computer helper (round 2), inventory Office manager PC: TeamViewer installed for the helper; Vendor record, computer helper: no agreement (office manager); addressable-164.308(a)(5)(ii)(C): failed logins to TeamViewer are never reviewed
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 3 (High), Item 47 (High)

Why it was recorded

> Unattended remote control by an outside party with no agreement is a direct path to the practice's administrator PC; the catalog's vendor threat assumes a contracted vendor, which this is not.

This risk is outside ePHIShield's threat catalog, so L.I.S.A.'s starting points and safeguard weights do not apply to it. The likelihood and impact are the reviewer's judgment on the facts above; the level of risk is read from NIST SP 800-30 Table I-2. In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Vendor compromise (catalog): likelihood Moderate, impact High, level Moderate, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: unattended access is on at all times with a fixed password and no second factor, from an outside party's own computer that the practice does not manage, and no one reviews TeamViewer sign-ins; nothing has to be defeated beyond one password.
Affected systems	Office manager PC and TeamViewer (personal edition)
Plausible information reach	The office manager PC: athenaOne practice administration, the Scans folder and downloaded reports, and the Gmail mailbox open on it
Sensitivity	Charts reached through athena administration, school and daycare forms and referral attachments in the Scans folder
Harm to patients and the practice	Full control of the administrator PC: viewing, copying or changing patient information, and changing athena users
Clinical and operational impact	Loss of trust in the administrator PC and the athena practice administration until rebuilt and reviewed
Supporting evidence	Inventory TeamViewer (personal edition) and Office manager PC (computer helper); vendor record for the helper (no agreement); addressable-164.308(a)(5)(ii)(C): TeamViewer sign-ins never reviewed
Rests on	TeamViewer (personal edition); Office manager PC; §164.308(a)(5)(ii)(C) (the practice's addressable determination)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from vendor compromise; both are counted. Why the ratings differ (Moderate there, High here): Vendor compromise rates a breach of a vendor's own systems and moves only on assessed vendor evidence. This is a standing remote-control channel into the administrator PC, open now with one fixed password, from a computer outside any agreement: a direct path, so its likelihood is High where vendor compromise is Moderate.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 3; Near-term correction: Item 47.

Front-desk PC running Windows 10 past end of support (recorded by ePHIShield's reviewer)

Threat source: Adversarial: external, malware · Assessed risk: High (likelihood High, impact High)

Threat event	Malware exploits a Windows 10 weakness that may go unpatched on the front-desk PC, which is signed in to athena all day under a shared account.
Asset, location or flow	Unsupported operating system; Front desk PC 2
Vulnerability	Windows 10 reached end of support on October 14, 2025. The record does not show that this PC is enrolled in Microsoft's paid Extended Security Updates (ESU); without enrollment it receives no security updates. No one sees antivirus alerts.
Existing safeguards	Built-in Windows Defender is reported on the practice PCs (whether it runs on this one is not established); athena is cloud-hosted, so no patient database sits on the PC.
Evidence	Computer helper (round 2), inventory Front desk PC 2: Windows 10 (out of vendor support since Oct 2025), shared account; system-access-controls (computer helper, round 2): the shared Windows accounts are local administrators on the PCs; Inventory gateway (computer helper; analyst on site): guest Wi-Fi on the same network as the practice PCs; antimalware-monitoring (computer helper): no one sees Defender alerts
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 48 (High)

Why it was recorded

> A known unsupported system is the one place in the practice where the unpatched-systems exposure is established rather than unknown; it is the established instance of that catalog risk, carried here for its own step.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Exploited unpatched or unsupported systems (catalog): likelihood High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: Windows 10 reached end of support on October 14, 2025 and the record does not show ESU enrollment, so without it any new weakness stays open; the PC runs under the shared FrontDesk account, which is a local administrator, sits on the network the guest Wi-Fi shares, and no one sees its Defender alerts.
Affected systems	Front desk PC 2
Plausible information reach	Front desk PC 2: the athenaOne session open all day, the downloads folder, and the other PCs on the same network
Sensitivity	Front-desk athena data (demographics, guarantor and insurance, schedule) and downloaded documents

Harm to patients and the practice	Malware on the PC can read the open athena session and downloads and spread to the other practice PCs
Clinical and operational impact	Check-out and payments stop on that PC until rebuilt; athena remains reachable from other devices
Supporting evidence	Inventory Front desk PC 2 (Windows 10 past end of support, shared account); system-access-controls (shared Windows accounts are local administrators); inventory gateway (guest Wi-Fi on the same network); antimalware-monitoring (no one sees alerts)
Rests on	Front desk PC 2; §164.312(a)(1) (“For each system on the inventory, does each user have …”); §164.308(a)(5)(ii)(B) (“Does anyone receive and act on alerts from that software”); Comcast Business gateway and Wi-Fi
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Part of the same current exposure as exploited unpatched or unsupported systems; counted once, there. What differs: The same current exposure: exploitation of an unpatched system to reach the practice network. This PC is where it is established rather than unknown, so it is counted once, inside the unpatched-systems rating, and kept here only for its own replacement step. The level is the same as the general threat's (High).

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Item 48.

Password-only remote access to athena and Gmail (recorded by ePHIShield's reviewer)

Threat source: Adversarial: external, credential theft · Assessed risk: High (likelihood High, impact High)

Threat event	Someone who phishes or guesses a physician's password signs in to athenaOne or Gmail from anywhere and reads or changes patient records.
Asset, location or flow	Remote sign-in to the record and email; athenaOne
Vulnerability	athena MFA is on only for the office manager's admin account; physicians use personal laptops with a password only, and Google 2-step verification is not enforced.
Existing safeguards	athenaOne named accounts and complexity rules; MFA on the office manager's admin account.
Evidence	Intake remote-access-mfa (round 2): password only; Inventory athenaOne (user list): MFA enforced only on the office manager's admin account; Computer helper (round 2): Google 2-step verification not enforced
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 19 (Critical)

Why it was recorded

> How remote access is authenticated is recorded but does not by itself rate any catalog threat, so no corrective step for it arises from the catalog; it is carried here as its own risk.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Phishing and stolen email credentials (catalog): likelihood Very High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: the physicians reach athenaOne from personal home laptops with a password only, Google 2-step verification is not enforced, and Windows and other passwords are reused; one phished, guessed or reused password is enough to sign in from anywhere.
Why below the computed value	Phishing's Very High likelihood is computed practice-wide, across every account and every message that can reach any staff member; this record is one path, the two physicians' sign-ins from their own home laptops, a smaller population of accounts and devices. High states that one path without claiming the practice-wide frequency; the level (High) is unchanged by the difference.
Affected systems	athenaOne, Google Workspace email, and Physicians' personal laptops
Plausible information reach	athenaOne (the full pediatric chart, demographics, guarantor and insurance, immunizations) and Google Workspace email
Sensitivity	The full chart of the practice's patients, most of them minors, and the forms and shot records in Gmail
Harm to patients and the practice	Reading, copying or changing charts under a physician's identity, undetected because sign-ins are not reviewed
Clinical and operational impact	Chart integrity in doubt until the account's activity is reviewed; physician access suspended while reset
Supporting evidence	Intake remote-access-mfa (round 2): password only; inventory athenaOne (user list): MFA only on the admin account; inventory Google Workspace: 2-step verification not enforced
Rests on	§164.312(d) (“If staff connect from outside the office, is a second …”); §164.312(d) (“How do users prove who they are — password only …”); athenaOne; Google Workspace email
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from phishing and stolen email credentials; both are counted. What differs: Phishing rates a workforce member giving up an email credential, which reaches the mailbox. This rates sign-in to athenaOne itself, the full chart, from any internet location with any stolen, guessed or reused password, a reach the email threat does not have. The missing second factor is weighed once in each threat's own consequence, not twice in one rating.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Item 19.

Waiting-room tablet signed in to the EHR all day (recorded by ePHIShield's reviewer)

Threat source: Adversarial: opportunistic visitor · Assessed risk: High (likelihood High, impact High)

Threat event	A parent or visitor using the check-in tablet navigates out of check-in and views or changes other patients' information.
Asset, location or flow	EHR access from the waiting room; Check-in kiosk tablet
Vulnerability	The tablet stays signed in to athenaOne under a front-desk staff account with full front-desk access, unattended in the waiting room.
Existing safeguards	Placed near the front desk.
Evidence	On-site observation: kiosk signed in under the front-desk account; On-site observation: kiosk password on the front-desk sticky note; Intake role-access (office manager): the tablet uses a front desk login
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 4 (High), Item 49 (High)

Why it was recorded

> A patient-facing device with staff-level access is not covered by the catalog's screen-visibility or shared-login threats, which assume staff devices.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Shared sign-in without individual attribution (catalog): likelihood Very High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: the tablet is observed signed in to athenaOne all day under a front-desk staff account, unattended in the waiting room, with the account's password on a sticky note at the front desk; a parent needs only to leave the check-in screen.
Why below the computed value	Shared sign-in's Very High likelihood is computed from shared logins in daily use by the whole staff; this record is one tablet reachable only by someone in the waiting room choosing to touch it. Opportunity is constant, use by a visitor is not, so High.
Affected systems	Check-in kiosk tablet and athenaOne
Plausible information reach	athenaOne with the front-desk role: every patient's demographics, guarantor and insurance, and schedule
Sensitivity	Children's identifying and insurance details for every patient, as the athena inventory records
Harm to patients and the practice	Viewing or changing other families' information by a visitor, with no record of who did it
Clinical and operational impact	Check-in moves to the front desk while the tablet is reconfigured

Supporting evidence	On-site observation: kiosk signed in under the front-desk account, password on the sticky note; intake role-access (office manager): the tablet uses a front desk login
Rests on	Check-in kiosk tablet; §164.312(a)(2)(i) (“If any logins are shared, which systems and how many …”); §164.308(a)(3)(i) (“Does each staff role get a different level of access …”)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from shared sign-in without individual attribution; both are counted. What differs: Shared sign-in rates the loss of attribution among workforce members. Here the person using the account is not a workforce member at all: a visitor in the waiting room reaches staff-level access to every patient. A different actor and consequence, so both are counted.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 4; Near-term correction: Item 49.

Texts and the practice Gmail app on unmanaged personal phones (recorded by ePHIShield's reviewer)

Threat source: Non-adversarial: workforce error; adversarial: device theft · Assessed risk: High (likelihood High, impact High)

Threat event	Appointment texts naming a child, and the practice mailbox reached through the Gmail app, stay on personal phones the practice does not manage, including the phones of staff who have left, where the practice cannot reach, wipe or account for them. (A text sent to the wrong number is rated under interception or misdirection in transit.)
Asset, location or flow	SMS threads with child names and appointment times, and the practice Gmail mailbox as reached through the Gmail app; Staff personal phones
Vulnerability	Staff text parents from personal phones with no MDM and no remote wipe, and the inventory records the practice Gmail app on the same phones; their encryption and passcodes are not known; threads and the signed-in mailbox remain with staff who leave.
Existing safeguards	None recorded.
Evidence	Inventory Staff personal phones (office manager): SMS threads with child names and appointment times; personal passcodes unknown; no MDM; email-phi (office manager): staff text parents; encryption-mobile (helper): remote wipe No; encryption not known; addressable-164.308(a)(3)(ii)(C): departed staff keep parent text threads on their personal phones
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 50 (High)

Why it was recorded

> Catalog lost-device and transmission threats do not reach retention on departed staff's phones or the choice of recipient.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Lost or stolen device (catalog): likelihood Very High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: staff text parents from personal phones with no management or remote wipe, and the record establishes that departed staff still hold parent text threads; the exposure exists now, not only on a future loss.
Why below the computed value	Lost device is computed at Very High likelihood for every unmanaged device holding patient information; likelihood High here because the exposure is the phones' continued, unmanaged holding rather than a loss event. Impact is not below the computed value.
Affected systems	Staff personal phones
Plausible information reach	SMS threads on the personal phones of current and former staff, and the practice Gmail mailbox through the Gmail app on the same phones; the flow record shows copier scans, intake forms and the answering service's messages arriving in that mailbox
Sensitivity	Appointment times and a child's first name in texts; whatever the recorded flows place in the mailbox (scanned forms, intake paperwork, after-hours messages); the chart itself is not on the phones
Harm to patients and the practice	Disclosure of scanned forms and messages for the patients whose documents passed through the mailbox, held by people the practice cannot reach
Clinical and operational impact	not established
Supporting evidence	Inventory Staff personal phones (office manager): SMS threads, practice email through the Gmail app, no MDM; flows (office manager): copier scans and forms to Gmail, Valley's messages to Gmail; encryption-mobile: no remote wipe; addressable-164.308(a)(3)(ii)(C): departed staff keep parent text threads
Rests on	Staff personal phones; §164.312(a)(2)(iv) (“Are phones and tablets that access patient information encrypted and …”); §164.308(a)(3)(ii)(C) (the practice's addressable determination); §164.312(e)(1) (“Is patient information ever sent by regular email or text …”)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from lost or stolen device; both are counted. What differs: Lost or stolen device rates a device leaving the practice's control by loss or theft, at the PCs' and laptops' reach. This rates threads and a signed-in mailbox kept on phones the practice never controlled, by people who have left: a different event with its own reach.
Same basis elsewhere	The recorded answer under §164.312(e)(1) (“Is patient information ever sent by regular email or text …”) also drives the rating of patient information kept by services with no agreement on record. Each analysis names the other; the exposure each rates is set out in its own basis.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Item 50.

Two retired unencrypted laptops in an unlocked closet (recorded by ePHIShield's reviewer)

Threat source: Adversarial: opportunistic theft; accidental: disposal process failure · Assessed risk: High (likelihood High, impact High)

Threat event	A retired laptop that may hold the prior record system's data leaves the practice's control unsanitized: taken from the unlocked closet by a visitor, vendor or cleaner, or discarded or given away with no wipe, since no disposal process exists.
Asset, location or flow	Retired laptops (2); Old laptops in storage closet (2)
Vulnerability	Retired, unencrypted, untracked, contents unknown, in an unlocked closet that vendors and visitors can reach; no disposal process.
Existing safeguards	Building locked after hours.
Evidence	Inventory Old laptops in storage closet (analyst observation): unlocked back storage closet; unencrypted Windows; contents unknown, possibly the prior EHR's local data or exports; disposal-process (observed): old laptops just went into the closet; server-location (observed): the closet is not secured; addressable-164.310(a)(2)(iii) (observed): parents and vendors can reach the unlocked storage closet; addressable-164.310(d)(2)(iii) (observed): no record of the closet laptops
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 5 (High), Item 38 (High), Item 39 (High), Item 51 (High), Item 55 (High), Item 56 (High)

Why it was recorded

> Retired equipment is a disposal matter, not devices to encrypt. These two laptops are the established instance of the disposal exposure; this risk gives the plan the same-day containment and the step that establishes what they hold, which the disposal threat's generic procedure does not.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Basis of the reviewer's rating

Computed starting value	Disposal or reuse of equipment and media (catalog): likelihood Very High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: no disposal process exists, the closet is unlocked and observed reachable by parents and by vendors who are left alone, the cleaning crew and landlord have access, and the laptops are on no device record, so a loss would not be noticed.

Why below the computed value	Disposal's Very High likelihood is computed for retirement of any device at a practice with no disposal process; these two laptops are already retired and still in the practice's possession, so the remaining event is their leaving the closet unsanitized. High states that; it is not lower on any established fact, and the level is the same.
Affected systems	Old laptops in storage closet (2)
Plausible information reach	Two retired unencrypted Windows laptops whose contents are not established; possibly the prior record system's data
Sensitivity	not established
Harm to patients and the practice	If they hold the prior system's data, disclosure of pre-2019 patient records in readable form
Clinical and operational impact	not established
Supporting evidence	Inventory Old laptops in storage closet (analyst observation); disposal-process and server-location (observed); addressable-164.310(a)(2)(iii) and addressable-164.310(d)(2)(iii) (observed)
Rests on	Old laptops in storage closet (2); §164.310(d)(2)(i) (“What happens to old computers, hard drives, phones, and copiers …”); §164.310(a)(1) (“Where is the server or main network equipment located, and …”); §164.310(a)(2)(iii) (the practice's addressable determination); §164.310(d)(2)(iii) (the practice's addressable determination)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Part of the same current exposure as disposal or reuse of equipment and media; counted once, there. What differs: The same current exposure: retired equipment leaving the practice's control unsanitized. These laptops are its established instance, so they are counted once, inside the disposal rating, and kept here for the same-day containment and the inspection step. The level is the same as the general threat's (High); the likelihood below it is explained above.

Safeguards that bear on it: §164.310(d)(2)(i) Disposal and §164.310(d)(1) Device and media controls.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 5; Near-term correction: Items 38, 39, 51, 55, and 56.

Lost or stolen device

Threat source: Adversarial/Environmental — theft or loss · Assessed risk: High (likelihood Very High, impact High)

Threat event	A laptop, tablet, phone, portable drive or other device holding patient information is lost or stolen.
Assets	Portable devices and media
Safeguards with a gap	§164.312(a)(2)(iv) Encryption and decryption, §164.310(d)(1) Device and media controls, §164.310(d)(2)(iii) Accountability, and §164.310(c) Workstation security
Treatment	Item 16 (Critical), Item 38 (High), Item 41 (High), Item 42 (High)

What could go wrong

> A device that stores patient information leaves the practice's control. Whether anything is disclosed depends mainly on whether its storage is encrypted and on how much patient information it holds at the time.[4]

> **What this does not mean.** A device that holds no patient information locally exposes little. Encryption greatly reduces what a lost device exposes, but only where it is turned on and configured correctly and the device is locked when lost; a password or key kept with the device, or remote access the device still has, can expose information even so. The analysis assumes none of this without a record.

The data environment

The analysis considered which devices hold patient information locally, and how much, whether the volume held is limited by a routine (such as deletion after upload) and whether that routine has been seen operating, and whether remote access is established.

Established in the record.

- §164.312(a)(2)(iv), “Are the hard drives on computers, laptops, and servers encrypted”: workstations: no; laptops: no; server: no; unencrypted devices: All office PCs; the two old laptops in the closet; physicians' personal laptops unknown; who confirmed: Kyle (believes BitLocker is not on); decision documented: no (reported by Computer helper (office manager's nephew, SYNTHETIC) by phone after the visit, plus analyst on-site observations and documents reviewed during the visit (policy binder, athena user list, athena agreement)).
- §164.312(a)(2)(iv), “Are phones and tablets that access patient information encrypted and passcode protected”: phones used: yes; encrypted: not sure; remote wipe: no; personal devices: yes (reported by Computer helper, source S-13 in Schedule H-1).
- §164.312(a)(2)(iv), the practice's addressable determination: implemented: no; documented: no (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)).
- §164.310(d)(1), “List the computers, laptops, tablets, phones, servers, and any USB drives or external disks that hold or access patient information”: list provided: no; imaging: no;

4. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

removable: no; leased: yes; unrecognized: Two old laptops in the storage closet from before athena; the copier (leased) scans to email; staff personal phones used for texting parents; the doctors' home laptops (observed by ePHIShield).

- §164.310(d)(2)(iii), “Is there a record of who has each laptop or portable device and when equipment moves between locations”: tracked: no (reported by Computer helper, source S-13 in Schedule H-1).
- §164.310(d)(2)(iii), the practice's addressable determination: implemented: no; documented: no (observed by ePHIShield).
- §164.310(c), “Can patients or visitors see any computer screens from the waiting area, check-in desk, or hallways”: visible: yes; where: Front desk PC 1 and 2 monitors face the waiting room chairs; kiosk tablet in waiting area; mitigations: no (observed by ePHIShield).
- §164.310(c), “Are workstations locked or logged off when staff step away”: policy: no; observed unlocked: yes (observed by ePHIShield).
- Still open (open item 3, Schedule H-7): Whether the physicians' personal laptops hold downloaded ePHI and are encrypted.
- Still open (open item 8, Schedule H-7): Whether staff phones are encrypted and passcode-locked, and whether departed staff still hold parent text threads.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.312(a)(2)(iv) Encryption and decryption	Not Implemented	three deficient, one reported	+1 (absent)	Encryption, correctly configured, or a reviewed equivalent alternative, keeps a lost device's contents unreadable or limits what it holds.
§164.310(d)(1) Device and media controls	Not Implemented	one deficient	+1 (absent)	Device and media controls track what leaves the facility.
§164.310(d)(2)(iii) Accountability	Not Implemented	two deficient	+1 (absent)	A movement record shows where portable equipment is.
§164.310(c) Workstation security	Not Implemented	two deficient	+1 (absent)	Physical protection of workstations makes theft harder.

Each safeguard's status is as examined in this analysis (Part E); the weight is how L.I.S.A.'s scoring counts it (Part C).

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The four safeguards weigh +1, +1, +1, +1; their average, +1, multiplied by 1.6 and rounded, moves likelihood two steps up, to Very High.

No recorded circumstance of the practice adjusts the result, so likelihood is Very High and impact stays at its starting point, High.

Not counted again: remote access is established and device encryption (§164.312(a)(2)(iv)) is not established as implemented (remote access does not by itself make a device more likely to be lost or stolen, and encryption (§164.312(a)(2)(iv)) is already a safeguard the lost-device threat weighs). The weakness is already weighed through the safeguard in the table above.

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: two retired unencrypted laptops in an unlocked closet (High); unauthorized physical access (Moderate); visible or unattended screens (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 16, 38, 41, and 42.

Once a gap is corrected, that safeguard would count as in place for this threat (and for every threat it bears on). The resulting rating is established by the next assessment, not assumed here.

Disposal or reuse of equipment and media

Threat source: Accidental — process failure · Assessed risk: High (likelihood Very High, impact High)

Threat event	Patient information is disclosed through hardware, media or leased copiers that are discarded, returned or reused without being cleared.
Assets	Retired hardware and media
Safeguards with a gap	§164.310(d)(2)(i) Disposal and §164.310(d)(2)(ii) Media re-use
Treatment	Item 39 (High), Item 40 (High), Item 5 (High), Item 38 (High), Item 51 (High), Item 55 (High), Item 56 (High)

What could go wrong

> An old computer is recycled, a leased copier with an internal drive is returned, or a laptop is handed to a new employee, still holding patient information.[5]

> **What this does not mean.** The exposure arises only when equipment leaves use or changes hands.

The data environment

The analysis considered how equipment is disposed of and how it is cleared before reuse.

5. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

Established in the record.

- §164.310(d)(2)(i), “What happens to old computers, hard drives, phones, and copiers when they are replaced or discarded”: process exists: no; written: no; method: Old laptops just went into the closet; vendor: None (observed by ePHIShield).
- §164.310(d)(2)(ii), “When a computer or phone is reassigned to another staff member, is it wiped first”: reuse happens: yes; method: New person just uses the shared login on that PC; adequate: no (reported by Computer helper, source S-13 in Schedule H-1).
- Systems and accounts the containment step names (Item 5): Old laptops in storage closet (2).
- Still open (open item 4, Schedule H-7): What the two retired closet laptops hold.
- Still open (open item 5, Schedule H-7): What credential and image cache the leased copier holds, and how its drive is handled at lease return.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.310(d)(2)(i) Disposal	Not Implemented	one deficient	+1 (absent)	Disposal procedures cover equipment leaving use.
§164.310(d)(2)(ii) Media re-use	Not Implemented	one deficient	+1 (absent)	Media re-use procedures cover equipment changing hands.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The two safeguards weigh +1, +1; their average, +1, multiplied by 1.6 and rounded, moves likelihood two steps up, to Very High.

No recorded circumstance of the practice adjusts the result, so likelihood is Very High and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: two retired unencrypted laptops in an unlocked closet (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 39, 40, 38, 51, 55, and 56; Immediate containment: Item 5.

Inappropriate access by a staff member

Threat source: Adversarial — insider · Assessed risk: High (likelihood High, impact High)

Threat event	A workforce member looks at or discloses patient records without a work reason.
Assets	EHR and clinical systems
Safeguards with a gap	§164.308(a)(3)(i) Workforce security, §164.308(a)(1)(ii)(D) Information system activity review, §164.312(a)(2)(i) Unique user identification, and §164.308(a)(1)(ii)(C) Sanction policy
Treatment	Item 9 (Critical), Item 15 (Critical), Item 27 (High), Item 28 (High), Item E2 (High)

What could go wrong

> A staff member opens the chart of a neighbor, relative, colleague or public figure out of curiosity, or discloses what they saw.[6]

> **What this does not mean.** The threat concerns access beyond a work reason, not ordinary use of records by staff who need them.

The data environment

The analysis considered whether access is limited by role, whether system activity can be attributed to individuals and is reviewed, and the size of the workforce.

Established in the record.

- §164.308(a)(3)(i), “Does anyone periodically review who has access to each system to make sure they should still have that access”: no (reported by Office manager (also billing)).
- §164.308(a)(1)(ii)(D), “Does anyone regularly look at who accessed patient records in the EHR, or at system security reports? How often, and who does it”: anyone reviews: no; what reviewed: Nobody looks at that. I didn't know athena had it (reported by Office manager (also billing)).
- §164.312(a)(2)(i), “Does every person have their own login for every system, or are any logins shared between staff”: all unique: no on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier; yes on Office manager PC, Staff personal phones, and Physicians' personal laptops; not sure on LabCorp lab interface and Old laptops in storage closet (2); any shared: no on LabCorp lab interface, Office manager PC, Staff personal phones, and Physicians' personal laptops; yes on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier; not sure on Old laptops in storage closet (2) (document read by ePHIShield: athenaOne active user list (printed during on-site visit)).

6. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.5, reviewed and approved by ePHIShield.

- §164.312(a)(2)(i), “If any logins are shared, which systems and how many people share them”: which system: Windows on front desk and exam room PCs; athenaOne kiosk login; the frontdesk@ Gmail and eFax logins; who uses: Front desk and both MAs (Windows FrontDesk account); MAs and providers (Windows Exam account); parents and front desk (kiosk tablet); why: Faster than logging in and out all day. The tablet needed to stay logged in for check-in; attributed: no (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(1)(ii)(C), “Is there a written policy describing consequences for staff who violate security or privacy rules, and have staff been told about it”: policy exists: yes; seen: yes; staff informed: no; notes: Template sanction policy is in the binder (Section 4). Not signed, no staff acknowledgments, staff interviewed on site were not aware of it (reported by Computer helper, source S-13 in Schedule H-1).
- Still open (open item 6, Schedule H-7): Whether athenaOne and Gmail keep audit logs, and for how long.
- Still open (open item 12, Schedule H-7): Whether the departed MA's athenaOne account was used after August 2025.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(3)(i) Workforce security	Partially Implemented	one deficient, one reported	−0.4 (partly in place)	Access matched to role limits what each person can see.
§164.308(a)(1)(ii)(D) Information system activity review	Not Implemented	one deficient	+1 (absent)	Regular review of activity can surface access without a reason.
§164.312(b) Audit controls	Unable to Determine	one unknown	+0.5 (not established)	Audit controls can record activity on systems holding patient information; whether a record names the individual depends on the system's sign-in and logging arrangements.
§164.312(a)(2)(i) Unique user identification	Partially Implemented	one deficient, one deficient in part	−0.4 (partly in place)	Unique identification is what lets that record be tied to a person.
§164.308(a)(1)(ii)(C) Sanction policy	Not Implemented	one deficient	+1 (absent)	Sanctions applied when the rules are broken give them consequences; a written sanction policy alone does not show they are applied.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The five safeguards weigh −0.4, +1, +0.5, −0.4, +1; their average, +0.34, multiplied by 1.6 and rounded, moves likelihood one step up, to High.

No recorded circumstance of the practice adjusts the result, so likelihood is High and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: access retained after someone leaves (High); shared sign-in without individual attribution (High); exploited unpatched or unsupported systems (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 9, 15, 27, and 28; Step to establish the facts: Item E2.

Access retained after someone leaves

Threat source: Adversarial — former insider · Assessed risk: High (likelihood Very High, impact High)

Threat event	A former workforce member still has working access to systems holding patient information.
Assets	All authenticated systems
Safeguards with a gap	§164.308(a)(3)(ii)(C) Termination procedures, §164.308(a)(4)(ii)(C) Access establishment and modification, and §164.308(a)(1)(ii)(D) Information system activity review
Treatment	Item 1 (Critical), Item 10 (Critical), Item 11 (Critical), Item 28 (High)

What could go wrong

> An account is not disabled when someone leaves, or a shared password they knew is not changed. The former employee, or someone who obtains their credentials, can still sign in.[7]

> **What this does not mean.** The risk exists only where departures occur and accounts or shared credentials survive them; the analysis reads the termination record.

The data environment

ePHIShield's reviewer (A. Reviewer (SYNTHETIC), October 21, 2026), reviewing the practice's determination under §164.308(a)(3)(ii)(C), found the alternative not adequate: SYNTHETIC REHEARSAL. The printed athenaOne user list shows the MA who left in 2025-08 still active; there is no checklist, and codes and shared passwords are not changed after departures. The reported 'EHR login removed' is contradicted by the document. Whether it is

7. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

an equivalent alternative measure: It depends on the office manager remembering, covers athena only, and has no checklist. Whether it operates as described: The printed athenaOne user list shows it did not operate for the MA who left in 2025-08 (evidence: documented).[8]

Established in the record.

- §164.308(a)(3)(ii)(C), “When someone leaves, what happens to their EHR login, email, building keys or codes, and any practice-owned device? Who does it and how quickly”: the practice's answer (ehr) is contradicted by the established answer to §164.308(a)(3)(ii)(C): “Are there any active logins belonging to people who no longer work here”; it is not counted as support.
- §164.308(a)(3)(ii)(C), “Are there any active logins belonging to people who no longer work here”: yes (document read by ePHIShield: athenaOne active user list (printed during on-site visit)).
- §164.308(a)(3)(ii)(C), the practice's addressable determination: implemented: no; documented: no (document read by ePHIShield: athenaOne active user list (printed during on-site visit)).
- §164.308(a)(4)(ii)(C), “When someone changes roles, is their access changed to match the new role, and is that recorded”: occurred: no; procedure: no (reported by Office manager (also billing)).
- §164.308(a)(4)(ii)(C), the practice's addressable determination: implemented: no; documented: no (reported by Office manager (also billing)).
- Systems and accounts the containment step names (Item 1): athenaOne.
- Still open (open item 12, Schedule H-7): Whether the departed MA's athenaOne account was used after August 2025.

Established adverse facts on §164.308(a)(1)(ii)(D) are stated under inappropriate access by a staff member.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(3)(ii)(C) Termination procedures	Not Implemented	two deficient, one contradicted, one reported	+1 (absent)	Termination procedures end access when employment ends.
§164.308(a)(4)(ii)(C) Access establishment and modification	Not Implemented	two deficient	+1 (absent)	Periodic access review catches accounts that termination missed.
§164.308(a)(1)(ii)(D) Information system activity review	Not Implemented	one deficient	+1 (absent)	Activity review can show an account used after its owner left.

Status as in Part E; weight as in Part C.

8. Engagement record. Professional review recorded under §164.308(a)(3)(ii)(C). Evidence Record, professional rulings.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, +1, +1; their average, +1, multiplied by 1.6 and rounded, moves likelihood two steps up, to Very High.

No recorded circumstance of the practice adjusts the result, so likelihood is Very High and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: inappropriate access by a staff member (High); shared sign-in without individual attribution (High); exploited unpatched or unsupported systems (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 1; Near-term correction: Items 10, 11, and 28.

Phishing and stolen email credentials

Threat source: Adversarial — external criminal actor · Assessed risk: High (likelihood Very High, impact High)

Threat event	A workforce member gives their password to a phishing message, letting an outsider into email or cloud accounts that hold patient information.
Assets	Email, cloud accounts
Safeguards with a gap	§164.308(a)(5)(i) Security awareness and training, §164.308(a)(5)(ii)(A) Security reminders, §164.312(d) Person or entity authentication, and §164.308(a)(5)(ii)(C) Log-in monitoring
Treatment	Item 17 (Critical), Item 18 (Critical), Item 29 (High), Item 30 (High), Item 31 (High), Item 70 (Medium)

What could go wrong

> A message that appears to come from a vendor, a colleague or the email provider leads a staff member to a fake sign-in page. The attacker then signs in as that person, reads mailboxes that may hold referrals, results or patient correspondence, and may send further phishing from the trusted account.[9]

> **What this does not mean.** Whether patient information is exposed depends on what the compromised account can reach; the analysis uses what the record shows about email use.

9. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.4, reviewed and approved by ePHIShield.

The data environment

The analysis considered whether patient information is sent or kept in email and whether remote access is established and how sign-in is protected.

Established in the record.

- §164.308(a)(5)(i), “Does every staff member receive security training, when does it happen, and are completion records kept”: all staff: no; when: Never formally; binder says annual; records kept: no; records seen: no; covered count: 0 (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)).
- §164.308(a)(5)(i), “Do new staff receive training before they are given access to patient information”: no (reported by Office manager (also billing)).
- §164.308(a)(5)(ii)(A), “Between trainings, does staff receive security reminders — emails, huddles, posters, newsletters”: No, not really. I'll mention things at staff meetings if something comes up (reported by Office manager (also billing)).
- §164.308(a)(5)(ii)(A), the practice's addressable determination: implemented: no; documented: no (reported by Office manager (also billing)).
- §164.312(d), “How do users prove who they are — password only, or password plus a code or app”: method: Password plus multi-factor for some systems; password only: yes (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(5)(ii)(C), “Does anyone review failed login attempts or get alerted to unusual login activity in the EHR, email, or remote access”: No. Kyle doesn't check that and I wouldn't know where to look (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(5)(ii)(C), the practice's addressable determination: implemented: no; documented: no (reported by Computer helper, source S-13 in Schedule H-1).

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(5)(i) Security awareness and training	Not Implemented	two deficient, one unknown	+1 (absent)	Training helps staff recognize the message.
§164.308(a)(5)(ii)(A) Security reminders	Not Implemented	two deficient	+1 (absent)	Reminders keep current phishing patterns in view.
§164.312(d) Person or entity authentication	Partially Implemented	one deficient in part, one reported	−0.4 (partly in place)	Authentication confirms that whoever signs in is who they claim to be. The current rule does not prescribe a method; a second sign-in factor is one stronger form, and where it is required a stolen password is usually not enough on its own. It does not stop every compromise (a relayed sign-in page or a prompt approved by mistake can still let an attacker in), and whether it is actually required at each sign-in must be established.
§164.308(a)(5)(ii)(C) Log-in monitoring	Not Implemented	two deficient	+1 (absent)	Sign-in monitoring can show an unfamiliar sign-in quickly.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood High and impact High, ePHIShield's starting points for a practice of this kind. The four safeguards weigh +1, +1, −0.4, +1; their average, +0.65, multiplied by 1.6 and rounded, moves likelihood one step up, to Very High.

No recorded circumstance of the practice adjusts the result, so likelihood is Very High and impact stays at its starting point, High.

Not counted again: remote access is established and person or entity authentication (§164.312(d)) is not established as implemented (the authentication defect is already weighed through §164.312(d), a safeguard of the phishing threat; adding a step counts it twice). The weakness is already weighed through the safeguard in the table above.

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: ransomware (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 17, 18, 29, 30, and 31; Longer-term work: Item 70.

Ransomware

Threat source: Adversarial — external criminal actor · Assessed risk: High (likelihood Very High, impact High)

Threat event	Ransomware encrypts practice systems, and possibly backups, making patient records unavailable; some variants also copy data out before encrypting.
Assets	All ePHI systems
Safeguards with a gap	§164.308(a)(5)(ii)(B) Protection from malicious software, §164.308(a)(7)(ii)(A) Data backup plan, §164.308(a)(7)(ii)(B) Disaster recovery plan, §164.312(d) Person or entity authentication, §164.308(a)(5)(i) Security awareness and training, and §164.308(a)(6)(ii) Response and reporting
Treatment	Item 12 (Critical), Item 13 (Critical), Item 17 (Critical), Item 18 (Critical), Item 29 (High), Item 32 (High), Item 33 (High), Item 34 (High), Item 35 (High), Item 36 (High), Item 37 (High), Item 46 (High)

What could go wrong

> A malicious program, usually delivered through a phishing message, a compromised remote-access account or an unpatched system, encrypts the files on the computers and servers it can reach. The practice cannot open its records until it restores from a clean backup or the files are recovered another way. Many current variants also copy data out first, which turns an availability problem into a possible disclosure.[10]

> For a practice whose record system is hosted by a vendor, the main record may be beyond the program's reach, but local files, email, scanned documents and any device that stores patient information locally are not.

> **What this does not mean.** The rating does not predict that an attack will happen; it combines how likely and how damaging one would be given the safeguards recorded. Good backups make recovery possible; they do not remove the exposure of information already copied out, or a demand for payment to keep it unpublished.

The data environment

The analysis considered where patient information is held locally rather than with a vendor and whether backups are kept separate from the systems they protect and have been restored in a test.

Established in the record.

- §164.308(a)(5)(ii)(B), “What protects the practice's computers from viruses and ransomware, and is it on every machine including any personal devices used for work”: product: Windows Defender (built-in); personal devices: no; reporting: no (reported by Computer helper, source S-13 in Schedule H-1).

10. **ePHIShield.** ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.4, reviewed and approved by ePHIShield.

- §164.308(a)(5)(ii)(B), “Does anyone receive and act on alerts from that software”: no (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(5)(ii)(B), the practice's addressable determination: implemented: no; documented: no (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(7)(ii)(A), “Does the backup include every system on the ePHI inventory, including cloud-hosted systems and imaging”: athena covers the chart. Gmail, the eFax account, and the scans on the office manager PC are not backed up by anyone that I know of (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(7)(ii)(B), “Is there a written procedure for restoring the records, and who would perform it”: written: no; seen: no; who: athena support, I guess (reported by Computer helper, source S-13 in Schedule H-1).
- §164.308(a)(6)(ii), “Is there a log of security incidents and what was done about each one”: log exists: no; outcomes recorded: no; seen: no (reported by Office manager (also billing)).
- §164.308(a)(6)(ii), “Describe the most recent security incident and how it was handled”: The misfaxed school form in 2025. The person who got it called us, said they shredded it. I re-faxed it to the right number. We didn't write anything up (reported by Office manager (also billing)).
- Still open (open item 1, Schedule H-7): Whether Windows Defender is running and current on every practice PC.
- Still open (open item 3, Schedule H-7): Whether the physicians' personal laptops hold downloaded ePHI and are encrypted.

Established adverse facts on §164.308(a)(5)(i) and §164.312(d) are stated under phishing and stolen email credentials.

Where the information is, and how it would be recovered:

- Held by vendors: Google Workspace email (Google), LabCorp lab interface (athenahealth), athenaOne (athenahealth), and eFax Corporate (eFax (Consensus Cloud Solutions)). These are the vendors' primary records. Their backup and recovery are the vendors' and are not evidenced in this record; that is not counted as a missing backup of the practice's, and it is not taken as proof that the vendors' backups are adequate.
- Stored on practice or personal equipment: Front desk PC 1, Front desk PC 2, Office manager PC, and Staff personal phones. Unless a backup of it is recorded, a copy here may be the only copy.
- Cached or working copies of records kept elsewhere: Canon multifunction copier. Their loss would not by itself lose the record; they matter for disclosure.
- Reaching records held elsewhere, with no stored copy recorded: Check-in kiosk tablet, Exam room PCs (4), and TeamViewer (personal edition).
- What these hold is not established: Old laptops in storage closet (2) and Physicians' personal laptops. A sole copy there can be neither assumed nor ruled out.
- Availability depends on Google, athenahealth, and eFax (Consensus Cloud Solutions) and on the practice's internet connection.

- Restoration: no restore has been tested, so the ability to restore is unverified; that is not an established restoration failure. No restoration failure is recorded.
- Backup coverage, as the practice described it: athena covers the chart. Gmail, the eFax account, and the scans on the office manager PC are not backed up by anyone that I know of.
- Permanent loss would follow only where information exists in one place with no backup: Front desk PC 1, Front desk PC 2, Office manager PC, and Staff personal phones, unless a backup of it is recorded; possibly Old laptops in storage closet (2) and Physicians' personal laptops, whose contents are not established.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(5)(ii)(B) Protection from malicious software	Partially Implemented	two deficient, one deficient in part	−0.4 (partly in place)	Malware protection can block or detect the program before it runs.
§164.308(a)(7)(ii)(A) Data backup plan	Not Implemented	one deficient, three unknown	+1 (absent)	Backups make it possible to restore the records without the attacker's help; they do not undo a copy taken out first.
§164.308(a)(7)(ii)(B) Disaster recovery plan	Not Implemented	one deficient, one reported	+1 (absent)	A restore procedure says how to recover; only a restore actually carried out and checked shows the backups work. A written procedure, or a written test plan, does not by itself show it.
§164.312(d) Person or entity authentication	Partially Implemented	one deficient in part, one reported	−0.4 (partly in place)	Strong authentication makes stolen passwords less useful to an attacker.
§164.308(a)(5)(i) Security awareness and training	Not Implemented	two deficient, one unknown	+1 (absent)	Training reduces the chance that staff open the message that delivers it.
§164.308(a)(6)(ii) Response and reporting	Not Implemented	two deficient	+1 (absent)	Incident response limits how far it spreads and how long recovery takes.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood High and impact Very High, ePHIShield's starting points for a practice of this kind. The six safeguards weigh −0.4, +1, +1, −0.4, +1, +1; their average, +0.53, multiplied by 1.6 and rounded, moves likelihood one step up, to Very High.

Adjusted for recorded circumstances of the practice: impact set to High (from Very High) by ePHIShield's reviewer's documented determination. Result: likelihood Very High, impact High.

Impact determination. Starting impact Very High; ePHIShield's reviewer set impact to High. SYNTHETIC REHEARSAL. Ransomware on the practice's equipment can encrypt the PCs and their local files, but not the athenaOne chart, which athenahealth holds; the chart stays available from any other device, and paper is the recorded fallback. The disclosure consequence stays: local scans and downloads, and the Gmail mailbox reached from an infected PC, can be copied out, and the office manager PC is reachable by unattended remote control. The impact is therefore one level below the starting point, not more. Affected systems and plausible reach: Front desk PCs 1 and 2, the exam room PCs and the office manager PC (Scans folder, downloaded reports) and the Gmail mailbox open on them; not the athenaOne chart, which athenahealth holds. Sensitivity of the information: School and daycare forms, shot records and referral attachments in Gmail and the Scans folder, as the inventory records. Harm to patients and the practice: Possible disclosure of the forms and scans copied out before encryption; loss of local documents not yet uploaded. Clinical and operational consequences: Front-desk and exam PCs unusable until rebuilt; the chart remains reachable in athenaOne from other devices, with paper as the recorded fallback. Evidence: Intake backup-coverage: athena covers the chart; Gmail, the eFax account and the scans on the office manager PC are not backed up; Inventory: Office manager PC holds a local Scans folder and downloaded reports; TeamViewer installed for the helper; Inventory: athenaOne is hosted by athenahealth; Intake emergency-mode: if athena was down the practice would use paper. (A. Reviewer (SYNTHETIC), October 21, 2026.)

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: phishing and stolen email credentials (High); exploited unpatched or unsupported systems (High); fire, flood, storm or power loss (Moderate); permanent data loss (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 12, 13, 17, 18, 29, 32, 33, 34, 35, 36, 37, and 46.

Shared sign-in without individual attribution on the Windows on front desk and exam room PCs; athenaOne kiosk login; the frontdesk@ Gmail and eFax logins

Threat source: Structural — control design · Assessed risk: High (likelihood Very High, impact High)

Threat event	Several people use one sign-in to reach patient information, so activity under it cannot be attributed to an individual from the system's records.
Assets	Windows on front desk and exam room PCs; athenaOne kiosk login; the frontdesk@ Gmail and eFax logins
Safeguards with a gap	§164.312(a)(2)(i) Unique user identification and §164.308(a)(1)(ii)(D) Information system activity review
Treatment	Item 15 (Critical), Item 28 (High), Item E2 (High)

What could go wrong

> When several staff use one account, whatever the system records of activity under it (viewing, changing, copying or deleting patient information) is recorded against the account, not a person. Systems do not necessarily record every kind of event, and where logging is absent or not adequately configured, an action may not be recorded at all.[11]

> Where an event is recorded, the record can show that something happened and when, but not which of the account's users did it. Establishing who acted then depends on other sources: who was working at the time, schedules, interviews. Those may settle the question or may not, especially if more than one user was present.

> **What this does not mean.** A shared sign-in does not make misuse undetectable. It removes individual attribution from whatever the system records, even where audit controls are in place and operating, which weakens accountability and makes an investigation slower and less certain. Whether an event is recorded at all depends on the system's logging, which is a separate safeguard (audit controls).

The data environment

The analysis considered which system the shared sign-in reaches and what patient information that system holds, how many people share it and where the system is, and whether the volume of information on the system is limited, and whether that limit has been seen operating.

Established in the record.

- Still open (open item 6, Schedule H-7): Whether athenaOne and Gmail keep audit logs, and for how long.

Established adverse facts on §164.308(a)(1)(ii)(D) and §164.312(a)(2)(i) are stated under inappropriate access by a staff member.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.312(a)(2)(i) Unique user identification	Partially Implemented	one deficient, one deficient in part	+1 (absent on this system)	Unique identification is the safeguard that is missing.
§164.312(b) Audit controls	Unable to Determine	one unknown	0 (no credit on this system)	Audit controls determine which activity is recorded at all. Where they operate on this system, what they record is attributed to the shared account, not the person; they do not restore individual attribution.
§164.308(a)(1)(ii)(D) Information system activity review	Not Implemented	one deficient	0 (no credit on this system)	Activity review can notice recorded events, but on this system cannot attribute them to a person, and cannot notice an event that was never recorded.

Status as in Part E; weight as in Part C. Safeguards are judged on the system where the risk exists; credit earned elsewhere in the practice does not reach it.

How the rating was reached

L.I.S.A. starts this threat at likelihood High and impact Moderate, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, 0, 0; their average, +0.33, multiplied by 1.6 and rounded, moves likelihood one step up, to Very High.

Adjusted for recorded circumstances of the practice: impact set to High (from Moderate) by ePHIShield's reviewer's documented determination. Result: likelihood Very High, impact High.

Impact determination. Starting impact Moderate; ePHIShield's reviewer set impact to High. SYNTHETIC REHEARSAL. The catalog's starting impact assumes a shared login on a workstation whose main consequence is lost attribution. Here the staff's shared accounts reach far more: the shared frontdesk@ mailbox holds school and daycare forms, shot records and Valley's after-hours messages; the shared eFax login holds every faxed referral and record the account retains; the shared FrontDesk and Exam Windows accounts keep those sessions open. Misuse through any of them reaches a large part of the patient population and cannot be traced to a person, so it cannot be investigated, sanctioned or assessed under §164.402. One level above the starting point. The waiting-room kiosk's account is rated separately (a visitor, not a workforce member) and is not counted here. Affected systems and plausible reach: The shared frontdesk@ Gmail mailbox, the shared eFax login and its retained faxes, and the shared FrontDesk and Exam Windows accounts on which those sessions stay open. Sensitivity of the information: School and daycare forms, shot records, referrals and records, and after-hours messages naming a child and the complaint, as the inventory and flow records state. Harm to patients and the practice: Access or disclosure across the whole patient population that cannot be attributed to a person, so the practice cannot investigate it,

11. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.4, reviewed and approved by ePHIShield.

apply sanctions or determine who saw what. Clinical and operational consequences: Any incident on these accounts is uninvestigable; a departure means changing every shared password at once. Evidence: Inventory Google Workspace email and eFax Corporate: shared logins; shared-account-detail (computer helper, round 2): Windows FrontDesk and Exam accounts, the frontdesk@ Gmail and eFax logins; not attributed. (A. Reviewer (SYNTHETIC), October 21, 2026.)

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: inappropriate access by a staff member (High); access retained after someone leaves (High); exploited unpatched or unsupported systems (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 15 and 28; Step to establish the facts: Item E2.

Interception or misdirection in transit

Threat source: Adversarial/Accidental · Assessed risk: High (likelihood High, impact High)

Threat event	Patient information is intercepted or sent to the wrong recipient while being transmitted electronically.
Assets	Email, interfaces, remote connections
Safeguards with a gap	§164.312(e)(1) Transmission security, §164.312(e)(2)(ii) Encryption, and §164.312(e)(2)(i) Integrity controls
Treatment	Item 43 (High), Item 45 (High)

What could go wrong

> A result is emailed unencrypted, a fax-to-email message is misaddressed, or an interface sends data over an unprotected connection.[12]

> **What this does not mean.** Sending patient information by email or another electronic channel is not by itself a violation or a vulnerability. The concern is transmission without protection adequate to the circumstances, such as unencrypted email to an outside recipient where encryption is reasonable and appropriate. The analysis follows the transmission paths the practice described; it does not assume paths that were not recorded.

12. **ePHIShield.** ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.4, reviewed and approved by ePHIShield.

The data environment

The analysis considered how patient information is sent outside the practice.

Established in the record.

- §164.312(e)(1), “Is patient information ever sent by regular email or text message”: ephi by email: yes; to whom: Parents (school/daycare forms, shot records), sometimes referral offices; texting staff: yes; email service: Gmail (Google Workspace); encrypted transit: not sure (reported by Office manager (also billing)).
- §164.312(e)(2)(ii), “Are the connections used to reach the EHR, email, and any remote access encrypted”: encrypted paths: athena in the browser (https); Gmail between Google servers; TeamViewer; unencrypted paths: Text messages from personal phones; Gmail to parents whose email provider may not support TLS; fax leg to recipient (reported by Computer helper, source S-13 in Schedule H-1).
- §164.312(e)(2)(ii), the practice's addressable determination: implemented: no; documented: no (reported by Computer helper, source S-13 in Schedule H-1).
- §164.312(e)(2)(i), the practice's addressable determination: implemented: no; documented: no (reported by Computer helper, source S-13 in Schedule H-1).
- Still open (open item 7, Schedule H-7): The facts of the 2025 misdirected fax needed for the breach assessment.
- Still open (open item 11, Schedule H-7): How staff confirm a number or address belongs to the child's parent or guardian before texting or emailing.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.312(e)(1) Transmission security	Not Implemented	one deficient, one reported	+1 (absent)	Transmission security protects information on the network.
§164.312(e)(2)(ii) Encryption	Partially Implemented	one deficient, one deficient in part, one observed	−0.4 (partly in place)	Encryption in transit keeps intercepted data unreadable.
§164.312(e)(2)(i) Integrity controls	Not Implemented	one deficient, one unknown	+1 (absent)	Integrity controls detect alteration in transit.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, −0.4, +1; their average, +0.53, multiplied by 1.6 and rounded, moves likelihood one step up, to High.

No recorded circumstance of the practice adjusts the result, so likelihood is High and impact stays at its starting point, High.

Incident history. Spring 2025: a school form was faxed to a wrong number, one digit off; the business that received it called and said it was shredded; the form was re-faxed to the right number and nothing was written up. Computed likelihood High; the reviewer's level (High) was not applied: the computed likelihood is already at or above it. (A. Reviewer (SYNTHETIC), October 21, 2026.)

In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 43 and 45.

Exploited unpatched or unsupported systems

Threat source: Adversarial — external · Assessed risk: High (likelihood High, impact High)

Threat event	An unpatched or unsupported system is exploited to gain access to the practice's network.
Assets	Servers, workstations, network devices
Safeguards with a gap	§164.308(a)(1)(ii)(D) Information system activity review, §164.308(a)(5)(ii)(B) Protection from malicious software, and §164.312(a)(1) Access control
Treatment	Item 12 (Critical), Item 13 (Critical), Item 14 (Critical), Item 28 (High), Item 46 (High), Item 63 (High), Item 71 (Medium), Item 48 (High)

What could go wrong

> A known weakness in an operating system, application or network device that has not been updated is used to get in.[13]

> **What this does not mean.** Current law does not name patching as a specification; the safeguards credited are those the Rule does name. Those three safeguards (activity review, malware protection and access control) do not by themselves establish that systems are patched or supported; ePHIShield's reviewer considers the recorded patching condition separately (Part F).

The data environment

The analysis considered whether systems are kept updated and protected.

Established in the record.

- §164.312(a)(1), “For each system on the inventory, does each user have their own individual account, is an account shared, or is no login required”: role based: yes; who

13. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.4, reviewed and approved by ePHIShield.

admins: Office manager (athena); Kyle (Windows); admin accounts: Office manager in athena; Kyle and the shared Windows accounts are local admins on the PCs; vendor controlled: yes (document read by ePHIShield: athenaOne active user list (printed during on-site visit)).

- Still open (open item 1, Schedule H-7): Whether Windows Defender is running and current on every practice PC.
- Still open (open item 2, Schedule H-7): The patch state of the PCs other than the Windows 10 front-desk PC, and of the gateway.

Established adverse facts on §164.308(a)(1)(ii)(D) are stated under inappropriate access by a staff member; §164.308(a)(5)(ii)(B) are stated under ransomware.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(1)(ii)(D) Information system activity review	Not Implemented	one deficient	+1 (absent)	Activity review can reveal an intrusion.
§164.308(a)(5)(ii)(B) Protection from malicious software	Partially Implemented	two deficient, one deficient in part	−0.4 (partly in place)	Malware protection can block what an exploit delivers.
§164.312(a)(1) Access control	Partially Implemented	one deficient in part	−0.4 (partly in place)	Access control limits what an intruder can reach.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood High and impact High, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, −0.4, −0.4; their average, +0.07, multiplied by 1.6 and rounded, moves likelihood by no steps, leaving it at High.

No recorded circumstance of the practice adjusts the result, so likelihood is High and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact High gives a level of risk of High.

Related risks

The same safeguard gaps also bear on: inappropriate access by a staff member (High); access retained after someone leaves (High); ransomware (High); shared sign-in without individual attribution (High). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 12, 13, 14, 28, 46, 63, and 48; Longer-term work: Item 71.

> **Evidence-verification follow-up.** One follow-up for this threat establishes whether what the rating credits only in part, or could not assess, is in place. They are not corrective actions; the practice owns them, and each is listed once, with its responsible person and timeframe, in Part G (evidence-verification follow-up).

Shared physical and network secrets never changed (recorded by ePHIShield's reviewer)

Threat source: Adversarial: former insider or opportunistic outsider · Assessed risk: Moderate (likelihood Moderate, impact High)

Threat event	A former employee, a cleaning-crew member or a visitor who knows the alarm code, the posted Wi-Fi password or the gateway's default admin password enters after hours or joins the network that carries the practice PCs; the copier's stored Gmail app password gives mailbox access to whoever reaches the copier's settings.
Asset, location or flow	Alarm code, Wi-Fi, gateway and copier credentials; Comcast Business gateway and Wi-Fi
Vulnerability	One alarm code known to all staff, the cleaning crew and the landlord, never changed after departures; Wi-Fi password written on the break-room whiteboard; gateway admin password believed default with the guest network on the same LAN; a shared Windows password on a sticky note at the front desk; a Gmail app password stored in a walk-up copier with no PIN.
Existing safeguards	Doors locked and alarm armed after hours (observed).
Evidence	facility-access (observed): all staff, the cleaning crew and the landlord have access; all staff know the alarm code; addressable-164.310(a)(2)(ii) (observed): alarm code shared by everyone and never changed; addressable-164.308(a)(3)(ii)(C) (office manager, round 2): shared Windows passwords and the alarm code not changed after departures; wifi-security (observed): Wi-Fi password written on the break-room whiteboard; password-practices (observed): one password on a sticky note at the front desk; Inventory gateway (helper; analyst): default admin password believed unchanged; guest SSID on same LAN; Inventory copier (computer helper): stored Gmail app password; walk-up, no PIN
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 7 (High), Item 52 (High), Item 53 (High), Item 55 (High), Item 56 (High), Item 61 (High), Item 72 (Medium)

Why it was recorded

> Shared secrets that survive departures are not rated by the catalog's shared-sign-in or departed-staff threats, which concern system accounts.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact High gives a level of risk of Moderate.

Basis of the reviewer's rating

Computed starting value	Unauthorized physical access (catalog): likelihood Moderate, impact High, level Moderate, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. Moderate: the alarm code, the posted Wi-Fi password, the default gateway password and the copier's stored Gmail app password are known to or reachable by former staff, the cleaning crew, the landlord and visitors, and none was changed after departures; using them needs a person who intends to, and no such use is recorded.
Affected systems	Comcast Business gateway and Wi-Fi, Canon multifunction copier, and Google Workspace email
Plausible information reach	The premises after hours, the network the practice PCs use, the gateway's settings, and the Gmail mailbox through the copier's app password
Sensitivity	Forms, shot records and after-hours messages in Gmail; the PCs' local files
Harm to patients and the practice	Undetected entry or network access by people who should no longer have it, and mailbox access without a password prompt
Clinical and operational impact	Codes and passwords must be changed for everyone at once
Supporting evidence	facility-access and addressable-164.310(a)(2)(ii) (observed): alarm code known to all and never changed; wifi-security and password-practices (observed); inventory gateway and copier
Rests on	§164.310(a)(1) (“Who can get into the office outside of business hours …”); §164.310(a)(2)(ii) (the practice's addressable determination); §164.308(a)(5)(ii)(D) (“What are the practice's rules for passwords — length, reuse …”); Comcast Business gateway and Wi-Fi; Canon multifunction copier
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from unauthorized physical access; both are counted. What differs: Unauthorized physical access rates people reaching workstations or equipment on the premises. These secrets also open the network, the gateway's settings and the Gmail mailbox, and they stay valid for people who have left, which the physical-access safeguards do not weigh.

Safeguards that bear on it: §164.310(a)(1) Facility access controls, §164.310(a)(2)(ii) Facility security plan, and §164.308(a)(5)(ii)(D) Password management.

Established in the record.

- §164.308(a)(5)(ii)(D), “What are the practice's rules for passwords — length, reuse across systems, sharing, and how they are stored or remembered”: rules: athena makes you use a strong password and change it. Windows passwords are simple and haven't been changed in years; reuse: yes; shared: yes; storage: Written down / memorized; one on a sticky note at the front desk (observed by ePHIShield).
- §164.308(a)(5)(ii)(D), “Do any staff share passwords or write them where others can see them”: yes (observed by ePHIShield).
- Systems and accounts the containment step names (Item 7): Comcast Business gateway and Wi-Fi.

- Still open (open item 5, Schedule H-7): What credential and image cache the leased copier holds, and how its drive is handled at lease return.

Established adverse facts on §164.310(a)(1) and §164.310(a)(2)(ii) are stated under unauthorized physical access.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 7; Near-term correction: Items 52, 53, 55, 56, and 61; Longer-term work: Item 72.

Patient information kept by services with no agreement on record (recorded by ePHIShield's reviewer)

Threat source: Adversarial or accidental: third party · Assessed risk: Moderate (likelihood Moderate, impact High)

Threat event	A service that receives and keeps the practice's patient information every day uses, keeps or discloses it outside the practice's control, or has a security incident it is not obliged to report, so the practice never learns of it and cannot assess or notify.
Asset, location or flow	School and daycare forms, shot records, faxed records and after-hours messages held by Google, eFax and Valley After-Hours Answering; Google Workspace email
Vulnerability	Google's Workspace BAA was not accepted in the admin console; no eFax or Valley agreement was produced when requested on site, and whether one exists is not established. Without an agreement nothing obliges the service to limit its use of the information or to report an incident to the practice.
Existing safeguards	The services' own commercial terms and security, which were not assessed.
Evidence	Vendor record, Google (computer helper, round 2): BAA not accepted in the admin console; ba-agreements (round 2; agreement read on site): only the athenahealth agreement could be produced; the practice says not all are signed; Flows (office manager): copier scans and forms to Gmail; Valley's after-hours messages by email to Gmail; referrals and records by eFax, retained in the eFax web account
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 2 (Critical), Item 24 (Critical)

Why it was recorded

> The missing agreements are compliance findings with their own corrective step; this records what the analysis must still weigh: the information is already held by these services every day, under no obligation to the practice. Whether any of it has been misused is not established.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact High gives a level of risk of Moderate.

Basis of the reviewer's rating

Computed starting value	Vendor compromise (catalog): likelihood Moderate, impact High, level Moderate, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. Moderate: the information reaches these services every day (copier scans and forms in Gmail, Valley's messages by email, faxes kept in the eFax account); they are established commercial services, and no misuse or incident is recorded, but none is obliged to tell the practice of one.
Affected systems	Google Workspace email and eFax Corporate
Plausible information reach	The Google Workspace mailbox, the eFax web account's retained faxes, and Valley's after-hours call messages
Sensitivity	School and daycare forms, shot records, referrals and records, and messages naming a child and the complaint
Harm to patients and the practice	Disclosure the practice never learns of, so no assessment or notice
Clinical and operational impact	not established
Supporting evidence	Vendor record Google (BAA not accepted); ba-agreements (only athenahealth's agreement produced); recorded flows into Gmail and eFax
Rests on	§164.308(b)(1) (“Is there a signed business associate agreement with each of …”); Google Workspace email; eFax Corporate; §164.312(e)(1) (“Is patient information ever sent by regular email or text …”)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Part of the same current exposure as vendor compromise; counted once, there. What differs: Vendor compromise covers a business associate that is compromised or handles the practice's information without adequate assurances; this is the second part of that threat, made explicit because the agreements do not move that rating. Counted once, inside it, at the same level.
Same basis elsewhere	The recorded answer under §164.312(e)(1) (“Is patient information ever sent by regular email or text …”) also drives the rating of texts and the practice Gmail app on unmanaged personal phones. Each analysis names the other; the exposure each rates is set out in its own basis.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 2; Near-term correction: Item 24.

Fire, flood, storm or power loss

Threat source: Environmental · Assessed risk: Moderate (likelihood Moderate, impact High)

Threat event	Fire, flood, storm or extended power loss damages systems and interrupts access to patient records.
Assets	On-premises infrastructure
Safeguards with a gap	§164.308(a)(7)(ii)(A) Data backup plan, §164.308(a)(7)(ii)(C) Emergency mode operation plan, and §164.310(a)(2)(i) Contingency operations
Treatment	Item 33 (High), Item 34 (High), Item 35 (High), Item 54 (High), Item 77 (Low)

What could go wrong

> The office is damaged or without power for days. Local equipment may be destroyed. Vendor-hosted systems are not damaged with the office, but they must be reached from somewhere else, and a wider event (a regional storm, a power or internet outage, or an outage at the vendor) can make them unavailable too.[14]

> **What this does not mean.** Where patient information is held only with vendors, damage to the office affects access more than the records themselves; the analysis does not assume a vendor stays available in a wider outage.

The data environment

The analysis considered whether patient information is held on site and whether there is a plan for operating and restoring access.

Established in the record.

- §164.308(a)(7)(ii)(C), “If systems were down for several days, how would the practice keep seeing patients and still protect patient information”: If athena was down we'd use paper and enter it later. If the internet is out we'd have to reschedule people. We've never had it go down for more than an hour or two (reported by Office manager (also billing)).
- §164.310(a)(2)(i), “In an after-hours emergency, who can get into the building and to the equipment to restore systems”: who: Me or either doctor; we all have keys; documented: no (reported by Office manager (also billing)).
- §164.310(a)(2)(i), the practice's addressable determination: implemented: no; documented: no (observed by ePHIShield).

Established adverse facts on §164.308(a)(7)(ii)(A) are stated under ransomware.

14. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(7)(i) Contingency plan	Not Implemented (weighed as such here: §164.308(a)(7)(ii)(A), §164.308(a)(7)(ii)(B), §164.308(a)(7)(ii)(C) beneath it bears on this threat)	one unknown	+1 (absent)	A contingency plan prepares the response.
§164.308(a)(7)(ii)(A) Data backup plan	Not Implemented	one deficient, three unknown	+1 (absent)	Backups preserve the data.
§164.308(a)(7)(ii)(C) Emergency mode operation plan	Not Implemented	one deficient	+1 (absent)	An emergency-mode plan keeps critical work going safely.
§164.310(a)(2)(i) Contingency operations	Partially Implemented	one deficient, one deficient in part	−0.4 (partly in place)	Contingency operations let the right people into the facility.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Low and impact High, ePHIShield's starting points for a practice of this kind. The four safeguards weigh +1, +1, +1, −0.4; their average, +0.65, multiplied by 1.6 and rounded, moves likelihood one step up, to Moderate.

No recorded circumstance of the practice adjusts the result, so likelihood is Moderate and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact High gives a level of risk of Moderate.

Related risks

The same safeguard gaps also bear on: ransomware (High); permanent data loss (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 33, 34, 35, and 54; Longer-term work: Item 77.

Unauthorized physical access

Threat source: Adversarial — external or unescorted visitor · Assessed risk: Moderate (likelihood Moderate, impact High)

Threat event	Someone without authorization gets physical access to workstations or equipment holding patient information.
Assets	Facility, workstations, servers
Safeguards with a gap	§164.310(a)(1) Facility access controls, §164.310(a)(2)(ii) Facility security plan, §164.310(a)(2)(iii) Access control and validation procedures, and §164.310(c) Workstation security
Treatment	Item 55 (High), Item 56 (High), Item 58 (High), Item 72 (Medium), Item 73 (Medium)

What could go wrong

> A visitor, contractor or intruder reaches a workstation, server or network closet, and uses, removes or tampers with it.[15]

> **What this does not mean.** Physical access is a path to a device; what it exposes depends on what the device holds and how it is signed in to.

The data environment

The analysis considered where equipment holding patient information is located and how it is secured.

Established in the record.

- §164.310(a)(1), “Who can get into the office outside of business hours, and how — keys, codes, badges? Is there a record of who holds each”: secured after hours: yes; who has access: Both doctors, me, the NP, the cleaning crew, and the landlord. All staff know the alarm code; observed: yes (observed by ePHIShield).
- §164.310(a)(1), “Where is the server or main network equipment located, and is that space locked”: has onsite equipment: yes; where: Comcast gateway on a shelf in the back storage closet; room secured: no; observed: yes (observed by ePHIShield).
- §164.310(a)(2)(ii), the practice's addressable determination: implemented: no; documented: no (observed by ePHIShield).
- §164.310(a)(2)(iii), “How are visitors, vendors, and repair technicians handled — signed in, escorted, left alone with equipment”: identified: no; logged: no; escorted: no; vendors: no (reported by Office manager (also billing)).
- §164.310(a)(2)(iii), the practice's addressable determination: implemented: no; documented: no (observed by ePHIShield).

Established adverse facts on §164.310(c) are stated under lost or stolen device.

15. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.310(a)(1) Facility access controls	Partially Implemented	one deficient, one deficient in part	−0.4 (partly in place)	Facility access controls limit who can enter.
§164.310(a)(2)(ii) Facility security plan	Partially Implemented	one deficient, one observed	−0.4 (partly in place)	A facility security plan addresses tampering and theft.
§164.310(a)(2)(iii) Access control and validation procedures	Not Implemented	two deficient	+1 (absent)	Visitor and technician control covers people who are not staff.
§164.310(c) Workstation security	Not Implemented	two deficient	+1 (absent)	Workstation security protects the devices themselves.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The four safeguards weigh −0.4, −0.4, +1, +1; their average, +0.3, multiplied by 1.6 and rounded, moves likelihood by no steps, leaving it at Moderate.

No recorded circumstance of the practice adjusts the result, so likelihood is Moderate and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact High gives a level of risk of Moderate.

Related risks

The same safeguard gaps also bear on: lost or stolen device (High); shared physical and network secrets never changed (Moderate); visible or unattended screens (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 55, 56, and 58; Longer-term work: Items 72 and 73.

Vendor compromise

Threat source: Adversarial — third party · Assessed risk: Moderate (likelihood Moderate, impact High)

Threat event	A vendor that handles the practice's patient information, or can reach it, is compromised, and the information is exposed.
Assets	Vendor-held ePHI
Safeguards with a gap	§164.308(b)(1) Business associate contracts and other arrangements, §164.308(b)(3) Written contract or other arrangement, §164.314(a)(1) Business associate contracts or other arrangements, and §164.314(a)(2)(i) Business associate contracts
Treatment	Item 20 (Critical), Item 21 (Critical), Item 22 (Critical), Item 23 (Critical), Item 2 (Critical), Item 24 (Critical)

What could go wrong

> A billing service, IT provider or software vendor suffers a breach, and the practice's information it holds or can reach is exposed.[16]

> Whether each vendor has the required business associate agreement is a separate question. It is assessed under the agreement requirements, and a missing or deficient agreement is reported as a finding with its own corrective step; it is not what this rating measures.

> **What this does not mean.** A business associate agreement is a contractual assurance: it obliges the vendor to safeguard the information and report incidents, and gives the practice recourse; a missing or deficient agreement is a contractual deficiency. Neither shows how secure the vendor's own systems are, so the agreements do not move this rating. Holding a vendor's audit report, certification or questionnaire does not move it either: it moves only where ePHIShield's reviewer assessed that evidence (its relevance to the service, its period, its scope and coverage, and its findings and exceptions) and concluded that it supports the protection. What is expected of a vendor is proportionate to the vendor.

The data environment

The analysis considered which vendors create, receive, maintain or transmit the practice's patient information, or have access that can reach it, and whether each has an executed agreement and what evidence about each such vendor's security was recorded, and what ePHIShield's reviewer concluded from it.

Established in the record.

- Agreement with Google: established deficient under §164.308(b)(1), §164.308(b)(3), §164.314(a)(1), and §164.314(a)(2)(i) (Part E).
- Agreement with Tri-State Office Systems (SYNTHETIC): established deficient under §164.308(b)(1), §164.308(b)(3), §164.314(a)(1), and §164.314(a)(2)(i) (Part E).
- Agreement with Kyle Pruitt (SYNTHETIC), independent computer helper: established deficient under §164.308(b)(1), §164.308(b)(3), §164.314(a)(1), and §164.314(a)(2)(i) (Part E).

16. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.5, reviewed and approved by ePHIShield.

- Systems and accounts the containment step names (Item 2): Google Workspace email.
- Still open (open item 9, Schedule H-7): Whether an agreement exists with eFax and with Valley After-Hours Answering (none was produced when requested on site).

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(b)(1) Business associate contracts and other arrangements	Partially Implemented	three deficient, one documented, two not provided	Not weighted (contractual)	Business associate agreements obtain the vendor's written assurances; they are assessed as contractual assurances and do not show the vendor's security.
§164.308(b)(3) Written contract or other arrangement	Partially Implemented	three deficient, one documented, two not provided	Not weighted (contractual)	The assurances must be written and executed.
§164.314(a)(1) Business associate contracts or other arrangements	Partially Implemented	three deficient, one documented, two not provided	Not weighted (contractual)	The agreements must contain the required terms.
§164.314(a)(2)(i) Business associate contracts	Partially Implemented	three deficient, one documented, two not provided	Not weighted (contractual)	Including incident and breach reporting.

Status as in Part E; weight as in Part C.

Contractual assurance and compromise exposure

The business associate agreements above are contractual assurances: they oblige each vendor and give the practice recourse, and any deficiency is a finding with its own corrective step. Their presence or absence is not evidence of how likely a vendor's own systems are to be compromised, so they do not move this rating. The rating moves only on what ePHIShield's reviewer concluded about each in-scope vendor's own security, from evidence assessed for its relevance, period, scope and exceptions. Holding a report earns nothing by itself.

Vendor	Reach to ePHI	Security evidence	Reviewer's conclusion	Weight
athenahealth (material)	creates, receives, maintains or transmits ePHI	None	Not assessed	0
Google	creates, receives, maintains or transmits ePHI	None	Not assessed	0
eFax (Consensus Cloud Solutions)	creates, receives, maintains or transmits ePHI	None	Not assessed	0
Tri-State Office Systems (SYNTHETIC)	has access capable of reaching ePHI	None	Not assessed	0
Valley After-Hours Answering (SYNTHETIC)	creates, receives, maintains or transmits ePHI	None	Not assessed	0
Kyle Pruitt (SYNTHETIC), independent computer helper	has access capable of reaching ePHI	None	Not assessed	0

In-scope vendors: business associates that handle the practice's ePHI or have access capable of reaching it, and any vendor whose access is not established. Supports −1, partly supports −0.4; does not support, or not assessed, 0 (no credit, no penalty). A material vendor hosts the main record system or was marked material by ePHIShield's reviewer. Vendor assurance lowers the likelihood by one step at most, and not at all while a material vendor is not assessed as supporting the protective conclusion.

Outside this rating, with the recorded reason: LabCorp (another provider, not a business associate); Comcast Business (a conduit, not a business associate); State immunization registry (not a business associate); Referral offices (another provider, not a business associate).

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact High, ePHIShield's starting points for a practice of this kind. The assurance concluded for the six in-scope vendors weighs 0, 0, 0, 0, 0, 0; their average, 0, multiplied by 1.6 and rounded, moves likelihood by no steps, leaving it at Moderate.

No recorded circumstance of the practice adjusts the result, so likelihood is Moderate and impact stays at its starting point, High.

In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact High gives a level of risk of Moderate.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 20, 21, 22, 23, and 24; Immediate containment: Item 2.

Item 20, Item 21, Item 22, and Item 23 concern the business associate agreements, a compliance requirement. They are listed with this threat because the agreements are among its safeguards, but they do not by themselves change this rating, which rests on ePHIShield's assessment of each vendor's own security evidence.

> **Evidence-verification follow-up.** Six follow-ups for this threat establish whether what the rating credits only in part, or could not assess, is in place. Listed once in Part G.

Misdirected fax never assessed; no working incident procedure (recorded by ePHIShield's reviewer)

Threat source: Non-adversarial: workforce error · Assessed risk: Moderate (likelihood High, impact Moderate)

Threat event	A misdirected fax or email is handled informally, so a reportable breach goes unassessed and unreported.
Asset, location or flow	Incident handling; eFax Corporate
Vulnerability	The binder's incident procedure is an uncustomized template with no names or contacts, and no one is named to decide whether an event is a breach; the 2025 misfax was not recorded or assessed. (The misdirection itself is rated under interception or misdirection in transit.)
Existing safeguards	Staff re-faxed to the correct number; the recipient said the form was shredded.
Evidence	Intake prior-incidents (office manager): one misdirected fax in spring 2025; Intake incident-detail (office manager): misfax handled informally, nothing written up; Policy binder (template, 2017): reviewed on site and rejected as not adopted
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 6 (High), Item 60 (High), Item 64 (High), Item 65 (High), Item 66 (High), Item 67 (High), Item 68 (High)

Why it was recorded

> An incident that already happened was never assessed under the breach notification rule; the template procedure is not a working one.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact Moderate gives a level of risk of Moderate.

Basis of the reviewer's rating

Computed starting value	Interception or misdirection in transit (catalog): likelihood High, impact High, level High, as L.I.S.A. computed it when the basis was recorded
Why this likelihood	SYNTHETIC REHEARSAL. High: the failure has already happened once (the spring 2025 misfax was handled informally and never assessed), nothing has changed since, and the only written procedure is an unadopted template that names no one.
Why below the computed value	Interception in transit is computed at High impact for the practice's electronic paths as a whole; a misdirected fax discloses one or a few patients' records to one wrong recipient, so impact Moderate. Likelihood stays High because it has already happened.
Affected systems	eFax Corporate and practice-wide

Plausible information reach	Every misdirected or disclosed record, on any channel, that goes unrecorded and unassessed; now, the 2025 school form
Sensitivity	A school form naming a child, faxed to a business, as the office manager describes it
Harm to patients and the practice	Individuals not notified of a breach that is owed; the practice out of compliance with the breach notification rule
Clinical and operational impact	The breach assessment, any notices and an incident procedure must now be done after the fact
Supporting evidence	Intake prior-incidents and incident-detail (office manager, round 1): the spring 2025 misfax, re-faxed and not written up; the binder's incident procedure rejected as not adopted
Rests on	§164.308(a)(6)(ii) (“Describe the most recent security incident and how it was …”); §164.308(a)(1)(ii)(A) (“Has the practice experienced any lost or stolen device, ransomware …”); eFax Corporate
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026
Relation to the catalog	Distinct from interception or misdirection in transit; both are counted. Why the ratings differ (High there, Moderate here): A different threat. Interception or misdirection in transit rates the disclosure itself (a fax, text or email reaching the wrong party), and the 2025 misfax raised its likelihood to High. This risk rates what happens after: a misdirection goes unrecorded, unassessed under §164.402 and unnotified. Its consequence is the failure of breach response, so the two are counted separately and the incident is not counted twice.

Established in the record.

- §164.308(a)(1)(ii)(A), “Has the practice ever had a security risk analysis performed, and if so when and by whom”: ever: no; seen: no; notes: We have the HIPAA binder but nobody has ever come in and done an assessment (reported by Office manager (also billing)).
- Systems and accounts the containment step names (Item 6): eFax Corporate.
- Still open (open item 7, Schedule H-7): The facts of the 2025 misdirected fax needed for the breach assessment.

Treatment

Each step is set out in full once, in Part G (priorities above). Immediate containment: Item 6; Near-term correction: Items 60, 64, 65, 66, 67, and 68.

Policy binder states controls that do not exist (recorded by ePHIShield's reviewer)

Threat source: Non-adversarial: reliance on inaccurate documentation · Assessed risk: Moderate (likelihood Moderate, impact Moderate)

Threat event	Staff or the practice rely on the binder's statements, for example that all ePHI is encrypted, and wrongly treat a lost device or emailed record as secured, so a notifiable breach is not assessed or reported.
Asset, location or flow	HIPAA policy binder (template, 2017)

Vulnerability	The uncustomized 2017 template states annual training (none has been given), that all ePHI is encrypted (nothing is), and leaves the security-official designation blank; staff are unaware of its policies.
Existing safeguards	None.
Evidence	training-program (binder read by ePHIShield on site; staff interviewed on site): never formally trained, although the binder says annual; addressable-164.312(a)(2)(iv) (binder read by ePHIShield on site; computer helper): the binder says all ePHI is encrypted, but nothing was set up; security-official (binder read by ePHIShield on site): the designation page is an unfilled placeholder; Evidence rulings: the binder's sanction, incident and workstation-use policies rejected as not adopted
Recorded by	A. Reviewer (SYNTHETIC), October 21, 2026
Treatment	Item 75 (Medium)

Why it was recorded

> Documentation that affirmatively misstates practice is outside the catalog, and the binder is the only written policy the practice has.

The likelihood and impact are the reviewer's judgment (basis below). In NIST SP 800-30 Table I-2 (Part C), likelihood Moderate with impact Moderate gives a level of risk of Moderate.

Basis of the reviewer's rating

Computed starting value	None: a risk identified by the reviewer outside the catalog has no computed starting value
Why this likelihood	SYNTHETIC REHEARSAL. Moderate: the binder is the only written policy and states annual training, full encryption and a designated official, none of which exists; staff do not use it, so reliance on it arises mainly when someone consults it after an event.
Affected systems	practice-wide
Plausible information reach	practice-wide: every decision made from the binder, chiefly whether a lost device or emailed record was secured
Sensitivity	not established
Harm to patients and the practice	A lost unencrypted device or misdirected record treated as secured, so a breach goes unassessed
Clinical and operational impact	Policies must be rewritten to describe actual practice
Supporting evidence	training-program and security-official (binder read by ePHIShield on site); addressable-164.312(a)(2)(iv) (binder states all ePHI is encrypted)
Rests on	§164.308(a)(5)(i) (“Does every staff member receive security training, when does it …”); §164.308(a)(2) (“Who is the person formally responsible for HIPAA security at …”); §164.312(a)(2)(iv) (the practice's addressable determination)
Reviewer	A. Reviewer (SYNTHETIC), October 21, 2026

Established in the record.

- §164.308(a)(2), “Who is the person formally responsible for HIPAA security at the practice, and is that assignment in writing”: name: Me (office manager); in writing: no; seen: no (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)).

Treatment

Each step is set out in full once, in Part G (priorities above). Longer-term work: Item 75.

Permanent data loss

Threat source: Structural/Accidental · Assessed risk: Moderate (likelihood High, impact Moderate)

Threat event	Hardware failure or accidental deletion permanently destroys patient records.
Assets	Primary record systems
Safeguards with a gap	§164.308(a)(7)(ii)(A) Data backup plan, §164.308(a)(7)(ii)(B) Disaster recovery plan, and §164.312(c)(1) Integrity
Treatment	Item 34 (High), Item 35 (High), Item 36 (High), Item 37 (High), Item 74 (Medium)

What could go wrong

> A drive fails, a file is deleted, or a device holding records that exist nowhere else stops working.[17]

> **What this does not mean.** Loss is permanent only where no retrievable copy exists. Documented backups show that copies are being made and kept; a restore that was carried out and checked demonstrates that the practice can actually recover from them. A written backup procedure or test plan, without that, documents the arrangement but does not demonstrate restoration capability.

The data environment

The analysis considered whether every place patient information is held is covered by backups.

Established in the record.

- §164.312(c)(1), “What prevents patient records from being changed or deleted improperly — permissions, amendment tracking, or version history”: protection: athena keeps a history of chart changes and signed notes can only be amended, not deleted; ehr native: yes (reported by Computer helper, source S-13 in Schedule H-1).
- Still open (open item 4, Schedule H-7): What the two retired closet laptops hold.

17. ePHIShield. ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.5, reviewed and approved by ePHIShield.

Established adverse facts on §164.308(a)(7)(ii)(A) and §164.308(a)(7)(ii)(B) are stated under ransomware.

Where the information is, and how it would be recovered, is set out under ransomware; it is the same for this threat.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.308(a)(7)(ii)(A) Data backup plan	Not Implemented	one deficient, three unknown	+1 (absent)	Backups keep retrievable copies.
§164.308(a)(7)(ii)(B) Disaster recovery plan	Not Implemented	one deficient, one reported	+1 (absent)	A documented restore procedure says how to recover them; only a restore that was carried out and checked shows that recovery works.
§164.312(c)(1) Integrity	Partially Implemented	one deficient in part	−0.4 (partly in place)	Integrity controls limit improper deletion.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood Moderate and impact Very High, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, +1, −0.4; their average, +0.53, multiplied by 1.6 and rounded, moves likelihood one step up, to High.

Adjusted for recorded circumstances of the practice: impact set to Moderate (from Very High) by ePHIShield's reviewer's documented determination. Result: likelihood High, impact Moderate.

Impact determination. Starting impact Very High; ePHIShield's reviewer set impact to Moderate. SYNTHETIC REHEARSAL. Permanent loss of the patient chart is not plausible from the practice's side: athenahealth holds it in athenaOne. What exists in one place with no backup is the office manager PC's Scans folder of documents awaiting upload, downloads on the front-desk PCs, and appointment text threads on staff personal phones. What the two retired laptops in the storage closet hold is not established; the closet-laptop risk's plan step has them inspected offline and their contents recorded before disposal, and this determination lapses if the record changes. Affected systems and plausible reach: The Scans folder on the office manager PC, downloads on the front-desk PCs and text threads on staff personal phones; not the athenaOne chart, which athenahealth holds. Sensitivity of the information: School and daycare forms and referral attachments awaiting upload, as the inventory records. Harm to patients and the practice: Loss of documents not yet in the chart; most can be requested again from the family or the sender. Clinical and operational consequences: Delay in care coordination while documents are re-obtained; no loss of the chart and no outage of athenaOne. Evidence: Intake backup-coverage: athena covers the chart; Gmail, the eFax account and the scans on the office manager PC are not backed up;

Inventory: Office manager PC holds a local Scans folder of documents before upload. Reviewed under heightened review: Two levels below the starting point: the patient chart is vendor-held, and the recorded sole copies are documents awaiting upload that can largely be re-obtained. (A. Reviewer (SYNTHETIC), October 21, 2026.)

In NIST SP 800-30 Table I-2 (Part C), likelihood High with impact Moderate gives a level of risk of Moderate.

Related risks

The same safeguard gaps also bear on: ransomware (High); fire, flood, storm or power loss (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 34, 35, 36, and 37; Longer-term work: Item 74.

Visible or unattended screens

Threat source: Accidental — workforce · Assessed risk: Moderate (likelihood Very High, impact Moderate)

Threat event	Patients or visitors see patient information on unattended or visible workstation screens.
Assets	Reception and clinical workstations
Safeguards with a gap	§164.310(c) Workstation security, §164.312(a)(2)(iii) Automatic logoff, and §164.310(b) Workstation use
Treatment	Item 57 (High), Item 58 (High), Item 59 (High)

What could go wrong

> A screen at reception or in a treatment room shows a schedule or chart to the next patient, or is left signed in when staff step away.[18]

> **What this does not mean.** The exposure is often a few records at a time, which is why impact starts lower than for system-wide threats. It is not always small: a schedule, a worklist or a search result on screen can show many patients at once.

The data environment

The analysis considered where workstations are placed relative to patients and visitors.

Established in the record.

- §164.312(a)(2)(iii), “Do computers lock themselves after a period of inactivity, and after how long”: enabled: no; observed: yes; alternative: athena logs you out after a while on its

18. **ePHIShield.** ePHIShield's explanation of the threat; professional interpretation. Threat library entry v0.3, reviewed and approved by ePHIShield.

own. Windows screen lock was turned off on the front PCs because staff complained (observed by ePHIShield).

- §164.312(a)(2)(iii), the practice's addressable determination: implemented: no; documented: no (observed by ePHIShield).

Established adverse facts on §164.310(c) are stated under lost or stolen device.

The safeguards this threat depends on

Safeguard	Status (Part E)	Evidence	Weight	What it does here
§164.310(c) Workstation security	Not Implemented	two deficient	+1 (absent)	Positioning and physical safeguards keep screens out of view.
§164.312(a)(2)(iii) Automatic logoff	Not Implemented	two deficient	+1 (absent)	Automatic logoff ends an unattended session.
§164.310(b) Workstation use	Not Implemented	one reported, one unknown	+1 (absent)	A workstation use policy sets expectations for staff.

Status as in Part E; weight as in Part C.

How the rating was reached

L.I.S.A. starts this threat at likelihood High and impact Moderate, ePHIShield's starting points for a practice of this kind. The three safeguards weigh +1, +1, +1; their average, +1, multiplied by 1.6 and rounded, moves likelihood two steps up, to Very High.

No recorded circumstance of the practice adjusts the result, so likelihood is Very High and impact stays at its starting point, Moderate.

In NIST SP 800-30 Table I-2 (Part C), likelihood Very High with impact Moderate gives a level of risk of Moderate.

Related risks

The same safeguard gaps also bear on: lost or stolen device (High); unauthorized physical access (Moderate). Each is analyzed under its own heading.

Treatment

Each step is set out in full once, in Part G (priorities above). Near-term correction: Items 57, 58, and 59.

E. Current safeguards and evidence

The safeguards examined in this analysis, with what the record establishes about each and how it is known. A status here describes the safeguard as it bears on the risks above; it is not a compliance ruling on the requirement as a whole. “Examined in part” means only some of the requirement's elements were examined. The weights the ratings give each status are in Part C.

The evidence column counts the questions each status rests on by what supports them: deficient (an established answer that counts against the safeguard), contradicted, observed by ePHIShield, documented, reported by the practice and not verified, not provided, asked and unknown, or not asked. Each question, with its source, documents, date, systems and any ruling, is in Schedule H-10.

Administrative safeguards

Safeguard	Status	Evidence	What the record shows
§164.308(a)(1)(ii)(A) Risk analysis	Not Implemented	one deficient	Deficiency recorded: “A risk analysis has been performed”: no; “Document produced and reviewed by analyst”: no. Established against it: “Has the practice ever had a security risk analysis performed, and if so when and by whom”: ever: no; seen: no; notes: We have the HIPAA binder but nobody has ever come in and done an assessment (reported by Office manager (also billing)).

Safeguard	Status	Evidence	What the record shows
§164.308(a)(1)(ii)(B) Risk management	Not Implemented	one deficient, one reported, one unknown	Established against it: “When a security problem is identified, how does the practice decide what to fix, who approves it, and how it gets tracked to completion”: how decided: If something breaks I call Kyle or athena support; who approves: The doctors approve anything that costs money; tracked: Not tracked, we just fix it; assigned: Me or Kyle; completion evidence: Nothing written (reported by Office manager (also billing)).
§164.308(a)(1)(ii)(C) Sanction policy	Not Implemented	one deficient	Deficiency recorded: “Staff have been informed of it”: no. Established against it: “Is there a written policy describing consequences for staff who violate security or privacy rules, and have staff been told about it”: policy exists: yes; seen: yes; staff informed: no; notes: Template sanction policy is in the binder (Section 4). Not signed, no staff acknowledgments, staff interviewed on site were not aware of it (reported by Computer helper, source S-13 in Schedule H-1). Professional determination: Not adequate by A. Reviewer (SYNTHETIC) (ePHIShield), 2026-10-21: SYNTHETIC REHEARSAL. The only sanction policy is an unsigned 2017 template no one adopted or communicated; staff are unaware of it and the record shows no sanctions process. Rejected document: “HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)” (D-2), offered for “Is there a written policy describing consequences for staff who violate security or privacy rules, and have staff been told about it?”. Ruling: evidence rejected by A. Reviewer (SYNTHETIC) (compliance solutions consultant), October 21, 2026: “SYNTHETIC REHEARSAL. The binder's sanction policy is an unsigned template with no staff acknowledgments; staff interviewed on site were not aware of it. It shows text that was bought, not a policy the practice adopted.” Source: Computer helper, source S-13 in Schedule H-1. Effect: the document earns no supporting credit; this is not a finding that the control is absent.
§164.308(a)(1)(ii)(D) Information system activity review	Not Implemented	one deficient	Deficiency recorded: “Somebody reviews access or security reports”: no. Established against it: “Does anyone regularly look at who accessed patient records in the EHR, or at system security reports? How often, and who does it”: anyone reviews: no; what reviewed: Nobody looks at that. I didn't know athena had it (reported by Office manager (also billing)).

Safeguard	Status	Evidence	What the record shows
§164.308(a)(2) Assigned security responsibility	Not Implemented	one deficient	Deficiency recorded: “Assignment is documented in writing”: no; “Written designation reviewed by analyst”: no. Established against it: “Who is the person formally responsible for HIPAA security at the practice, and is that assignment in writing”: name: Me (office manager); in writing: no; seen: no (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)).
§164.308(a)(3)(i) Workforce security	Partially Implemented	one deficient, one reported	Deficiency recorded: the recorded answer (no) counts against the safeguard. Established against it: “Does anyone periodically review who has access to each system to make sure they should still have that access”: no (reported by Office manager (also billing)).
§164.308(a)(3)(ii)(A) Authorization and/or supervision	Not Implemented	one deficient, one unknown	Deficiency recorded: “Approval is recorded”: no. Established against it: “Who approves a new staff member's access to the EHR and other systems, and is the approval recorded”: who approves: I do, when I set them up; recorded: no (reported by Office manager (also billing)).
§164.308(a)(3)(ii)(C) Termination procedures	Not Implemented	two deficient, one contradicted, one reported	“When someone leaves, what happens to their EHR login, email, building keys or codes, and any practice-owned device? Who does it and how quickly”: the practice's answer (ehr) is contradicted by the established answer to §164.308(a)(3)(ii)(C): “Are there any active logins belonging to people who no longer work here”; it is not counted as support. Deficiency recorded: the recorded answer (yes) counts against the safeguard. Established against it: “Are there any active logins belonging to people who no longer work here”: yes (document read by ePHIShield: athenaOne active user list (printed during on-site visit)). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Office manager removes people from athena when she remembers; no checklist; evidence the alternative operates: None; user list showed a departed MA still active; remaining exposure recorded: athenaOne account of MA who left 2025-08 still active; shared Windows passwords and alarm code not changed after departures; departed staff keep parent text threads on their personal phones (document read by ePHIShield: athenaOne active user list (printed during on-site visit)). The practice described what it does instead, but the determination not to implement the specification was not documented.

Safeguard	Status	Evidence	What the record shows
§164.308(a)(3)(ii)(C) (continued)			§164.306(d)(3)(ii)(B)(1) requires that documentation. Professional determination: Not adequate by A. Reviewer (SYNTHETIC) (ePHIShield), 2026-10-21: SYNTHETIC REHEARSAL. The printed athenaOne user list shows the MA who left in 2025-08 still active; there is no checklist, and codes and shared passwords are not changed after departures. The reported 'EHR login removed' is contradicted by the document.
§164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions	Not Applicable	no answers	Not applicable: Applies only to a health care clearinghouse within a larger organization; this entity is not assessed as a clearinghouse.
§164.308(a)(4)(ii)(C) Access establishment and modification	Not Implemented	two deficient	Deficiency recorded: “Someone at the practice has changed roles”: no; “There is a set way to adjust access if it happens”: no. Established against it: “When someone changes roles, is their access changed to match the new role, and is that recorded”: occurred: no; procedure: no (reported by Office manager (also billing)). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: athena roles assigned at setup by the office manager; never reviewed; evidence the alternative operates: None; remaining exposure recorded: Generic kiosk account in athenaOne with front-desk role; no periodic review of who has access (reported by Office manager (also billing)). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Safeguard	Status	Evidence	What the record shows
§164.308(a)(5)(i) Security awareness and training	Not Implemented	two deficient, one unknown	Deficiency recorded: “Every workforce member receives training”: no; “Completion records are kept”: no; “Records reviewed by analyst”: no; fewer people trained than the recorded workforce (0 of the 7 recorded workforce members covered). Established against it: “Does every staff member receive security training, when does it happen, and are completion records kept”: all staff: no; when: Never formally; binder says annual; records kept: no; records seen: no; covered count: 0 (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)). Deficiency recorded: the recorded answer (no) counts against the safeguard. Established against it: “Do new staff receive training before they are given access to patient information”: no (reported by Office manager (also billing)). Not established after 2 attempt(s), first with the practice administrator and then by another route (ask the HIPAA security official instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.
§164.308(a)(5)(ii)(A) Security reminders	Not Implemented	two deficient	Established against it: “Between trainings, does staff receive security reminders — emails, huddles, posters, newsletters”: No, not really. I'll mention things at staff meetings if something comes up (reported by Office manager (also billing)). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Occasional verbal mentions at staff meetings; evidence the alternative operates: None; remaining exposure recorded: Staff have no recurring prompts about phishing, texting, or passwords (reported by Office manager (also billing)). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Safeguard	Status	Evidence	What the record shows
§164.308(a)(5)(ii)(B) Protection from malicious software	Partially Implemented	two deficient, one deficient in part	Deficiency recorded: “Personal devices used for work are covered”: no; “Staff know how and to whom to report”: no. Established against it: “What protects the practice's computers from viruses and ransomware, and is it on every machine including any personal devices used for work”: product: Windows Defender (built-in); personal devices: no; reporting: no (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: the recorded answer (no) counts against the safeguard. Established against it: “Does anyone receive and act on alerts from that software”: no (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Relies on built-in Windows Defender on practice PCs; nothing on personal phones or the physicians' home laptops; evidence the alternative operates: None; no console or alerts reviewed; remaining exposure recorded: No one sees alerts; personal laptops and phones that reach athena and Gmail are unmanaged (reported by Computer helper, source S-13 in Schedule H-1). Partly established when intake closed. Established parts are kept; still not established: Present on every practice machine. The practice described what it does instead, but the determination not to implement the specification was not documented.
§164.308(a)(5)(ii)(B) (continued)			§164.306(d)(3)(ii)(B)(1) requires that documentation.
§164.308(a)(5)(ii)(C) Log-in monitoring	Not Implemented	two deficient	Established against it: “Does anyone review failed login attempts or get alerted to unusual login activity in the EHR, email, or remote access”: No. Kyle doesn't check that and I wouldn't know where to look (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Nothing done; evidence the alternative operates: None; remaining exposure recorded: Failed logins to athena, Gmail and TeamViewer are never reviewed (reported by Computer helper, source S-13 in Schedule H-1).

Safeguard	Status	Evidence	What the record shows
§164.308(a)(5)(ii)(D) Password management	Not Implemented	two deficient	Deficiency recorded: “Any accounts shared between staff”: yes. Established against it: “What are the practice's rules for passwords — length, reuse across systems, sharing, and how they are stored or remembered”: rules: athena makes you use a strong password and change it. Windows passwords are simple and haven't been changed in years; reuse: yes; shared: yes; storage: Written down / memorized; one on a sticky note at the front desk (observed by ePHIShield). Deficiency recorded: the recorded answer (yes) counts against the safeguard. Established against it: “Do any staff share passwords or write them where others can see them”: yes (observed by ePHIShield).
§164.308(a)(6)(i) Security incident procedures	Not Implemented	two unknown	A document was reviewed and rejected by ePHIShield's reviewer: SYNTHETIC REHEARSAL. The binder's incident procedure is a template with no names or contacts; the office manager's own account of what happens (call her, then the helper or athena) and the informally handled 2025 misfax do not follow it. The answer rests on the practice's statement. A document was reviewed and rejected by ePHIShield's reviewer: SYNTHETIC REHEARSAL. Same template: its steps are generic, it names no one, and the practice did not follow it for the 2025 misdirected fax. The answer rests on the practice's statement. Professional determination: Not adequate by A. Reviewer (SYNTHETIC) (ePHIShield), 2026-10-21: SYNTHETIC REHEARSAL. The binder procedure is an unadopted template naming no one; the 2025 misdirected fax was handled outside it, with no record or assessment. Rejected document: “HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)” (D-2), offered for “If a computer were infected, a laptop stolen, or records emailed to the wrong person, is there a written procedure telling staff what to do and whom to tell?”. Ruling: evidence rejected by A. Reviewer (SYNTHETIC) (compliance solutions consultant), October 21, 2026: “SYNTHETIC REHEARSAL. The binder's incident procedure is a template with no names or contacts; the office manager's own account of what happens (call her, then the helper or athena) and the informally handled 2025 misfax do not follow it.”

Safeguard	Status	Evidence	What the record shows
§164.308(a)(6)(i) (continued)			Source: Computer helper, source S-13 in Schedule H-1. Effect: the document earns no supporting credit; this is not a finding that the control is absent. Rejected document: “HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)” (D-2), offered for “Read the practice's incident procedure. Which of the things the rule names does it actually cover, and what would happen if someone followed it exactly?”. Ruling: evidence rejected by A. Reviewer (SYNTHETIC) (compliance solutions consultant), October 21, 2026: “SYNTHETIC REHEARSAL. Same template: its steps are generic, it names no one, and the practice did not follow it for the 2025 misdirected fax.” Source: Computer helper, source S-13 in Schedule H-1. Effect: the document earns no supporting credit; this is not a finding that the control is absent.
§164.308(a)(6)(ii) Response and reporting	Not Implemented	two deficient	Deficiency recorded: “An incident log exists”: no; “Outcomes are recorded for each entry”: no; “Log reviewed by analyst”: no. Established against it: “Is there a log of security incidents and what was done about each one”: log exists: no; outcomes recorded: no; seen: no (reported by Office manager (also billing)). Established against it: “Describe the most recent security incident and how it was handled”: The misfaxed school form in 2025. The person who got it called us, said they shredded it. I re-faxed it to the right number. We didn't write anything up (reported by Office manager (also billing)).
§164.308(a)(7)(i) Contingency plan	Not Implemented	one unknown	Every required specification beneath this standard is an established deficiency (§164.308(a)(7)(ii)(A), §164.308(a)(7)(ii)(B), §164.308(a)(7)(ii)(C)), so the standard is not met; its own question is asked and not established.

Safeguard	Status	Evidence	What the record shows
§164.308(a)(7)(ii)(A) Data backup plan	Not Implemented	one deficient, three unknown	Established against it: “Does the backup include every system on the ePHI inventory, including cloud-hosted systems and imaging”: athena covers the chart. Gmail, the eFax account, and the scans on the office manager PC are not backed up by anyone that I know of (reported by Computer helper, source S-13 in Schedule H-1). Not established before the reporting date after 4 attempt(s). This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established. Not established after 3 attempt(s), first with the IT provider and then by another route (ask the practice administrator, for the vendor's documentation or a vendor contact who can answer instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.
§164.308(a)(7)(ii)(B) Disaster recovery plan	Not Implemented	one deficient, one reported	Deficiency recorded: “A written restore procedure exists”: no; “Procedure reviewed by analyst”: no. Established against it: “Is there a written procedure for restoring the records, and who would perform it”: written: no; seen: no; who: athena support, I guess (reported by Computer helper, source S-13 in Schedule H-1).
§164.308(a)(7)(ii)(C) Emergency mode operation plan	Not Implemented	one deficient	Established against it: “If systems were down for several days, how would the practice keep seeing patients and still protect patient information”: If athena was down we'd use paper and enter it later. If the internet is out we'd have to reschedule people. We've never had it go down for more than an hour or two (reported by Office manager (also billing)).
§164.308(a)(7)(ii)(D) Testing and revision procedures	Unable to Determine	one unknown	Not asked: it depends on whether the answer to “If the office lost its systems to fire, flood, ransomware, or extended power loss, is there a written plan for continuing patient care and recovering the records?” (§164.308(a)(7)(i)), which was not established. This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established. Settle the earlier question first.

Safeguard	Status	Evidence	What the record shows
§164.308(b)(1) Business associate contracts and other arrangements	Partially Implemented	three deficient, one documented, two not provided	Established against it: the agreement with Google, Tri-State Office Systems (SYNTHETIC), and Kyle Pruitt (SYNTHETIC), independent computer helper does not meet this requirement as read (Schedule H-10). Read vendor by vendor: an executed agreement on record, its terms read as compliant: athenahealth; no agreement (the practice says there is none): Google, Tri-State Office Systems (SYNTHETIC), Kyle Pruitt (SYNTHETIC), independent computer helper; requested, and no agreement produced: eFax (Consensus Cloud Solutions), Valley After-Hours Answering (SYNTHETIC).
§164.308(b)(3) Written contract or other arrangement	Partially Implemented	three deficient, one documented, two not provided	Established against it: the agreement with Google, Tri-State Office Systems (SYNTHETIC), and Kyle Pruitt (SYNTHETIC), independent computer helper does not meet this requirement as read (Schedule H-10). Read vendor by vendor: an executed agreement on record, its terms read as compliant: athenahealth; no agreement (the practice says there is none): Google, Tri-State Office Systems (SYNTHETIC), Kyle Pruitt (SYNTHETIC), independent computer helper; requested, and no agreement produced: eFax (Consensus Cloud Solutions), Valley After-Hours Answering (SYNTHETIC).

Physical safeguards

Safeguard	Status	Evidence	What the record shows
§164.310(a)(1) Facility access controls	Partially Implemented	one deficient, one deficient in part	Established against it: “Who can get into the office outside of business hours, and how — keys, codes, badges? Is there a record of who holds each”: secured after hours: yes; who has access: Both doctors, me, the NP, the cleaning crew, and the landlord. All staff know the alarm code; observed: yes (observed by ePHIShield). Deficiency recorded: “That space is locked or otherwise restricted”: no. Established against it: “Where is the server or main network equipment located, and is that space locked”: has onsite equipment: yes; where: Comcast gateway on a shelf in the back storage closet; room secured: no; observed: yes (observed by ePHIShield).

Safeguard	Status	Evidence	What the record shows
§164.310(a)(2)(i) Contingency operations	Partially Implemented	one deficient, one deficient in part	Deficiency recorded: “The arrangement is written down”: no. Established against it: “In an after-hours emergency, who can get into the building and to the equipment to restore systems”: who: Me or either doctor; we all have keys; documented: no (reported by Office manager (also billing)). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Key holders could open the office; nothing on site needs restoring since records are in athena; evidence the alternative operates: Observed key holders; remaining exposure recorded: No written arrangement; low exposure because no on-site record system (observed by ePHIShield). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.
§164.310(a)(2)(ii) Facility security plan	Partially Implemented	one deficient, one observed	Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Locked exterior doors and an alarm; no written facility security plan; evidence the alternative operates: Observed locks and alarm panel; remaining exposure recorded: Alarm code shared by everyone and never changed; storage closet with old laptops and the gateway unlocked (observed by ePHIShield). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Safeguard	Status	Evidence	What the record shows
§164.310(a)(2)(iii) Access control and validation procedures	Not Implemented	two deficient	Deficiency recorded: “Visitors are identified on arrival”: no; “Visitors are logged”: no; “Visitors are escorted where ePHI is accessible”: no; “Applies to IT and equipment vendors as well”: no. Established against it: “How are visitors, vendors, and repair technicians handled — signed in, escorted, left alone with equipment”: identified: no; logged: no; escorted: no; vendors: no (reported by Office manager (also billing)). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Front desk sees who comes in; copier and repair techs are let in and left alone; evidence the alternative operates: None; remaining exposure recorded: Parents and vendors can reach hallway workstations and the unlocked storage closet (observed by ePHIShield). Not directly observed; this requirement is better supported by on-site observation than by representation. The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Safeguard	Status	Evidence	What the record shows
§164.310(b) Workstation use	Not Implemented	one reported, one unknown	A document was reviewed and rejected by ePHIShield's reviewer: SYNTHETIC REHEARSAL. The binder is an uncustomized 2017 template that the practice never adopted; the record shows shared Windows accounts, the Windows screen lock turned off on the front and exam PCs, and a password on a sticky note at the front desk, which the template's workstation rules do not describe. The answer rests on the practice's statement. Professional determination: Not adequate by A. Reviewer (SYNTHETIC) (ePHIShield), 2026-10-21: SYNTHETIC REHEARSAL. The only workstation rules are an unadopted 2017 template; observed practice (shared accounts, screen lock off, a posted password) contradicts them, and nothing governs the physicians' personal-laptop work from home. Rejected document: “HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)” (D-2), offered for “Is there a written rule about what staff may and may not do on practice computers, including personal use and web browsing?”. Ruling: evidence rejected by A. Reviewer (SYNTHETIC) (compliance solutions consultant), October 21, 2026: “SYNTHETIC REHEARSAL. The binder is an uncustomized 2017 template that the practice never adopted; the record shows shared Windows accounts, the Windows screen lock turned off on the front and exam PCs, and a password on a sticky note at the front desk, which the template's workstation rules do not describe.” Source: Computer helper, source S-13 in Schedule H-1.
§164.310(b) (continued)			Effect: the document earns no supporting credit; this is not a finding that the control is absent.
§164.310(c) Workstation security	Not Implemented	two deficient	Deficiency recorded: “Privacy filters, screen angle, or barriers in place”: no; A screen showing ePHI is visible to patients or visitors. Established against it: “Can patients or visitors see any computer screens from the waiting area, check-in desk, or hallways”: visible: yes; where: Front desk PC 1 and 2 monitors face the waiting room chairs; kiosk tablet in waiting area; mitigations: no (observed by ePHIShield). Deficiency recorded: “Staff are expected to lock screens when stepping away”: no. Established against it: “Are workstations locked or logged off when staff step away”: policy: no; observed unlocked: yes (observed by ePHIShield).

Safeguard	Status	Evidence	What the record shows
§164.310(d)(1) Device and media controls	Not Implemented	one deficient	Deficiency recorded: “A device list was provided”: no; “Imaging or diagnostic equipment storing ePHI”: no; “Backup drives, USB media, external storage”: no; devices found that the inventory does not list. Established against it: “List the computers, laptops, tablets, phones, servers, and any USB drives or external disks that hold or access patient information”: list provided: no; imaging: no; removable: no; leased: yes; unrecognized: Two old laptops in the storage closet from before athena; the copier (leased) scans to email; staff personal phones used for texting parents; the doctors' home laptops (observed by ePHIShield). Partly established when intake closed. Established parts are kept; still not established: Desktops, laptops, tablets accounted for; Copiers or multifunction printers with internal drives.
§164.310(d)(2)(i) Disposal	Not Implemented	one deficient	Deficiency recorded: “A disposal process exists”: no; “It is written down”: no. Established against it: “What happens to old computers, hard drives, phones, and copiers when they are replaced or discarded”: process exists: no; written: no; method: Old laptops just went into the closet; vendor: None (observed by ePHIShield).
§164.310(d)(2)(ii) Media re-use	Not Implemented	one deficient	Deficiency recorded: “Method removes data rather than deleting files”: no. Established against it: “When a computer or phone is reassigned to another staff member, is it wiped first”: reuse happens: yes; method: New person just uses the shared login on that PC; adequate: no (reported by Computer helper, source S-13 in Schedule H-1).
§164.310(d)(2)(iii) Accountability	Not Implemented	two deficient	Deficiency recorded: “Device custody is tracked”: no. Established against it: “Is there a record of who has each laptop or portable device and when equipment moves between locations”: tracked: no (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Nothing; all PCs stay in the office, nobody tracks the laptops in the closet; evidence the alternative operates: None; remaining exposure recorded: No record of the two closet laptops, the kiosk tablet, or what is on them (observed by ePHIShield).

Technical safeguards

Safeguard	Status	Evidence	What the record shows
§164.312(a)(1) Access control	Partially Implemented	one deficient in part	Established against it: “For each system on the inventory, does each user have their own individual account, is an account shared, or is no login required”: role based: yes; who admins: Office manager (athena); Kyle (Windows); admin accounts: Office manager in athena; Kyle and the shared Windows accounts are local admins on the PCs; vendor controlled: yes (document read by ePHIShield: athenaOne active user list (printed during on-site visit)). None of the 2 addressable specifications under this standard is implemented. Addressable does not mean optional: under §164.306(d)(3) each must be assessed, then implemented where reasonable and appropriate, or the reason documented and an equivalent alternative implemented where reasonable and appropriate. The standard itself must still be met (§164.306(c)). Confirm that the practice meets this standard by some other means, or the standard is not met.
§164.312(a)(2)(i) Unique user identification	Partially Implemented	one deficient, one deficient in part	Deficiency recorded: “Every user has their own log-in”: no on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier; “Any shared or generic accounts exist”: yes on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier. Established against it: “Does every person have their own login for every system, or are any logins shared between staff”: all unique: no on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier; yes on Office manager PC, Staff personal phones, and Physicians' personal laptops; not sure on LabCorp lab interface and Old laptops in storage closet (2); any shared: no on LabCorp lab interface, Office manager PC, Staff personal phones, and Physicians' personal laptops; yes on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, and Canon multifunction copier; not sure on Old laptops in storage closet (2) (document read by ePHIShield: athenaOne active user list (printed during on-site visit)). Deficiency recorded: “Inside that system, each person still signs in with their own credentials, so access to the patient information is attributed to a named person”: no.

Safeguard	Status	Evidence	What the record shows
§164.312(a)(2)(i) (continued)			Established against it: “If any logins are shared, which systems and how many people share them”: which system: Windows on front desk and exam room PCs; athenaOne kiosk login; the frontdesk@ Gmail and eFax logins; who uses: Front desk and both MAs (Windows FrontDesk account); MAs and providers (Windows Exam account); parents and front desk (kiosk tablet); why: Faster than logging in and out all day. The tablet needed to stay logged in for check-in; attributed: no (reported by Computer helper, source S-13 in Schedule H-1).
§164.312(a)(2)(ii) Emergency access procedure	Not Implemented	one deficient	Deficiency recorded: “A procedure exists for urgent access”: no; “It is written down”: no. Established against it: “If the person who normally controls access were unavailable during an emergency, how would authorized staff get the patient information they need”: procedure exists: no; what: Call athena support, or one of the doctors could log in; they have admin too I think; documented: no; systems covered: athenaOne (reported by Office manager (also billing)).
§164.312(a)(2)(iii) Automatic logoff	Not Implemented	two deficient	Deficiency recorded: “Sessions terminate after inactivity”: no. Established against it: “Do computers lock themselves after a period of inactivity, and after how long”: enabled: no; observed: yes; alternative: athena logs you out after a while on its own. Windows screen lock was turned off on the front PCs because staff complained (observed by ePHIShield). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: athenaOne's own session timeout; Windows lock disabled on front and exam PCs; evidence the alternative operates: Analyst observed unlocked front desk PC with no one present; remaining exposure recorded: Windows desktops, Gmail and eFax stay open on shared PCs; kiosk tablet stays signed in to athenaOne all day (observed by ePHIShield). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Safeguard	Status	Evidence	What the record shows
§164.312(a)(2)(iv) Encryption and decryption	Not Implemented	three deficient, one reported	Deficiency recorded: “Workstation drives encrypted”: no; “Laptop drives encrypted”: no; “Server drives encrypted”: no; “If absent, the addressable decision is documented”: no. Established against it: “Are the hard drives on computers, laptops, and servers encrypted”: workstations: no; laptops: no; server: no; unencrypted devices: All office PCs; the two old laptops in the closet; physicians' personal laptops unknown; who confirmed: Kyle (believes BitLocker is not on); decision documented: no (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “A lost device can be wiped remotely”: no. Established against it: “Are phones and tablets that access patient information encrypted and passcode protected”: phones used: yes; encrypted: not sure; remote wipe: no; personal devices: yes (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Relies on athena storing the chart in the cloud.
§164.312(a)(2)(iv) (continued)			Binder says all ePHI is encrypted but nothing was set up; evidence the alternative operates: None; remaining exposure recorded: Office manager PC scan folder, the two closet laptops (contents unknown), copier drive, Gmail on personal phones (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.
§164.312(b) Audit controls	Unable to Determine	one unknown	Not established before the reporting date after 4 attempt(s). This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established.
§164.312(c)(1) Integrity	Partially Implemented	one deficient in part	Established against it: “What prevents patient records from being changed or deleted improperly — permissions, amendment tracking, or version history”: protection: athena keeps a history of chart changes and signed notes can only be amended, not deleted; ehr native: yes (reported by Computer helper, source S-13 in Schedule H-1).
§164.312(c)(2) Mechanism to authenticate electronic protected health information	Unable to Determine	one unknown	Not established before the reporting date after 4 attempt(s). This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established.

Safeguard	Status	Evidence	What the record shows
§164.312(d) Person or entity authentication	Partially Implemented	one deficient in part, one reported	Established against it: “How do users prove who they are — password only, or password plus a code or app”: method: Password plus multi-factor for some systems; password only: yes (reported by Computer helper, source S-13 in Schedule H-1).
§164.312(e)(1) Transmission security	Not Implemented	one deficient, one reported	Deficiency recorded: staff text about patients from personal phones. Established against it: “Is patient information ever sent by regular email or text message”: ephi by email: yes; to whom: Parents (school/daycare forms, shot records), sometimes referral offices; texting staff: yes; email service: Gmail (Google Workspace); encrypted transit: not sure (reported by Office manager (also billing)).
§164.312(e)(2)(i) Integrity controls	Not Implemented	one deficient, one unknown	Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: Relies on athena and LabCorp interfaces; nothing checked by the practice; evidence the alternative operates: None; remaining exposure recorded: Practice cannot say whether interfaces are integrity-protected; no confirmation of eFax delivery integrity (reported by Computer helper, source S-13 in Schedule H-1). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.
§164.312(e)(2)(ii) Encryption	Partially Implemented	one deficient, one deficient in part, one observed	Established against it: “Are the connections used to reach the EHR, email, and any remote access encrypted”: encrypted paths: athena in the browser (https); Gmail between Google servers; TeamViewer; unencrypted paths: Text messages from personal phones; Gmail to parents whose email provider may not support TLS; fax leg to recipient (reported by Computer helper, source S-13 in Schedule H-1). Deficiency recorded: “The specification is fully implemented”: no; “That decision is written down”: no. Established against it: the practice's addressable determination as recorded — implemented: no; decision documented: no; alternative described: athena web traffic is encrypted by the vendor; email and texts are sent as ordinary messages; evidence the alternative operates: None; remaining exposure recorded: SMS from personal phones to parents with child names; plain Gmail to parents with forms attached (reported by Computer helper, source S-13 in Schedule H-1). The practice described what it does instead, but the determination not to implement the specification was not documented. §164.306(d)(3)(ii)(B)(1) requires that documentation.

Organizational requirements

Safeguard	Status	Evidence	What the record shows
§164.314(a)(1) Business associate contracts or other arrangements	Partially Implemented	three deficient, one documented, two not provided	Established against it: the agreement with Google, Tri-State Office Systems (SYNTHETIC), and Kyle Pruitt (SYNTHETIC), independent computer helper does not meet this requirement as read (Schedule H-10). Read vendor by vendor: an executed agreement on record, its terms read as compliant: athenahealth; no agreement (the practice says there is none): Google, Tri-State Office Systems (SYNTHETIC), Kyle Pruitt (SYNTHETIC), independent computer helper; requested, and no agreement produced: eFax (Consensus Cloud Solutions), Valley After-Hours Answering (SYNTHETIC).
§164.314(a)(2)(i) Business associate contracts	Partially Implemented	three deficient, one documented, two not provided	Established against it: the agreement with Google, Tri-State Office Systems (SYNTHETIC), and Kyle Pruitt (SYNTHETIC), independent computer helper does not meet this requirement as read (Schedule H-10). Read vendor by vendor: an executed agreement on record, its terms read as compliant: athenahealth; no agreement (the practice says there is none): Google, Tri-State Office Systems (SYNTHETIC), Kyle Pruitt (SYNTHETIC), independent computer helper; requested, and no agreement produced: eFax (Consensus Cloud Solutions), Valley After-Hours Answering (SYNTHETIC).
§164.314(a)(2)(iii) Business associate contracts with subcontractors	Not Applicable	no answers	Not applicable: Entity is not assessed as a business associate.
§164.314(b)(1) Requirements for group health plans	Not Applicable	no answers	Not applicable: Applies to group health plans; the entity is not assessed as one and was recorded as not sponsoring one.

General rules

Safeguard	Status	Evidence	What the record shows
§164.302 Applicability	Applies (general provision)	two reported	—
§164.306(a) General requirements	Applies (general provision)	one observed, two reported	What the status rests on: observed: ephi-locations; reported: ephi-systems, workforce-count.
§164.306(b) Flexibility of approach	Applies (general provision)	one reported	—

Not assessed in this engagement

> These requirements are examined in a full Security Rule assessment and were not examined in this risk analysis. Nothing is concluded about them here: they are neither met nor unmet in this report.

- §164.306(e) Maintenance
- §164.308(a)(1)(i) Security management process
- §164.308(a)(3)(ii)(B) Workforce clearance procedure
- §164.308(a)(4)(i) Information access management
- §164.308(a)(4)(ii)(B) Access authorization
- §164.308(a)(7)(ii)(E) Applications and data criticality analysis
- §164.308(a)(8) Evaluation
- §164.310(a)(2)(iv) Maintenance records
- §164.310(d)(2)(iv) Data backup and storage
- §164.316(a) Policies and procedures
- §164.316(b)(1) Documentation
- §164.316(b)(2)(i) Time limit
- §164.316(b)(2)(ii) Availability
- §164.316(b)(2)(iii) Updates

F. Professional determinations and limitations

Professional determinations

Safeguard	Determination	Basis	Reviewer
§164.308(a)(1)(ii)(C) Sanction policy	Not adequate (synthetic demonstration; not an ePHIShield determination)	SYNTHETIC REHEARSAL. The only sanction policy is an unsigned 2017 template no one adopted or communicated; staff are unaware of it and the record shows no sanctions process.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(3)(ii)(C) Termination procedures	Not adequate (synthetic demonstration; not an ePHIShield determination)	SYNTHETIC REHEARSAL. The printed athenaOne user list shows the MA who left in 2025-08 still active; there is no checklist, and codes and shared passwords are not changed after departures. The reported 'EHR login removed' is contradicted by the document.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(6)(i) Security incident procedures	Not adequate (synthetic demonstration; not an ePHIShield determination)	SYNTHETIC REHEARSAL. The binder procedure is an unadopted template naming no one; the 2025 misdirected fax was handled outside it, with no record or assessment.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.310(b) Workstation use	Not adequate (synthetic demonstration; not an ePHIShield determination)	SYNTHETIC REHEARSAL. The only workstation rules are an unadopted 2017 template; observed practice (shared accounts, screen lock off, a posted password) contradicts them, and nothing governs the physicians' personal-laptop work from home.	A. Reviewer (SYNTHETIC), October 21, 2026

In addition, ePHIShield's reviewer read 13 own-words answers and recorded whether each establishes what it describes.

Professional readings of own-words answers

Requirement	Question	Reading	Reason	Reviewer
§164.308(a)(1)(ii)(B)	When a security problem is identified, how does the practice decide what to fix, who approves it, and how it gets tracked to completion?	Adverse	SYNTHETIC REHEARSAL. Problems are fixed as they arise: nothing is tracked, no owner or target date is recorded, and nothing is written. That is not a risk management process.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(3)(i)	Does each staff role get a different level of access in the EHR, or does everyone see everything?	Affirmative	SYNTHETIC REHEARSAL. athena roles (front desk, clinical, provider) are assigned per person; the kiosk's front-desk login is analyzed separately.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(5)(ii)(A)	Between trainings, does staff receive security reminders — emails, huddles, posters, newsletters?	Adverse	SYNTHETIC REHEARSAL. No reminders beyond occasional mentions at staff meetings.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(5)(ii)(B)	What protects the practice's computers from viruses and ransomware, and is it on every machine including any personal devices used for work?	Partial	SYNTHETIC REHEARSAL. Built-in Windows Defender is reported on the practice PCs; whether every PC runs it is not known, no one sees its alerts, and the personal devices have nothing.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(5)(ii)(C)	Does anyone review failed login attempts or get alerted to unusual login activity in the EHR, email, or remote access?	Adverse	SYNTHETIC REHEARSAL. Nobody reviews failed or unusual sign-ins in any system.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(6)(ii)	Describe the most recent security incident and how it was handled.	Adverse	SYNTHETIC REHEARSAL. The misdirected fax was handled informally: no record, no assessment of whether it was a reportable breach.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(7)(ii)(A)	Does the backup include every system on the ePHI inventory, including cloud-hosted systems and imaging?	Adverse	SYNTHETIC REHEARSAL. The chart is held by athenahealth, whose own recovery is not evidenced here and is not counted as a practice gap. The Scans folder on the office manager's PC is a sole copy with no backup, so a backup plan does not cover all of the practice's ePHI.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.308(a)(7)(ii)(C)	If systems were down for several days, how would the practice keep seeing patients and still protect patient information?	Adverse	SYNTHETIC REHEARSAL. An informal paper fallback for short outages; nothing says how patient information is protected or accessed in a longer emergency.	A. Reviewer (SYNTHETIC), October 21, 2026

Requirement	Question	Reading	Reason	Reviewer
§164.310(a)(2)(i)	In an after-hours emergency, who can get into the building and to the equipment to restore systems?	Partial	SYNTHETIC REHEARSAL. The office manager and both physicians hold keys and could open the office in an emergency; the arrangement is informal and not written.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.312(a)(1)	For each system on the inventory, does each user have their own individual account, is an account shared, or is no login required?	Partial	SYNTHETIC REHEARSAL. athenaOne enforces role-based access, as the printed user list shows. On the practice PCs the shared FrontDesk and Exam Windows accounts are local administrators, so anyone using them, or malware running under them, has full control of the workstation: access control operates for the record system, not for the PCs.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.312(c)(1)	What prevents patient records from being changed or deleted improperly — permissions, amendment tracking, or version history?	Partial	SYNTHETIC REHEARSAL. athenaOne's own change history and amend-only signed notes are reported for the chart; nothing protects the integrity of Gmail, the eFax account, the Scans folder or the phones.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.312(d)	How do users prove who they are — password only, or password plus a code or app?	Partial	SYNTHETIC REHEARSAL. Passwords authenticate the named accounts, and a second factor only the office manager's athena admin account; the shared Windows, kiosk, Gmail and eFax accounts do not identify the person signing in.	A. Reviewer (SYNTHETIC), October 21, 2026
§164.312(e)(2)(ii)	Are the connections used to reach the EHR, email, and any remote access encrypted?	Partial	SYNTHETIC REHEARSAL. athena in the browser is encrypted (https); texts from personal phones, the fax leg and email to parents whose providers may not use TLS are not.	A. Reviewer (SYNTHETIC), October 21, 2026

Limitations

The analysis rests on 92 recorded answers: 11 documented, 17 observed and 64 reported. Reported answers are the practice's statements and were not verified. Of these 92 answers, four replace a statement the practice first gave that later evidence overturned (a later answer from another respondent, or a document or observation by ePHIShield, reversed a yes-or-no part or replaced a stated fact); of the 64 reported answers, one is contradicted by an established fact and is not counted as support. Schedule H-10 keeps each original statement beneath the answer that replaced it, with its source, what changed, the resolution and the round. The other reported answers were not tested by a document or observation.

These safeguards were not established, so the ratings that depend on them count them as unverified rather than in place: §164.312(b) audit controls. Settling them may lower those ratings.

> **Site visit and places not visited.** ePHIShield visited 2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (October 21, 2026, ePHIShield analyst). These places were neither visited nor evaluated remotely: Physicians' homes (remote access to athenaOne from personal laptops); Computer helper's home (remote support from his own computer). Nothing there was observed; what the analysis records about them rests on the answers of the practice and its vendors, and it makes no statement about physical conditions there (who else is in the room, who else uses the device, what can be seen or overheard).

> 14 requirements of a full Security Rule assessment were not examined (Part E). This report makes no statement about them.

> Applied in the analysis but not examined as a requirement of its own: §164.306(d) Implementation specifications: required and addressable, whose §164.306(d)(3) and §164.306(d)(3)(ii)(B)(1) is applied in Part E. It is therefore not listed as not examined.

> Beyond ePHIShield's catalog, the reviewer recorded ten risks particular to the practice (Part D). Other threats outside the catalog were not separately rated; any found later should be added at the next assessment.

Safeguards whose credit rests on the reviewer's judgment

No safeguard used in the ratings rests on evidence that shows it operating in some parts or systems and only reported in others, or on a written policy where the requirement is to apply it.

Professional risk-coverage review

18 established adverse facts in the areas the catalog may not fully evaluate and the patching condition behind the unpatched-systems rating were each considered by ePHIShield's reviewer, who either recorded a supplemental risk (Part D) or documented why the existing analysis carries the exposure; where only evidence is missing (the patching condition), the reviewer may instead record a verification follow-up. No such fact is scored automatically.

Area	Where	Established	Coverage review	Reviewer
Remote authentication	practice-wide	Remote access recorded as by password only	Recorded as a reviewer's risk (Part D: password-only remote access to athena and Gmail), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026
Shared credentials	practice-wide	Passwords recorded as shared	Carried by shared sign-in without individual attribution; access retained after someone leaves: SYNTHETIC REHEARSAL. Shared and written-down passwords are the condition rated under shared sign-ins and access kept by former staff; the sticky note and shared Windows accounts were observed. (evidence: Intake password storage: one password on a sticky note at the front desk)	A. Reviewer (SYNTHETIC), October 21, 2026

Area	Where	Established	Coverage review	Reviewer
Incident procedures	practice-wide	Incident procedure recorded as not meeting: names people, contacts current	Recorded as a reviewer's risk (Part D: misdirected fax never assessed; no working incident procedure), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026
Emergency access	practice-wide	No emergency access procedure recorded	Carried by fire, flood, storm or power loss; ransomware: SYNTHETIC REHEARSAL. No emergency access procedure is recorded; the exposure is loss of access in an outage, rated under disaster and ransomware. (evidence: Intake emergency-access: no procedure)	A. Reviewer (SYNTHETIC), October 21, 2026
Wireless segmentation	practice-wide	Guest network recorded as sharing the practice network	Carried by exploited unpatched or unsupported systems; ransomware; shared physical and network secrets never changed: SYNTHETIC REHEARSAL. The guest Wi-Fi shares the network of the practice PCs, so a guest device has a path to them: weighed in the unpatched-systems and ransomware ratings as a path to exploitable PCs (the Windows 10 PC among them, counted inside the unpatched-systems rating) ...	A. Reviewer (SYNTHETIC), October 21, 2026
Patching condition behind the unpatched-systems rating	practice-wide	Patching recorded as server not_applicable, EHR yes (reported); no date of the last update recorded. The safeguards credited against unpatched systems do not by themselves establish this	Recorded as a reviewer's risk (Part D: front-desk PC running Windows 10 past end of support), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.308(a)(3)(ii)(C)	The practice says this exposure remains: athenaOne account of MA who left 2025-08 still active; shared Windows passwords and alarm code not changed after departures; departed staff keep parent text threads on their personal phones.	Recorded as a reviewer's risk (Part D: shared physical and network secrets never changed; texts and the practice Gmail app on unmanaged personal phones), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026

Area	Where	Established	Coverage review	Reviewer
Exposure the practice says remains	164.308(a)(4)(ii)(C)	The practice says this exposure remains: Generic kiosk account in athenaOne with front-desk role; no periodic review of who has access.	Recorded as a reviewer's risk (Part D: waiting-room tablet signed in to the EHR all day), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.308(a)(5)(ii)(A)	The practice says this exposure remains: Staff have no recurring prompts about phishing, texting, or passwords.	Carried by phishing and stolen email credentials: SYNTHETIC REHEARSAL. Security reminders are one of the safeguards the phishing rating weighs, and it is weighed absent there; the reminders step treats it. (evidence: addressable-164.308(a)(5)(ii)(A): no recurring prompts) Weight used in the rating (Part D): §164.308(a)(5)(ii)(A) +1 (absent) in phishing and stolen email credentials.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.308(a)(5)(ii)(B)	The practice says this exposure remains: No one sees alerts; personal laptops and phones that reach athena and Gmail are unmanaged.	Carried by ransomware; exploited unpatched or unsupported systems; password-only remote access to athena and Gmail; texts and the practice Gmail app on unmanaged personal phones: SYNTHETIC REHEARSAL. Unwatched Defender alerts are weighed under ransomware and unpatched systems, where malicious-software protection is weighed as partly in place (-0.4: built-in Defender is present, its coverage and alerts are not) … Weight used in the rating (Part D): §164.308(a)(5)(ii)(B) −0.4 (partly in place) in ransomware; §164.308(a)(5)(ii)(B) −0.4 (partly in place) in exploited unpatched or unsupported systems.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.308(a)(5)(ii)(C)	The practice says this exposure remains: Failed logins to athena, Gmail and TeamViewer are never reviewed.	Carried by phishing and stolen email credentials; unattended personal remote-access tool on the office PC: SYNTHETIC REHEARSAL. Log-in monitoring is weighed absent in the phishing rating, which treats it with the alerting step; the unreviewed TeamViewer sign-ins are carried by the TeamViewer risk. (evidence: addressable-164.308(a)(5)(ii)(C): failed logins never reviewed) Weight used in the rating (Part D): §164.308(a)(5)(ii)(C) +1 (absent) in phishing and stolen email credentials.	A. Reviewer (SYNTHETIC), October 21, 2026

Area	Where	Established	Coverage review	Reviewer
Exposure the practice says remains	164.310(a)(2)(i)	The practice says this exposure remains: No written arrangement; low exposure because no on-site record system.	Carried by fire, flood, storm or power loss: SYNTHETIC REHEARSAL. The unwritten emergency facility access is weighed in the disaster rating, with the step to document it; the practice's own note that exposure is low is consistent with a cloud-hosted record. (evidence: addressable-164.310(a)(2)(i): no written arrangement) Weight used in the rating (Part D): §164.310(a)(2)(i) −0.4 (partly in place) in fire, flood, storm or power loss.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.310(a)(2)(ii)	The practice says this exposure remains: Alarm code shared by everyone and never changed; storage closet with old laptops and the gateway unlocked.	Recorded as a reviewer's risk (Part D: shared physical and network secrets never changed; two retired unencrypted laptops in an unlocked closet), where the reasons are given	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.310(a)(2)(iii)	The practice says this exposure remains: Parents and vendors can reach hallway workstations and the unlocked storage closet.	Carried by unauthorized physical access; visible or unattended screens; two retired unencrypted laptops in an unlocked closet: SYNTHETIC REHEARSAL. Visitors and vendors near hallway workstations are rated under unauthorized physical access and visible screens, where visitor control and workstation security count as absent; the reachable closet is carried by the closet-laptop risk. Weight used in the rating (Part D): §164.310(a)(2)(iii) +1 (absent) in unauthorized physical access.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.310(d)(2)(iii)	The practice says this exposure remains: No record of the two closet laptops, the kiosk tablet, or what is on them.	Carried by lost or stolen device; two retired unencrypted laptops in an unlocked closet: SYNTHETIC REHEARSAL. Untracked devices are weighed in the lost-device rating, with the device inventory and movement-record steps; the retired closet laptops are carried by the closet-laptop risk, which records what they hold before disposal. (evidence: addressable-164.310(d)(2)(iii) (observed): no record of the closet laptops or the kiosk) Weight used in the rating (Part D): §164.310(d)(2)(iii) +1 (absent) in lost or stolen device.	A. Reviewer (SYNTHETIC), October 21, 2026

Area	Where	Established	Coverage review	Reviewer
Exposure the practice says remains	164.312(a)(2)(iii)	The practice says this exposure remains: Windows desktops, Gmail and eFax stay open on shared PCs; kiosk tablet stays signed in to athenaOne all day.	Carried by visible or unattended screens; waiting-room tablet signed in to the EHR all day: SYNTHETIC REHEARSAL. Open desktops, Gmail and eFax on shared PCs are rated under visible or unattended screens, where automatic logoff counts as absent; the kiosk signed in all day is carried by the kiosk risk. (evidence: addressable-164.312(a)(2)(iii) (observed): sessions stay open; kiosk signed in) Weight used in the rating (Part D): §164.312(a)(2)(iii) +1 (absent) in visible or unattended screens.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.312(a)(2)(iv)	The practice says this exposure remains: Office manager PC scan folder, the two closet laptops (contents unknown), copier drive, Gmail on personal phones.	Carried by lost or stolen device; disposal or reuse of equipment and media; two retired unencrypted laptops in an unlocked closet; texts and the practice Gmail app on unmanaged personal phones: SYNTHETIC REHEARSAL. Unencrypted PCs are weighed in the lost-device rating with the encryption step; the copier drive under disposal … Weight used in the rating (Part D): §164.312(a)(2)(iv) +1 (absent) in lost or stolen device.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.312(e)(2)(i)	The practice says this exposure remains: Practice cannot say whether interfaces are integrity-protected; no confirmation of eFax delivery integrity.	Carried by interception or misdirection in transit: SYNTHETIC REHEARSAL. Transmission integrity is weighed absent in the interception and misdirection rating, with the interface integrity step; the eFax delivery question is part of the same path. (evidence: addressable-164.312(e)(2)(i): interfaces and eFax integrity unknown) Weight used in the rating (Part D): §164.312(e)(2)(i) +1 (absent) in interception or misdirection in transit.	A. Reviewer (SYNTHETIC), October 21, 2026
Exposure the practice says remains	164.312(e)(2)(ii)	The practice says this exposure remains: SMS from personal phones to parents with child names; plain Gmail to parents with forms attached.	Carried by interception or misdirection in transit; texts and the practice Gmail app on unmanaged personal phones: SYNTHETIC REHEARSAL. Plain email to parents is rated under interception and misdirection, where encryption counts as absent, with the secure-channel step; texts naming children from personal phones are carried by the personal-phones risk. (evidence: addressable-164.312(e)(2)(ii): SMS with child names; plain Gmail to parents) Weight used in the rating (Part D): §164.312(e)(2)(ii) −0.4 (partly in place) in interception or misdirection in transit.	A. Reviewer (SYNTHETIC), October 21, 2026

Scope reconciliation. The record holds 17 confirmed flows of patient information, five suggested flows recorded as absent (each with its reason), no unresolved and no still suspected. Every suggested flow is settled, but four items about what a system holds remain open: Open item 3 (Physicians' personal laptops); Open item 4 (Old laptops in storage closet (2)); Open item 5 (Canon multifunction copier); Open item 8 (Staff personal phones) (Schedule H-7).

> Whether Old laptops in storage closet (2) holds or reaches patient information is not established. Assessed by A. Reviewer (SYNTHETIC) (October 21, 2026) as a limitation that does not invalidate this risk analysis: SYNTHETIC REHEARSAL. Two retired pre-2019 laptops whose contents nobody knows; they are analyzed under the disposal and lost-device threats and carried by the closet-laptop risk, whose step establishes what they hold.

21 items remain open in the unresolved-items register, 15 of them material; each is listed in Schedule H-7 with its owner and the evidence that settles it, and the material ones also in Part A.

G. Risk treatment plan

The steps below are grouped by phase and, within a phase, ordered by remediation priority and then by assessed risk. Priority reflects the obligation, the risk and ePHIShield's professional judgment; it is a separate measure from the level of risk. Implementing the plan is the practice's responsibility.

Steps are grouped by what they do: immediate containment of an established, urgent exposure; near-term correction; and longer-term work. Steps that verify what is not yet established are listed separately. Where no reviewer set a timeframe, the one shown is ePHIShield's default, marked “default”: 3 days for immediate containment, otherwise the sooner of the step's priority (Critical 30 days, High 90 days, Medium 6 months, Low 12 months) and the level of the risk it treats (Very High 30 days, High 60 days, Moderate 6 months, Low 12 months). These are ePHIShield's recommendations, not HIPAA deadlines; a deadline the law itself sets, such as breach notification, is stated with the step it applies to.

Immediate containment

Item	Requirement	Action	Priority	Timeframe	Risks treated
1	§164.308(a)(3)(ii)(C)	Immediately disable any active account belonging to a former workforce member and review access logs for that account. (Immediate: set by ePHIShield's reviewer.) Asset: athenaOne. Owner: Office manager (athenaOne practice admin). Verify with: Reprinted athenaOne user list, dated today, showing the departed MA's account disabled. Why: It reduces access retained after someone leaves: The practice reported that this specification is not implemented as written. Basis: §164.308(a)(3)(ii)(C) (addressable implementation specification; Not Implemented). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: SYNTHETIC REHEARSAL. The printed athenaOne user list shows the MA who left in 2025-08 still active: disable that account today; the termination checklist is separate, near-term work (A. Reviewer (SYNTHETIC), 2026-10-21).	Critical	same day (ePHIShield target)	Access retained after someone leaves
2	Risk management (§164.308(a)(1)(ii)(B)); §164.308(b)(1); §164.308(b)(3); §164.314(a)(1); §164.314(a)(2)(i)	Accept Google's Workspace business associate agreement in the admin console (a same-day administrator action). This is also Google's part of the agreement project in Items 20 to 24. (Immediate: set by ePHIShield's reviewer.) Asset: Google Workspace email. Owner: Office manager (acting security lead). Verify with: A screenshot of the Workspace admin console showing the agreement accepted, dated the same day. Why: It reduces patient information kept by services with no agreement on record: Google's Workspace BAA was not accepted in the admin console; no eFax or Valley agreement was produced when requested on site, and whether one exists is not established. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	Critical	same day where feasible (ePHIShield target)	Patient information kept by services with no agreement on record

Item	Requirement	Action	Priority	Timeframe	Risks treated
3	Risk management (§164.308(a)(1)(ii)(B))	Today: turn off TeamViewer's unattended access on the office manager PC, so no session can start without someone at the PC accepting it. (Immediate: set by ePHIShield's reviewer.) Asset: Office manager PC. Owner: Office manager. Verify with: Dated screenshot of TeamViewer's settings on the office manager PC showing unattended access off, or the program uninstalled. Why: It reduces unattended personal remote-access tool on the office PC: A personal-edition TeamViewer allows unattended access at any time with a fixed password and no second factor; the helper has no written agreement or BAA, and no one reviews its sign-ins. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	same day where feasible (ePHIShield target)	Unattended personal remote-access tool on the office PC
4	Risk management (§164.308(a)(1)(ii)(B))	Today: sign the front-desk account out of the check-in tablet and change that account's password, which is on the sticky note. (Immediate: set by ePHIShield's reviewer.) Asset: Check-in kiosk tablet. Owner: Office manager (athenaOne practice admin). Verify with: athenaOne session or user view showing the tablet signed out, and the date of the password change. Why: It reduces waiting-room tablet signed in to the EHR all day: The tablet stays signed in to athenaOne under a front-desk staff account with full front-desk access, unattended in the waiting room. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	same day where feasible (ePHIShield target)	Waiting-room tablet signed in to the EHR all day
5	Risk management (§164.308(a)(1)(ii)(B))	Today: lock the storage closet, or move both retired laptops to a locked cabinet, and note who holds the key. (Immediate: set by ePHIShield's reviewer.) Asset: Old laptops in storage closet (2). Owner: Office manager. Verify with: Same-day photo of the locked closet or cabinet. Why: It reduces two retired unencrypted laptops in an unlocked closet: Retired, unencrypted, untracked, contents unknown, in an unlocked closet that vendors and visitors can reach; no disposal process. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	same day where feasible (ePHIShield target)	Two retired unencrypted laptops in an unlocked closet

Item	Requirement	Action	Priority	Timeframe	Risks treated
6	Risk management (§164.308(a)(1)(ii)(B))	Today: write down what the office manager knows of the 2025 misdirected fax (what the form held, when it was learned of, who received it and what they said) and open the §164.402 assessment with counsel. (Immediate: set by ePHIShield's reviewer.) Asset: eFax Corporate. Owner: Office manager (acting security lead), with counsel. Verify with: The dated written account of the 2025 fax and the opened assessment file the same day. Why: It reduces misdirected fax never assessed; no working incident procedure: The binder's incident procedure is an uncustomized template with no names or contacts, and no one is named to decide whether an event is a breach; the 2025 misfax was not recorded or assessed. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	same day where feasible (ePHIShield target)	Misdirected fax never assessed; no working incident procedure
7	Risk management (§164.308(a)(1)(ii)(B))	Today: take down the sticky note and the whiteboard password, and change the posted Windows password, the Wi-Fi password and the alarm code; give staff the new ones in person. (Immediate: set by ePHIShield's reviewer.) Asset: Comcast Business gateway and Wi-Fi. Owner: Office manager. Verify with: Same-day photo of the cleared front desk and whiteboard and a dated note of the Windows, Wi-Fi and alarm code changes. Why: It reduces shared physical and network secrets never changed: One alarm code known to all staff, the cleaning crew and the landlord, never changed after departures. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	same day where feasible (ePHIShield target)	Shared physical and network secrets never changed

Same day, not containment: the step every later item depends on

Item	Requirement	Action	Priority	Timeframe	Risks treated
8	§164.308(a)(2)	Designate a named security official in writing with defined responsibility, authority, and allocated time for the HIPAA security program. (Immediate: every other step in this plan needs an accountable owner, so the designation comes first.) Asset: The written designation of the security official. Owner: The practice's leadership (the owners or managing physician). Verify with: The signed, dated written designation of the security official, with the responsibilities and time allotted. Why: The practice answered no to “Assignment is documented in writing”; a compliance requirement with no rated risk. Basis: §164.308(a)(2) (standard; Not Implemented).	High	same day where feasible (ePHIShield target)	Compliance requirement; no rated risk

Near-term correction

Item	Requirement	Action	Priority	Timeframe	Risks treated
9, 10, 11	§164.308(a)(3)(ii)(C); §164.308(a)(3)(i); §164.308(a)(4)(ii)(C)	One access-review routine, with each obligation kept: (1) Define access levels by job role, document the role-to-permission mapping, and reconcile system user lists against current staff at least quarterly [§164.308(a)(3)(i)] (2) Adjust and document system access at every role change, and perform a periodic documented review of all user rights [§164.308(a)(4)(ii)(C)] (3) Implement a written termination checklist covering all system accounts, email, remote access, physical keys and codes, and device return, completed and signed on the final day of work [§164.308(a)(3)(ii)(C)]. One owner runs it; the same user lists serve each part. Items 9, 11 are part of this step (one piece of work). The text above includes the work of Items 9 (§164.308(a)(3)(i)), 11 (§164.308(a)(4)(ii)(C)). Asset: athenaOne, Gmail, eFax and Windows accounts; alarm codes and keys. Owner: Office manager (acting security lead). Verify with: The adopted termination checklist and the first completed, signed one. Why: It reduces access retained after someone leaves and inappropriate access by a staff member: The practice reported that this specification is not implemented as written. Basis: §164.308(a)(3)(ii)(C) (addressable implementation specification; Not Implemented), §164.308(a)(3)(i) (standard; Partially Implemented), §164.308(a)(4)(ii)(C) (addressable implementation specification; Not Implemented). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: Departures are handled from memory and the departed MA's athenaOne account was still active on the printed user list: the checklist is the prerequisite for removing every account, code and key, and it treats several risks (departed-staff access, shared sign-in, insider misuse) (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8.	Critical	30 days (ePHIShield target)	Access retained after someone leaves; Inappropriate access by a staff member

Item	Requirement	Action	Priority	Timeframe	Risks treated
12, 13	§164.308(a)(5)(ii)(B); Risk management (§164.308(a)(1)(ii)(B))	Close the gaps in the existing endpoint protection (Windows Defender (built-in)): confirm it is running on every device that accesses ePHI, and extend it where it is not; make sure its alerts reach a named person who acts on them; reconcile its coverage with the device inventory. The same work also completes: (13) Confirm whether the existing endpoint protection (Windows Defender (built-in)) includes behavior-based detection and response on every practice machine, and add it only where it does not. Asset: Practice PCs (front desk, exam room, office manager). Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: Get-MpComputerStatus output for every practice PC, and the name of the person who receives Defender alerts. Why: It reduces ransomware and exploited unpatched or unsupported systems: The practice reported that this specification is not implemented as written. Basis: §164.308(a)(5)(ii)(B) (addressable implementation specification; Partially Implemented). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: Built-in Defender's coverage is unknown and no one sees its alerts, an immediate exposure on every office PC while ransomware is rated High and the Windows 10 PC is past support (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8.	Critical	30 days (ePHIShield target)	Ransomware; Exploited unpatched or unsupported systems

Item	Requirement	Action	Priority	Timeframe	Risks treated
14, 15, 17	§164.312(a)(2)(i); §164.312(a)(1); §164.312(d)	Make every user of every ePHI system uniquely identified where the ePHI is reached: give each person their own account, or put any shared device log-in behind an application sign-in that identifies each person individually. Still needed at: athenaOne (only its shared login on the Check-in kiosk tablet); Google Workspace email; eFax Corporate; Front desk PC 1; Front desk PC 2; Exam room PCs (4); Check-in kiosk tablet; Canon multifunction copier. Items 14, 17 are part of this step (one piece of work). The text above includes the work of Items 14 (§164.312(a)(1)), 17 (§164.312(d)). Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: User lists for each listed system showing one named account per person. Why: It reduces shared sign-in without individual attribution, inappropriate access by a staff member, phishing and stolen email credentials, ransomware and exploited unpatched or unsupported systems: The practice answered no to “Inside that system, each person still signs in with their own credentials, so access to the patient information is attributed to a named person”. Basis: §164.312(a)(2)(i) (required implementation specification; Partially Implemented), §164.312(d) (standard; Partially Implemented), §164.312(a)(1) (standard; Partially Implemented). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: Shared accounts are in use today on the systems listed, including the waiting-room kiosk; this step treats several risks (shared sign-in, kiosk, insider misuse, departed-staff access) (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8.	Critical	30 days (ePHIShield target)	Inappropriate access by a staff member; Shared sign-in without individual attribution; Exploited unpatched or unsupported systems; Phishing and stolen email credentials; Ransomware

Item	Requirement	Action	Priority	Timeframe	Risks treated
16	§164.312(a)(2)(iv)	Encrypt all office PCs, verify coverage against the device inventory and keep the evidence. Old laptops in storage closet (2) is retired: secure it now, then wipe or destroy it under the disposal step. Physicians' personal laptops are not managed by the practice: practice-wide encryption is not credited there. Either bring them under management with encryption enforced, or prohibit storing or downloading ePHI on them and obtain each user's signed attestation. Asset: Old laptops in storage closet (2); Physicians' personal laptops; all office PCs. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: manage-bde -status output for each office PC showing BitLocker on. Why: It reduces lost or stolen device: The practice reported that this specification is not implemented as written. Basis: §164.312(a)(2)(iv) (addressable implementation specification; Not Implemented). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: No office PC is encrypted and the closet laptops and office PCs are reachable today by vendors left alone and by the cleaning crew; this step treats several risks (lost device, disposal, physical access) (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8.	Critical	30 days (ePHIShield target)	Lost or stolen device

Item	Requirement	Action	Priority	Timeframe	Risks treated
18, 19	Risk management (§164.308(a)(1)(ii)(B))	Turn on athenaOne MFA for every user and enforce Google 2-step verification. The same work also completes: (18) Keep the second factor already in use, and extend it to the paths that reach ePHI from outside the office, through email or through a vendor's access and still sign in with a password alone. Sign-in at in-office workstations to on-premises systems is not included. Asset: athenaOne. Owner: Office manager (athenaOne practice admin), with the computer helper for Google (the independent computer helper only once a written agreement is in place). Verify with: athenaOne user security settings showing MFA for every user, and the Google Admin page showing 2-step verification enforced. Why: It reduces password-only remote access to athena and Gmail, phishing and stolen email credentials and ransomware: athena MFA is on only for the office manager's admin account; physicians use personal laptops with a password only, and Google 2-step verification is not enforced. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer; also completes §164.312(d). Priority: Critical rather than the High risk's default (High), on the reviewer's documented basis: Password-only sign-in from personal home laptops to the whole chart is an immediate exposure today; the second factor is the prerequisite for every other remote-access measure (A. Reviewer (SYNTHETIC), 2026-10-21).	Critical	30 days (ePHIShield target)	Password-only remote access to athena and Gmail; Phishing and stolen email credentials; Ransomware

20, 21, 22, 23, 24	§164.308(b)(1); §164.308(b)(3); §164.314(a)(1); §164.314(a)(2)(i); Risk management (§164.308(a)(1)(ii)(B))	Execute a business associate agreement with Tri-State Office Systems (SYNTHETIC) (none is in place). Until each is executed, stop or limit what ePHI reaches that vendor. Google's agreement is the work of Item 2 and is not repeated here. If the support of Kyle Pruitt (SYNTHETIC), independent computer helper continues, execute an agreement before any further access to ePHI; if the support ends, end the access instead. Each new or replacement agreement contains the terms §164.314(a)(2)(i) requires: the business associate complies with the applicable requirements of the Security Rule, ensures that its subcontractors that handle ePHI agree to the same, and reports to the practice any security incident of which it becomes aware, including breaches of unsecured protected health information as §164.410 requires (ePHIShield recommends a reporting period of no more than five calendar days). The executed agreement with athenahealth, read and found to contain the required terms, stands; it is not re-executed. Keep a register reconciling every vendor with ePHI access to its executed agreement. For eFax (Consensus Cloud Solutions) and Valley After-Hours Answering (SYNTHETIC): obtain the executed business associate agreement with eFax (Consensus Cloud Solutions) and Valley After-Hours Answering (SYNTHETIC) (none was produced when requested; whether one exists is not established); where none exists, execute one before any further disclosure. Items 21, 22, 23, 24 are part of this step (one piece of work); their requirements are listed at left. (24) Stop placing new patient information in a service with no agreement until it has one: [Google: see Item 2]; obtain the eFax and Valley agreements, or move faxing to a plan that carries one and route after-hours messages to an address covered by one. The agreement step in the plan remains the contractual record; this step limits what reaches the services until then. Asset: Tri-State Office Systems (SYNTHETIC); Kyle Pruitt (SYNTHETIC), independent computer helper. Owner: Office manager. Verify with: A signed agreement (or the vendor's accepted standard agreement) for Tri-State Office Systems (SYNTHETIC) and Kyle Pruitt (SYNTHETIC), independent computer helper, each dated and filed with the practice's records; for Google, the dated record filed under Item 2; for eFax (Consensus Cloud Solutions) and Valley After-Hours Answering	Critical	30 days (ePHIShield target)	Vendor compromise (contractual assurance; it does not lower the rating); Patient information kept by services with no agreement on record (contractual assurance; it does not lower the rating)

Item	Requirement	Action	Priority	Timeframe	Risks treated
		(SYNTHETIC), the executed agreement or the practice's dated record that none exists and what was done instead. Why: It reduces patient information kept by services with no agreement on record: The practice answered no to “A signed agreement exists for every vendor listed”. Basis: §164.308(b)(1) (standard; Partially Implemented), §164.308(b)(3) (required implementation specification; Partially Implemented), §164.314(a)(1) (standard; Partially Implemented), §164.314(a)(2)(i) (required implementation specification; Partially Implemented); contractual compliance, not a fix for a security-compromise risk. Priority: Critical rather than the Moderate risk's default (Medium), on the reviewer's documented basis: A written business associate contract is a statutory requirement before disclosure continues (§164.308(b)(1), §164.502(e)); patient information is already held every day by services with no agreement (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8; Item 2.			
25	§164.308(a)(1)(ii)(A)	Adopt this assessment as the practice's documented risk analysis: review it, record the practice's acceptance and the date, and act on the risk management steps it identifies. Asset: This risk analysis. Owner: The physicians (practice owners), with the office manager. Verify with: The practice's dated, signed acceptance of this risk analysis. Why: The practice answered no to “A risk analysis has been performed”; a compliance requirement with no rated risk. Basis: §164.308(a)(1)(ii)(A) (required implementation specification; Not Implemented).	Critical	30 days (ePHIShield target)	Compliance requirement; no rated risk
26	§164.308(a)(1)(ii)(B)	Maintain a risk management plan that assigns an owner and target date to every risk rated Moderate or higher and records the decision when a risk is accepted. Asset: This report's risk register. Owner: Office manager (acting security lead). Verify with: A risk register listing each Moderate or higher risk in this report with its owner and target date. Why: Part of this was established and part was not; still outstanding: Workstations are kept updated; a compliance requirement with no rated risk. Basis: §164.308(a)(1)(ii)(B) (required implementation specification; Not Implemented). After: Item 8.	Critical	30 days (ePHIShield target)	Compliance requirement; no rated risk

Item	Requirement	Action	Priority	Timeframe	Risks treated
27	§164.308(a)(1)(ii)(C)	Adopt a written sanction policy that expressly covers security policy violations, obtain signed workforce acknowledgement, and retain the acknowledgements. Asset: The sanction policy (all workforce members). Owner: Office manager. Verify with: The adopted sanction policy and the signed workforce acknowledgements. Why: It reduces inappropriate access by a staff member: The practice answered no to “Staff have been informed of it”. Basis: §164.308(a)(1)(ii)(C) (required implementation specification; Not Implemented). Retention, as the Rule states it: §164.316(b)(2)(i): “Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.”	High	60 days (ePHIShield target)	Inappropriate access by a staff member
28, 31	§164.308(a)(1)(ii)(D); §164.308(a)(5)(ii)(C)	Establish a documented schedule for reviewing EHR access reports and system security logs, naming the reviewer, the frequency, and how exceptions are escalated and recorded. The same work also completes: (31) Enable and review failed log-in and impossible-travel alerting for email, remote access, and the EHR, and define who receives and acts on the alerts. Asset: Activity records of athenaOne and Google Workspace email. Owner: Office manager (acting security lead). Verify with: The written review schedule and the first dated review record (who reviewed which report and what was found). Why: It reduces exploited unpatched or unsupported systems, inappropriate access by a staff member, access retained after someone leaves, shared sign-in without individual attribution and phishing and stolen email credentials: The practice answered no to “Somebody reviews access or security reports”. Basis: §164.308(a)(1)(ii)(D) (required implementation specification; Not Implemented), §164.308(a)(5)(ii)(C) (addressable implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Inappropriate access by a staff member; Access retained after someone leaves; Shared sign-in without individual attribution; Exploited unpatched or unsupported systems; Phishing and stolen email credentials

Item	Requirement	Action	Priority	Timeframe	Risks treated
29	§164.308(a)(5)(i)	Train the workforce members not yet trained (0 of 7 are recorded as trained) before they next reach ePHI, keep completion records with the security documentation, and continue training periodically (the rule sets no frequency; ePHIShield recommends at least annually). Asset: Security training for all workforce members. Owner: Office manager. Verify with: Training completion records for every workforce member, with dates. Why: It reduces phishing and stolen email credentials and ransomware: The practice answered no to “Every workforce member receives training” and “Completion records are kept”. Basis: §164.308(a)(5)(i) (standard; Not Implemented).	High	60 days (ePHIShield target)	Phishing and stolen email credentials; Ransomware
30	§164.308(a)(5)(ii)(A)	Send brief recurring security reminders — at minimum quarterly — covering current threats such as phishing and device loss, and retain a copy of each. Asset: Security reminders to the workforce. Owner: Office manager. Verify with: Copies of the security reminders sent, with their dates. Why: It reduces phishing and stolen email credentials: The practice reported that this specification is not implemented as written. Basis: §164.308(a)(5)(ii)(A) (addressable implementation specification; Not Implemented). Retention: §164.316(b)(2)(i), quoted under Item 27.	High	60 days (ePHIShield target)	Phishing and stolen email credentials
32	§164.308(a)(6)(ii)	Maintain a security incident log recording each suspected or known incident, the response taken, the mitigation, and the outcome, retained for six years (§164.316(b)(2)(i)). Asset: The security incident log. Owner: Office manager (acting security lead). Verify with: The incident log, with the entries recorded since it was started. Why: It reduces ransomware: The practice answered no to “An incident log exists” and “Outcomes are recorded for each entry”. Basis: §164.308(a)(6)(ii) (required implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Ransomware

Item	Requirement	Action	Priority	Timeframe	Risks treated
33	§164.308(a)(7)(i)	Develop a written contingency plan covering data backup, disaster recovery, and emergency mode operation for every system that holds ePHI. Asset: Gmail, the eFax account and the office manager PC's Scans folder; athenaOne downtime. Owner: Office manager (acting security lead). Verify with: The written contingency plan, dated. Why: It reduces ransomware and fire, flood, storm or power loss: The standard is not fully met because §164.308(a)(7)(ii)(A) (Data backup plan); §164.308(a)(7)(ii)(B) (Disaster recovery plan); §164.308(a)(7)(ii)(C) (Emergency mode operation plan) are established deficiencies. Basis: §164.308(a)(7)(i) (standard; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Ransomware; Fire, flood, storm or power loss

Item	Requirement	Action	Priority	Timeframe	Risks treated
34, 35, 36, 37	§164.308(a)(7)(ii)(A); Risk management (§164.308(a)(1)(ii)(B)); §164.308(a)(7)(ii)(B)	Back up every system holding ePHI on an automated schedule, and verify that a restore actually works. The same work also completes: (35) Keep a copy that ransomware on the office network cannot alter or delete, sized to what is at risk: for Office manager PC (Scans folder), a versioned or offline copy; for Google Workspace email and eFax Corporate, the service's own retention or a separate cloud backup; and test a restore from it. (36) Perform and document a full restoration test at least annually, recording elapsed time and data integrity, and compare the result to the practice's tolerable downtime. (37) Write down the procedure for restoring lost data: which systems and backups it covers, who performs the restore and how to reach them, and the steps in order. Keep a copy where it can be reached when the practice's systems are down. Asset: Google Workspace email; eFax Corporate; Office manager PC (Scans folder). Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: Backup job report covering Gmail, the eFax account and the Scans folder; and a dated restore test record with the elapsed time and what was checked (the record shows no restore tested). Why: It reduces ransomware, fire, flood, storm or power loss and permanent data loss: Part of this was established and part was not; still outstanding: How often, What is backed up, Backups are encrypted and Where backups are stored. Basis: §164.308(a)(7)(ii)(A) (required implementation specification; Not Implemented), §164.308(a)(7)(ii)(B) (required implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Ransomware; Fire, flood, storm or power loss; Permanent data loss

Item	Requirement	Action	Priority	Timeframe	Risks treated
38, 41	§164.310(d)(1); §164.310(d)(2)(iii)	Maintain a device inventory covering every asset that stores or accesses ePHI, with assignment, encryption status, and disposition recorded, and list in it every system, service and device that stores or transmits ePHI, with an owner and a review date (the written ePHI asset inventory). The same work also completes: (41) Record device assignment and any transfer between staff or locations, including the responsible individual and date. Asset: Devices and media holding ePHI: Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet, Staff personal phones, Physicians' personal laptops, Old laptops in storage closet (2) and Canon multifunction copier. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The updated device inventory, dated. Why: It reduces lost or stolen device and two retired unencrypted laptops in an unlocked closet: The practice answered no to “A device list was provided”, “Imaging or diagnostic equipment storing ePHI” and “Backup drives, USB media, external storage”. Basis: §164.310(d)(1) (standard; Not Implemented), §164.310(d)(2)(iii) (addressable implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Two retired unencrypted laptops in an unlocked closet; Lost or stolen device

Item	Requirement	Action	Priority	Timeframe	Risks treated
39	§164.310(d)(2)(i)	Adopt a media disposal procedure requiring verified destruction or cryptographic erasure of every device that held ePHI, including leased copiers at end of term, with certificates retained. For personal devices the practice does not own (Staff personal phones and Physicians' personal laptops), the step is removal of practice data (a selective wipe of the practice's managed apps where available) with the owner's signed attestation, not destruction or a certificate. Asset: Practice devices and media holding ePHI: Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet and Canon multifunction copier. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The adopted disposal procedure and the destruction or wipe certificate for each device disposed of; for a personal device, the owner's signed attestation that practice data was removed. Why: It reduces disposal or reuse of equipment and media and two retired unencrypted laptops in an unlocked closet: The practice answered no to “A disposal process exists”. 1 point was confirmed by direct observation. Basis: §164.310(d)(2)(i) (required implementation specification; Not Implemented). After: Item 8. Retention: §164.316(b)(2)(i), quoted under Item 27.	High	60 days (ePHIShield target)	Two retired unencrypted laptops in an unlocked closet; Disposal or reuse of equipment and media
40	§164.310(d)(2)(ii)	Require documented wipe or reimage of any device before reassignment to another user. Asset: Practice devices and media holding ePHI: Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet and Canon multifunction copier. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The reuse procedure and the wipe record for the last reassigned device. Why: It reduces disposal or reuse of equipment and media: The practice described measures for this requirement but produced no supporting documentation. Basis: §164.310(d)(2)(ii) (required implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Disposal or reuse of equipment and media

Item	Requirement	Action	Priority	Timeframe	Risks treated
42	§164.312(a)(2)(iv)	Require encryption and passcode enforcement on all mobile devices that access ePHI, or prohibit such access. Asset: Mobile phones that reach ePHI. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The device management report showing encryption and passcode enforcement on each phone, or the written prohibition. Why: It reduces lost or stolen device: The practice reported that this specification is not implemented as written. Basis: §164.312(a)(2)(iv) (addressable implementation specification; Not Implemented). After: Item 8.	High	60 days (ePHIShield target)	Lost or stolen device
43, 45	§164.312(e)(2)(ii); §164.312(e)(1)	Keep the encryption already in use (athena in the browser (https)) and close the paths still unprotected: Text messages from personal phones; Gmail to parents whose email provider may not support TLS; fax leg to recipient. For each, encrypt it or send it through the patient portal or another encrypted channel, or document why encryption is not reasonable and appropriate for that path. Item 43 is part of this step (one piece of work): (43) Protect ePHI on the paths still unprotected (Text messages from personal phones; Gmail to parents whose email provider may not support TLS; fax leg to recipient) by encryption, the patient portal or another encrypted channel where that is reasonable and appropriate; a path left as it is has its documented reason. This does not require routing every external transmission through the portal. Asset: External transmissions of ePHI (email, portal, fax and texts). Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The setting or written instruction for each path named (encrypted email, portal use, fax handling). Why: It reduces interception or misdirection in transit: The practice reported that this specification is not implemented as written. Basis: §164.312(e)(2)(ii) (addressable implementation specification; Partially Implemented), §164.312(e)(1) (standard; Not Implemented). Removed under Item 50, so not kept here: Gmail between Google servers. Removed under Item 47, so not kept here: TeamViewer. After: Item 8.	High	60 days (ePHIShield target)	Interception or misdirection in transit

Item	Requirement	Action	Priority	Timeframe	Risks treated
46	Risk management (§164.308(a)(1)(ii)(B)); network separation, not transmission encryption	Separate the guest wireless network from the network carrying practice systems, so that a guest device cannot reach clinical equipment. Asset: The guest wireless network. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The wireless controller or firewall configuration showing the guest network isolated, or a test from a guest device. Why: It reduces ransomware and exploited unpatched or unsupported systems: The practice reported that this specification is not implemented as written. Basis: §164.312(e)(2)(ii) (addressable implementation specification; Partially Implemented). After: Item 8.	High	60 days (ePHIShield target)	Ransomware; Exploited unpatched or unsupported systems
47	Risk management (§164.308(a)(1)(ii)(B))	Remove the personal-edition TeamViewer and review its connection log for sessions the helper did not make; if outside support continues, put it under a written agreement and BAA and use an attended remote tool with a second factor. Asset: Office manager PC. Owner: Office manager, with the computer helper (the independent computer helper only once a written agreement is in place). Verify with: The program uninstalled from every practice PC (dated screenshot of installed programs), the dated note of the connection-log review, and any continuing remote support under a written agreement with a named account and a second factor. Why: It reduces unattended personal remote-access tool on the office PC: A personal-edition TeamViewer allows unattended access at any time with a fixed password and no second factor; the helper has no written agreement or BAA, and no one reviews its sign-ins. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	60 days (ePHIShield target)	Unattended personal remote-access tool on the office PC

Item	Requirement	Action	Priority	Timeframe	Risks treated
48	Risk management (§164.308(a)(1)(ii)(B))	Replace or upgrade the Windows 10 PC. Until it is replaced, use it only for athenaOne in the browser, have Defender's status on it confirmed, and route its Defender alerts to a named person. Asset: Front desk PC 2. Owner: Office manager (acting security lead); the computer helper only once a written agreement is in place. Verify with: A screenshot of the front-desk PC's Windows version after the upgrade or the replacement invoice, and the shared local-administrator account removed. Why: It reduces front-desk PC running Windows 10 past end of support: Windows 10 reached end of support on October 14, 2025. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer. After: Item 8.	High	60 days (ePHIShield target)	Front-desk PC running Windows 10 past end of support
49	Risk management (§164.308(a)(1)(ii)(B))	Take the front-desk staff account off the tablet: use it only for a check-in arrangement that cannot reach other patients' records (ask athena what it offers), or remove the tablet from the waiting room. Asset: Check-in kiosk tablet. Owner: Office manager (athenaOne practice admin). Verify with: The check-in tablet configured so it cannot show the record system unattended (kiosk mode or a check-in account limited to check-in), shown by a dated screenshot of its settings and of the athena role it uses, or the tablet removed from the waiting room. Why: It reduces waiting-room tablet signed in to the EHR all day: The tablet stays signed in to athenaOne under a front-desk staff account with full front-desk access, unattended in the waiting room. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer.	High	60 days (ePHIShield target)	Waiting-room tablet signed in to the EHR all day

Item	Requirement	Action	Priority	Timeframe	Risks treated
50	Risk management (§164.308(a)(1)(ii)(B))	Move appointment messaging to athena's patient messaging or a practice-managed number; until then, no child names in texts and send only to the number of the parent or guardian on file in athena. Remove the practice Gmail account from personal phones, or allow it only on phones with a passcode, encryption and remote wipe enforced through Google Workspace's basic mobile management; have departing staff delete parent threads and sign out of the practice mailbox, with a signed attestation. Asset: Staff personal phones. Owner: Office manager (acting security lead), with the physicians. Verify with: The written texting rule acknowledged by each staff member; the Google Workspace device list showing which phones hold the practice mailbox and that passcode, encryption and remote wipe are enforced (or the account removed); a dated list of staff phones (or texting moved to the athena patient messaging). Why: It reduces texts and the practice Gmail app on unmanaged personal phones: Staff text parents from personal phones with no MDM and no remote wipe, and the inventory records the practice Gmail app on the same phones; their encryption and passcodes are not known. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer. After: Item 8.	High	60 days (ePHIShield target)	Texts and the practice Gmail app on unmanaged personal phones
51	Risk management (§164.308(a)(1)(ii)(B))	Have an IT provider under a written agreement inspect each laptop offline and record what it holds (a dated record); then wipe or destroy both with a certificate and record their disposal. They are not to be returned to use. Asset: Old laptops in storage closet (2). Owner: Office manager (acting security lead); an IT provider under a written agreement, once engaged. Verify with: The dated inspection record and the destruction or wipe certificate. Why: It reduces two retired unencrypted laptops in an unlocked closet: Retired, unencrypted, untracked, contents unknown, in an unlocked closet that vendors and visitors can reach; no disposal process. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer. After: Item 8; Item 20.	High	60 days (ePHIShield target)	Two retired unencrypted laptops in an unlocked closet

Item	Requirement	Action	Priority	Timeframe	Risks treated
52, 53	§164.308(a)(5)(ii)(D); Good practice (no requirement)	Adopt a written password standard for the practice (keep the password rules athenahealth enforces in athenaOne; set length, no reuse and a change on any suspected compromise for Windows, email and the other accounts the practice controls), apply it on every system, and stop shared or posted credentials, which the record shows are in use. The same work also completes: (53) Provide a password manager so staff can hold distinct, strong passwords without writing them down. Asset: Passwords for athenaOne and Google Workspace email and the workstations. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The written password standard and each system's password settings (screenshot or export). Why: It reduces shared physical and network secrets never changed: Asked “Do any staff share passwords or write them where others can see them?”, the practice answered yes. Basis: §164.308(a)(5)(ii)(D) (addressable implementation specification; Not Implemented). Priority: High rather than the Moderate risk's default (Medium), on the reviewer's documented basis: SYNTHETIC REHEARSAL. Shared and posted passwords were observed. The same-day removal and change of the posted passwords is the containment of the shared-secrets and kiosk risks; this step is the near-term work of applying password rules on every system (A. Reviewer (SYNTHETIC), 2026-10-21). After: Item 8.	High	90 days (ePHIShield target)	Shared physical and network secrets never changed
54	§164.308(a)(7)(ii)(C)	Document emergency mode operating procedures, including downtime forms, controlled use of personal devices, and the process for reconciling paper records into the EHR after recovery. Asset: The contingency plan covering athenaOne and Google Workspace email. Owner: Office manager. Verify with: The written emergency mode procedure and the downtime forms. Why: It reduces fire, flood, storm or power loss: The practice described measures for this requirement but produced no supporting documentation. Basis: §164.308(a)(7)(ii)(C) (required implementation specification; Not Implemented).	High	90 days (ePHIShield target)	Fire, flood, storm or power loss

Item	Requirement	Action	Priority	Timeframe	Risks treated
55, 61	Risk management (§164.308(a)(1)(ii)(B)); §164.310(a)(1)	Issue individual alarm codes and remove the codes of the cleaning crew and former staff where the panel allows; change the gateway's admin password; replace the copier's stored Gmail app password with a scan-only account; add code and password changes to the departure checklist. The same work also completes: (55) Maintain a current list of everyone holding keys, codes, or badges, recover access on departure, and change shared codes after any departure (ePHIShield also recommends at least annually). Asset: Comcast Business gateway and Wi-Fi. Owner: Office manager, with the computer helper (the independent computer helper only once a written agreement is in place). Verify with: The alarm panel code list, gateway admin page and copier scan settings. Why: It reduces shared physical and network secrets never changed, unauthorized physical access and two retired unencrypted laptops in an unlocked closet: One alarm code known to all staff, the cleaning crew and the landlord, never changed after departures. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer; also completes §164.310(a)(1). Priority: High rather than the Moderate risk's default (Medium), on the reviewer's documented basis: The posted and shared secrets were observed in use; after the same-day change, the remaining work treats several risks (kiosk, physical access, shared sign-in) (A. Reviewer (SYNTHETIC), 2026-10-21).	High	90 days (ePHIShield target)	Shared physical and network secrets never changed; Two retired unencrypted laptops in an unlocked closet; Unauthorized physical access
56	§164.310(a)(1)	Secure network and server equipment in a locked room or cabinet with access limited to named individuals. Asset: Network and server equipment and the room or cabinet that holds it. Owner: Office manager. Verify with: A photo of the locked room or cabinet and the list of who holds its key. Why: It reduces unauthorized physical access, shared physical and network secrets never changed and two retired unencrypted laptops in an unlocked closet: The practice described measures for this requirement but produced no supporting documentation. 2 points were confirmed by direct observation. Basis: §164.310(a)(1) (standard; Partially Implemented).	High	90 days (ePHIShield target)	Two retired unencrypted laptops in an unlocked closet; Shared physical and network secrets never changed; Unauthorized physical access

Item	Requirement	Action	Priority	Timeframe	Risks treated
57	§164.310(b)	Adopt a workstation use policy covering permitted functions, personal use, and the specific conditions for remote and personal-device access to ePHI. Asset: The workstation use policy (all workstations). Owner: Office manager (acting security lead). Verify with: The adopted workstation use policy and the signed acknowledgements. Why: It reduces visible or unattended screens: The practice described measures for this requirement but produced no supporting documentation. Basis: §164.310(b) (standard; Not Implemented). After: Item 8.	High	90 days (ePHIShield target)	Visible or unattended screens
58	§164.310(c)	Reposition or fit a privacy filter at: Front desk PC 1 and 2 monitors face the waiting room chairs; kiosk tablet in waiting area, and set and check a lock-when-leaving expectation. Asset: Front desk PC 1 and 2 monitors face the waiting room chairs; kiosk tablet in waiting area. Owner: Office manager. Verify with: A dated photo of each listed screen repositioned or fitted with a privacy filter. Why: It reduces unauthorized physical access and visible or unattended screens: The practice answered yes to “A screen showing ePHI is visible to patients or visitors”. Basis: §164.310(c) (standard; Not Implemented).	High	60 days (ePHIShield target)	Unauthorized physical access; Visible or unattended screens
59	§164.312(a)(2)(iii)	Configure automatic screen lock at or under 15 minutes on every workstation and enable EHR session timeout, with shorter intervals in patient-facing areas. Asset: Workstations and record-system sessions. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The screen lock or session timeout setting for each listed system (policy export or screenshot). Why: It reduces visible or unattended screens: The practice reported that this specification is not implemented as written. Basis: §164.312(a)(2)(iii) (addressable implementation specification; Not Implemented). After: Item 8.	High	90 days (ePHIShield target)	Visible or unattended screens

Item	Requirement	Action	Priority	Timeframe	Risks treated
60	Risk management (§164.308(a)(1)(ii)(B))	Complete and document the §164.402 assessment of the 2025 misdirected fax. An impermissible disclosure is presumed a breach unless a documented assessment shows a low probability that the information was compromised; the recipient's statement that the form was shredded is one factor. Whether notification is owed depends on that documented breach determination (§164.402(2)); it is not assumed here. If the assessment concludes the fax was a breach of unsecured protected health information, the periods run from discovery (§164.404(a)(2)), not from the assessment: notice to the individual without unreasonable delay and in no case later than 60 calendar days after discovery (§164.404(b)), except as provided in §164.412; for a breach involving less than 500 individuals, notice to the Secretary not later than 60 days after the end of the calendar year in which it was discovered (§164.408(c)); media notice applies only to a breach involving more than 500 residents of a State or jurisdiction (§164.406); and any state-law requirement counsel identifies. A spring 2025 discovery date would put both federal periods in the past, so any notice owed would be sent without further delay, as counsel advises. Then have staff check each fax number against the recipient's number on file before sending. Asset: eFax Corporate. Owner: Office manager (acting security lead), with counsel. Verify with: The signed §164.402 assessment. Why: It reduces misdirected fax never assessed; no working incident procedure: The binder's incident procedure is an uncustomized template with no names or contacts, and no one is named to decide whether an event is a breach; the 2025 misfax was not recorded or assessed. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer. Priority: High rather than the Moderate risk's default (Medium), on the reviewer's documented basis: The §164.402 breach risk assessment of the 2025 misdirected fax is a legal requirement that was never done; the notice periods in §164.404(b) run from discovery (A. Reviewer (SYNTHETIC), 2026-10-21). Treated under Item 64, not here: the incident procedure. After: Item 8.	High	30 days to complete the assessment (ePHIShield target)	Misdirected fax never assessed; no working incident procedure

Item	Requirement	Action	Priority	Timeframe	Risks treated
62	§164.308(a)(1)(ii)(A)	Retain the completed risk analysis and update it when systems, operations or risks change materially, reviewing it periodically (ePHIShield recommends at least annually). Asset: This risk analysis. Owner: Office manager (acting security lead). Verify with: The practice's written schedule for updating the risk analysis, with the date of the next review. Why: The practice answered no to “A risk analysis has been performed”; a compliance requirement with no rated risk. Basis: §164.308(a)(1)(ii)(A) (required implementation specification; Not Implemented). After: Item 8. Retention: §164.316(b)(2)(i), quoted under Item 27.	High	90 days (ePHIShield target)	Compliance requirement; no rated risk
63	Risk management (§164.308(a)(1)(ii)(B))	Keep the existing update routine (Windows does it automatically; Kyle checks when he comes in), record when each cycle is done, and bring workstations and network equipment into it. Asset: Systems to keep updated: Front desk PC 1, Front desk PC 2, Exam room PCs (4), Office manager PC, Check-in kiosk tablet, Canon multifunction copier and Comcast Business gateway and Wi-Fi. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: For each system, the date of its last update cycle (an update status report or console export). Why: It reduces exploited unpatched or unsupported systems: Part of this was established and part was not; still outstanding: Workstations are kept updated. Basis: §164.308(a)(1)(ii)(B) (required implementation specification; Not Implemented). After: Item 8.	High	90 days (ePHIShield target)	Exploited unpatched or unsupported systems

64, 65, 66, 67, 68	§164.308(a)(6)(i); Good practice (no requirement)	The practice reports that it has a written security incident procedure, but no copy has been verified. Obtain a dated copy and confirm it is the procedure in use; having one does not show that it is adequate. Then bring it up to date: name who receives reports and who decides; replace the contacts that are no longer current; tell staff to preserve an affected system rather than wipe or reimage it, unless harm is still occurring; state when to involve legal counsel and, if the practice holds cyber insurance, its carrier; keep a contact list (IT support, the record system vendor, legal counsel, and the cyber insurance carrier if the practice has a policy) where it can be reached when systems are down; add a section that sets out the breach risk assessment of §164.402 for any impermissible use or disclosure, and the notification periods the law sets if a breach of unsecured protected health information is found: notice to each affected individual without unreasonable delay and in no case later than 60 calendar days after discovery (§164.404(b)), except as provided in §164.412; notice to prominent media outlets for a breach involving more than 500 residents of a State or jurisdiction (§164.406); and notice to the Secretary, contemporaneously with the individual notices for a breach involving 500 or more individuals (§164.408(b)), otherwise not later than 60 days after the end of each calendar year, for breaches discovered during the preceding calendar year (§164.408(c)); review it at least annually (ePHIShield's recommendation) and brief staff on it. If no written procedure can be produced, adopt one that covers identifying, responding to, mitigating and documenting incidents; names who receives reports and who decides; tells staff to preserve an affected system rather than wipe it, unless harm is still occurring; states when to involve legal counsel and, if the practice holds cyber insurance, its carrier; sets out the breach risk assessment of §164.402 for any impermissible use or disclosure, and the notification periods the law sets if a breach of unsecured protected health information is found: notice to each affected individual without unreasonable delay and in no case later than 60 calendar days after discovery (§164.404(b)), except as provided in §164.412; notice to prominent media outlets for a breach involving more than 500 residents of a State or jurisdiction	High	90 days (ePHIShield target)	Misdirected fax never assessed; no working incident procedure

Item	Requirement	Action	Priority	Timeframe	Risks treated
		(§164.406); and notice to the Secretary, contemporaneously with the individual notices for a breach involving 500 or more individuals (§164.408(b)), otherwise not later than 60 days after the end of each calendar year, for breaches discovered during the preceding calendar year (§164.408(c)); and keeps a contact list (IT support, the record system vendor, legal counsel, and the cyber insurance carrier if the practice has a policy) where it can be reached when systems are down. Items 65, 66, 67, 68 are part of this step (one piece of work). The text above includes the work of Items 65 (§164.308(a)(6)(i)), 66 (§164.308(a)(6)(i)), 67 (§164.308(a)(6)(i)), 68 (§164.308(a)(6)(i)). Asset: The written security incident procedure. Owner: Office manager (acting security lead). Verify with: The written incident procedure with its review date, and the record of the staff briefing. Why: It reduces misdirected fax never assessed; no working incident procedure: The practice described measures for this requirement but produced no supporting documentation. Basis: §164.308(a)(6)(i) (standard; Not Implemented). After: Item 8.			
69	§164.312(a)(2)(ii)	Document an emergency access procedure with sealed or vaulted administrative credentials, at least two authorized holders, and a record of any use. Asset: Emergency access to athenaOne. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The written emergency access procedure and the record of the sealed or vaulted credentials. Why: The practice answered no to “A procedure exists for urgent access”; a compliance requirement with no rated risk. Basis: §164.312(a)(2)(ii) (required implementation specification; Not Implemented). After: Item 8.	High	90 days (ePHIShield target)	Compliance requirement; no rated risk

Longer-term work

Item	Requirement	Action	Priority	Timeframe	Risks treated
70	Good practice (no requirement)	Run periodic simulated phishing exercises and use the results to direct training. Asset: Workforce members who use Google Workspace email (simulated phishing is aimed at people, not devices). Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The phishing simulation platform's results report for the most recent campaign. Why: It reduces phishing and stolen email credentials: The practice reported that this specification is not implemented as written. Basis: Good practice beyond the rule (no requirement); it supports §164.308(a)(5)(ii)(B), an addressable (Partially Implemented). After: Item 8.	Medium	6 months (ePHIShield target; good practice beyond the rule)	Phishing and stolen email credentials
71	Risk management (§164.308(a)(1)(ii)(B))	Have an external vulnerability scan of the practice's internet-facing address (Comcast Business gateway and Wi-Fi) run at least once a year and after any change to it, and have a named person read the result; an internal scan of the office is not proportionate for a practice whose records are vendor-hosted and whose network is a gateway and workstations. Asset: Comcast Business gateway and Wi-Fi. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The latest scan report, dated, with the person who read it and the fixes it led to. Why: It reduces exploited unpatched or unsupported systems: The record establishes that no vulnerability scanning is done (representation), and no other step covers it. Basis: §164.308(a)(1)(ii)(B) (required implementation specification; Not Implemented). After: Item 8.	Medium	6 months (ePHIShield target)	Exploited unpatched or unsupported systems

Item	Requirement	Action	Priority	Timeframe	Risks treated
72	§164.310(a)(2)(ii)	Document a facility security plan covering locks, alarm coverage, visitor control, and after-hours procedures for each location. Asset: The practice's facility (keys, codes, alarm and visitors). Owner: Office manager. Verify with: The written facility security plan. Why: It reduces unauthorized physical access and shared physical and network secrets never changed: The practice reported that this specification is not implemented as written. Basis: §164.310(a)(2)(ii) (addressable implementation specification; Partially Implemented).	Medium	6 months (ePHIShield target)	Shared physical and network secrets never changed; Unauthorized physical access
73	§164.310(a)(2)(iii)	Require visitors and service vendors to sign in and be escorted in any area where ePHI or ePHI systems are accessible. Asset: The practice's facility (keys, codes, alarm and visitors). Owner: Office manager. Verify with: The visitor and vendor sign-in log, with entries. Why: It reduces unauthorized physical access: The practice reported that this specification is not implemented as written. Basis: §164.310(a)(2)(iii) (addressable implementation specification; Not Implemented).	Medium	6 months (ePHIShield target)	Unauthorized physical access
74	§164.312(c)(1)	Restrict who can delete or amend records in athenaOne to defined roles, and protect the integrity of ePHI kept outside it (email, fax and local files). athenaOne's own amendment history is reported (not verified): it needs no new control; confirm it from the system's audit view. Asset: athenaOne. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The record system's role permissions showing who can delete or amend records. Why: It reduces permanent data loss: The practice described measures for this requirement but produced no supporting documentation. Basis: §164.312(c)(1) (standard; Partially Implemented). After: Item 8.	Medium	6 months (ePHIShield target)	Permanent data loss

Item	Requirement	Action	Priority	Timeframe	Risks treated
75	Risk management (§164.308(a)(1)(ii)(B))	Mark the binder as not adopted; replace its statements with policies that describe what the practice actually does, as each control in this plan is put in place. Asset: HIPAA policy binder (template, 2017). Owner: Office manager (acting security lead), with the physicians' approval. Verify with: The replaced or annotated binder, approved and dated, each policy matching what the office actually does. Why: It reduces policy binder states controls that do not exist: The uncustomized 2017 template states annual training (none has been given), that all ePHI is encrypted (nothing is), and leaves the security-official designation blank; staff are unaware of its policies. Basis: Risk management (§164.308(a)(1)(ii)(B)) of a risk recorded by ePHIShield's reviewer. After: Item 8.	Medium	6 months (ePHIShield target)	Policy binder states controls that do not exist
76	§164.308(a)(3)(ii)(A)	Require documented supervisor approval before any system access is granted, and retain the approval record for the life of the account plus the retention period. Asset: User accounts in athenaOne and Google Workspace email. Owner: Office manager. Verify with: Approval records for the most recently created accounts. Why: The practice answered no to “Approval is recorded”; a compliance requirement with no rated risk. Basis: §164.308(a)(3)(ii)(A) (addressable implementation specification; Not Implemented). Retention: §164.316(b)(2)(i), quoted under Item 27.	Medium	6 months (ePHIShield target)	Compliance requirement; no rated risk
77	§164.310(a)(2)(i)	Document emergency facility access arrangements, ensuring at least two authorized individuals can reach systems after hours for recovery. Asset: The practice's facility (keys, codes, alarm and visitors). Owner: Office manager. Verify with: The written emergency facility access arrangement naming at least two people. Why: It reduces fire, flood, storm or power loss: The practice reported that this specification is not implemented as written. Basis: §164.310(a)(2)(i) (addressable implementation specification; Partially Implemented).	Low	6 months (ePHIShield target)	Fire, flood, storm or power loss

Evidence-verification follow-up

Work that establishes whether safeguards credited only in part, vendors not assessed, and the patching condition behind the ratings are as the practice reported. None is a corrective action for an established weakness. Timeframes are ePHIShield's recommendations, not HIPAA deadlines: 30 days for a High or Very High risk and 60 for a Moderate one are initial defaults, which ePHIShield's reviewer may adjust for urgency and circumstances. The practice owns these follow-ups and its own remediation. Any further ePHIShield service, such as reviewing vendor evidence or verifying remediation after delivery, is separately agreed unless the signed engagement includes it.

Risk	Follow-up	Priority	Responsible	Recommended
Exploited unpatched or unsupported systems	Obtain evidence of the actual patching condition of the systems holding or reaching ePHI (an update or patch report from the IT provider, or an observation) Asset: Systems holding or reaching ePHI. Verify with: An update or patch status report, dated, for each system.	High	The practice (the person it names, until a security official is designated), with its IT provider	within 30 days
Vendor compromise	Obtain proportionate security evidence from athenahealth (a material vendor) and have it assessed Asset: athenahealth. Verify with: The vendor's security evidence (a SOC 2 report, a certification or a completed security questionnaire), dated, and the practice's written assessment of it.	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days (a material vendor)
Vendor compromise	Obtain proportionate security evidence from Google and have it assessed Asset: Google. Verify with: A completed security questionnaire or the vendor's written statement of its safeguards, dated, and the practice's note of what was read (proportionate to a vendor that is not material).	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days
Vendor compromise	Obtain proportionate security evidence from eFax (Consensus Cloud Solutions) and have it assessed Asset: eFax (Consensus Cloud Solutions). Verify with: A completed security questionnaire or the vendor's written statement of its safeguards, dated, and the practice's note of what was read (proportionate to a vendor that is not material).	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days
Vendor compromise	Obtain proportionate security evidence from Tri-State Office Systems (SYNTHETIC) and have it assessed Asset: Tri-State Office Systems (SYNTHETIC). Verify with: A completed security questionnaire or the vendor's written statement of its safeguards, dated, and the practice's note of what was read (proportionate to a vendor that is not material).	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days

Risk	Follow-up	Priority	Responsible	Recommended
Vendor compromise	Obtain proportionate security evidence from Valley After-Hours Answering (SYNTHETIC) and have it assessed Asset: Valley After-Hours Answering (SYNTHETIC). Verify with: A completed security questionnaire or the vendor's written statement of its safeguards, dated, and the practice's note of what was read (proportionate to a vendor that is not material).	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days
Vendor compromise	Obtain a signed attestation from Kyle Pruitt (SYNTHETIC), independent computer helper of the safeguards on the devices and accounts used for the practice's work, once an agreement is executed (or end the access) Asset: Kyle Pruitt (SYNTHETIC), independent computer helper. Verify with: The individual's signed, dated attestation of safeguards (no audit report is expected from an individual).	Medium	The practice (the person it names, until a security official is designated), with the vendor	within 60 days

Verification requests and steps to establish the facts

Each step asks for evidence: of a safeguard the practice reported but that was not verified (marked “Verify”), or of a fact the analysis could not establish. None is corrective work for an established weakness; if the evidence shows a gap, the gap is corrected as the step says.

Item	Requirement	Step	Priority	Timeframe
E1	§164.308(a)(7)(ii)(D)	Confirm and document whether this is in place: test the contingency plan periodically (ePHIShield recommends an annual tabletop exercise), document the outcome, and revise the plan to address every gap identified. Asset: The contingency plan covering athenaOne and Google Workspace email. Owner: Office manager (acting security lead). Verify with: The dated record of the last contingency plan test or tabletop exercise, and the revisions made. Why: The question for this requirement was not asked before the reporting date; a compliance requirement with no rated risk. Basis: §164.308(a)(7)(ii)(D) (addressable implementation specification; Unable to Determine).	Medium	60 days (ePHIShield target)
E2	§164.312(b)	Confirm and document whether this is in place: enable audit logging on every ePHI system, set and document a log retention period that supports investigation (the Security Rule specifies no retention period for system audit logs; the 6-year retention of §164.316(b)(2)(i) applies to the documentation §164.316(b)(1) requires: policies and procedures, and written records of actions, activities or assessments the Rule requires to be documented), and document any system that cannot log. Asset: Audit logs of athenaOne and Google Workspace email. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: A sample audit log or access report from each listed system, and the written retention period. Why: It reduces shared sign-in without individual attribution and inappropriate access by a staff member: The question for this requirement was asked; the respondent did not know. Basis: §164.312(b) (standard; Unable to Determine).	High	30 days (ePHIShield target)
E3	§164.312(c)(2)	Confirm and document the integrity verification athenaOne provides for the records it holds (its vendor's statement or the audit view). A backup platform check waits for the backup step: the record shows no practice backup to check. Asset: athenaOne. Owner: Office manager (acting security lead); the independent computer helper only once a written agreement is in place. Verify with: The record system's or backup platform's integrity verification setting or report. Why: The question for this requirement was asked; the respondent did not know; a compliance requirement with no rated risk. Basis: §164.312(c)(2) (addressable implementation specification; Unable to Determine).	Low	60 days (ePHIShield target)

Not applicable to this practice, observed in place, or covered by another step

These catalog steps are not separate work for this practice: their precondition (a server, a practice-side interface, a backup platform, an office network) is absent from the recorded inventory, the condition they ask for was directly observed, or another step does the same work. Each row gives the requirement's status as Part E rates it, and where that is not Implemented, what is in place and what is not.

Requirement	Catalog step	Why no separate step
§164.306(a)	Confirm and document whether this is in place: create and maintain a written ePHI asset inventory covering every system, device, and service that stores or transmits patient information, with an owner and a review date.	Part E: Reported, Not Verified. In place: The written ePHI asset inventory is produced by the device inventory step. The work is done under Item 38. Not in place: The answer to “List every system, application, or service where patient information is stored or processed electronically — EHR, practice management, billing, imaging, lab interfaces, patient portal, email, texting.
Item 44, §164.312(e)(2)(i)	Confirm transport integrity protection on all automated interfaces and ensure interface error alerts are routed to a monitored destination.	Part E: Not Implemented. In place: The recorded interfaces (LabCorp lab interface) are the vendor's, with no practice-side component to configure; transport protection on them is the vendor's, covered by the vendor assurance work. Not in place: Not established before the reporting date after 4 attempt(s).

H. Schedules

H-1 to H-4. Systems, locations and information flows. H-5. Risk register. H-6. Documents reviewed. H-7. Unresolved items. H-8. Sources. H-9. Traceability. H-10. Evidence behind each status. H-11. Historical source wording for combined work.

H-1 to H-4. Systems, locations and information flows

H-1. Systems and equipment that hold or reach patient information

From the structured system inventory. Each attribute shows how it is known. An attribute nobody supplied is listed as not recorded; it is not inferred. The basis column cites the source key below.

Source key. S-n is a source (who said so, or how ePHIShield saw it) exactly as recorded; D-n is a document reviewed. The rows cite the identifier; the same identifiers are used in Schedule H-10.

Key	Source or document
S-1	Office manager; athenaOne user list
S-2	Computer helper
S-3	Office manager
S-4	Analyst observation; computer helper
S-5	Office manager; computer helper
S-6	Analyst observation
S-7	Computer helper; analyst observation
S-8	ePHIShield analyst (on-site visit), with the computer helper
S-9	ePHIShield analyst
S-10	Office manager (also billing), pre-visit intake form
S-11	ePHIShield

Key	Source or document
S-12	the practice
S-13	Computer helper (office manager's nephew, SYNTHETIC) by phone after the visit, plus analyst on-site observations and documents reviewed during the visit (policy binder, athena user list, athena agreement)
S-14	ePHIShield (answer given by Office manager (also billing), pre-visit intake form)
S-15	Computer helper (round 2): BAA not accepted in the Google admin console
S-16	Office manager (round 1): not sure; ePHIShield analyst on site: requested, and no agreement was produced
S-17	Office manager (round 1 vendor list): no agreement with the copier dealer
S-18	Office manager (round 1 vendor list): no agreement; paid informally
D-1	athenaOne active user list (printed during on-site visit)
D-2	HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)
D-3	athenahealth service agreement with BAA addendum (PDF, 2019)

System	Attribute	Recorded	Basis
athenaOne (SYS-001)	What the system is used for	EHR, practice management/billing, patient portal, scheduling, lab and immunization registry interfaces	Documented, S-1 (D-1)
	Where it runs	athenahealth cloud	Documented, S-1 (D-1)
	Where it is physically or logically located	Vendor	Documented, S-1 (D-1)
	What patient information it holds or reaches	Full pediatric chart, demographics, guarantor and insurance, claims, immunizations	Documented, S-1 (D-1)
	Who uses it	7 named users plus 1 generic kiosk account (and 1 departed MA still active)	Documented, S-1 (D-1)
	Who maintains it	athenahealth; office manager is practice admin	Documented, S-1 (D-1)
	How users sign in to it	Web browser; MFA enforced only on the office manager's admin account	Documented, S-1 (D-1)
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Documented, S-1
Google Workspace email (SYS-002)	What the system is used for	Practice email; copier scan-to-email	Reported, S-2
	Where it runs	Google cloud	Reported, S-2
	Where it is physically or logically located	Vendor	Reported, S-2

System	Attribute	Recorded	Basis
	What patient information it holds or reaches	School/daycare forms, shot records, referral attachments	Reported, S-2
	Who uses it	Individual accounts for providers and office manager; shared frontdesk@ account	Reported, S-2
	Who maintains it	Kyle set it up; Business Starter edition; BAA not accepted in admin console	Reported, S-2
	How users sign in to it	Browser and Gmail app on personal phones; 2-step verification not enforced	Reported, S-2
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-2
eFax Corporate (SYS-003)	What the system is used for	Inbound/outbound fax (referrals, records requests)	Reported, S-3
	Where it runs	Vendor cloud	Reported, S-3
	Where it is physically or logically located	Vendor	Reported, S-3
	What patient information it holds or reaches	Faxed records, retained in the eFax web account	Reported, S-3
	Who uses it	One shared login used by front desk and office manager	Reported, S-3
	Who maintains it	Office manager	Reported, S-3
	How users sign in to it	Web portal and email delivery to frontdesk@	Reported, S-3
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-3
LabCorp lab interface (SYS-004)	What the system is used for	Electronic lab orders and results	Reported, S-3
	Where it runs	athenahealth/LabCorp interface	Reported, S-3
	Where it is physically or logically located	Vendor	Reported, S-3
	What patient information it holds or reaches	Orders and results	Reported, S-3
	Who uses it	Clinical staff via athenaOne	Reported, S-3
	Who maintains it	athenahealth	Reported, S-3
	How users sign in to it	Interface, no practice-side component	Reported, S-3

System	Attribute	Recorded	Basis
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-3
Front desk PC 1 (SYS-005)	What the system is used for	Check-in, scheduling, eFax, Gmail	Observed, S-4
	Where it runs	On premises	Observed, S-4
	Where it is physically or logically located	Front desk, monitor faces waiting room	Observed, S-4
	What patient information it holds or reaches	Browser sessions; downloads folder	Observed, S-4
	Who uses it	Front desk and MAs via shared Windows 'FrontDesk' account	Observed, S-4
	Who maintains it	Computer helper	Observed, S-4
	How users sign in to it	Shared local Windows account, screen lock off	Observed, S-4
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Observed, S-4
Front desk PC 2 (SYS-006)	What the system is used for	Check-in, checkout, payments	Reported, S-2
	Where it runs	On premises	Reported, S-2
	Where it is physically or logically located	Front desk	Reported, S-2
	What patient information it holds or reaches	Browser sessions; downloads folder	Reported, S-2
	Who uses it	Shared 'FrontDesk' account	Reported, S-2
	Who maintains it	Computer helper	Reported, S-2
	How users sign in to it	Windows 10 (out of vendor support since Oct 2025), shared account	Reported, S-2
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-2
Exam room PCs (4) (SYS-007)	What the system is used for	Charting in exam rooms	Reported, S-2
	Where it runs	On premises	Reported, S-2
	Where it is physically or logically located	Exam rooms 1-4	Reported, S-2

System	Attribute	Recorded	Basis
	What patient information it holds or reaches	Browser sessions	Reported, S-2
	Who uses it	MAs, NP, physicians via shared 'Exam' Windows account	Reported, S-2
	Who maintains it	Computer helper	Reported, S-2
	How users sign in to it	Shared Windows account; athenaOne individual logins	Reported, S-2
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-2
Office manager PC (SYS-008)	What the system is used for	Billing, athena admin, scanning	Reported, S-5
	Where it runs	On premises	Reported, S-5
	Where it is physically or logically located	Office manager's office (door unlocked by day)	Reported, S-5
	What patient information it holds or reaches	Local 'Scans' folder of documents before upload to athena; downloaded reports	Reported, S-5
	Who uses it	Office manager (own Windows account)	Reported, S-5
	Who maintains it	Computer helper	Reported, S-5
	How users sign in to it	Own Windows account; TeamViewer installed for the helper	Reported, S-5
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-5
Check-in kiosk tablet (SYS-009)	What the system is used for	Patient check-in in the waiting room	Observed, S-6
	Where it runs	On premises (iPad)	Observed, S-6
	Where it is physically or logically located	Waiting room stand	Observed, S-6
	What patient information it holds or reaches	athenaOne session under generic front-desk account	Observed, S-6
	Who uses it	Parents; front desk	Observed, S-6
	Who maintains it	Office manager	Observed, S-6
	How users sign in to it	Generic 'kiosk' athenaOne login left signed in all day; password on sticky note	Observed, S-6
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Observed, S-6

System	Attribute	Recorded	Basis
Staff personal phones (SYS-010)	What the system is used for	Texting parents about appointment logistics; Gmail app	Reported, S-3
	Where it runs	Personal	Reported, S-3
	Where it is physically or logically located	With staff	Reported, S-3
	What patient information it holds or reaches	SMS threads with child names, appointment times; practice email	Reported, S-3
	Who uses it	Front desk, MAs, office manager	Reported, S-3
	Who maintains it	Nobody	Reported, S-3
	How users sign in to it	Personal passcodes (unknown); no MDM	Reported, S-3
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-3
Physicians' personal laptops (SYS-011)	What the system is used for	Finishing notes from home	Reported, S-3
	Where it runs	Personal	Reported, S-3
	Where it is physically or logically located	Physicians' homes	Reported, S-3
	What patient information it holds or reaches	athenaOne browser sessions; possibly downloads	Reported, S-3
	Who uses it	Both pediatricians	Reported, S-3
	Who maintains it	Nobody	Reported, S-3
	How users sign in to it	athenaOne password only	Reported, S-3
	Location served	Physicians' homes (remote access to athenaOne from personal laptops) (LOC-002)	From the system's recorded location
Old laptops in storage closet (2) (SYS-012)	What the system is used for	Retired laptops from before the athena conversion (pre-2019)	Observed, S-6
	Where it runs	On premises	Observed, S-6
	Where it is physically or logically located	Unlocked back storage closet	Observed, S-6
	What patient information it holds or reaches	Unknown; possibly the prior EHR's local data or exports	Observed, S-6
	Who uses it	None	Observed, S-6

System	Attribute	Recorded	Basis
	Who maintains it	Nobody	Observed, S-6
	How users sign in to it	Unencrypted Windows	Observed, S-6
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Observed, S-6
Canon multifunction copier (SYS-013)	What the system is used for	Print, scan-to-email, copy	Reported, S-2
	Where it runs	On premises (leased)	Reported, S-2
	Where it is physically or logically located	Hallway	Reported, S-2
	What patient information it holds or reaches	Internal drive image cache; stored Gmail app password	Reported, S-2
	Who uses it	All staff	Reported, S-2
	Who maintains it	Copier dealer	Reported, S-2
	How users sign in to it	Walk-up, no PIN	Reported, S-2
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Reported, S-2
Comcast Business gateway and Wi-Fi (SYS-014)	What the system is used for	Internet, firewall, staff and guest Wi-Fi	Observed, S-7
	Where it runs	On premises	Observed, S-7
	Where it is physically or logically located	Unlocked back storage closet	Observed, S-7
	What patient information it holds or reaches	None (transit only)	Observed, S-8
	Who uses it	All	Observed, S-7
	Who maintains it	Comcast (firmware); helper set up Wi-Fi	Observed, S-7
	How users sign in to it	Default admin password believed unchanged; guest SSID on same LAN	Observed, S-7
	Location served	2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC) (LOC-001)	Observed, S-7
TeamViewer (personal edition) (SYS-015)	What the system is used for	Helper's remote support into the office manager PC	Reported, S-2
	Where it runs	TeamViewer cloud	Reported, S-2

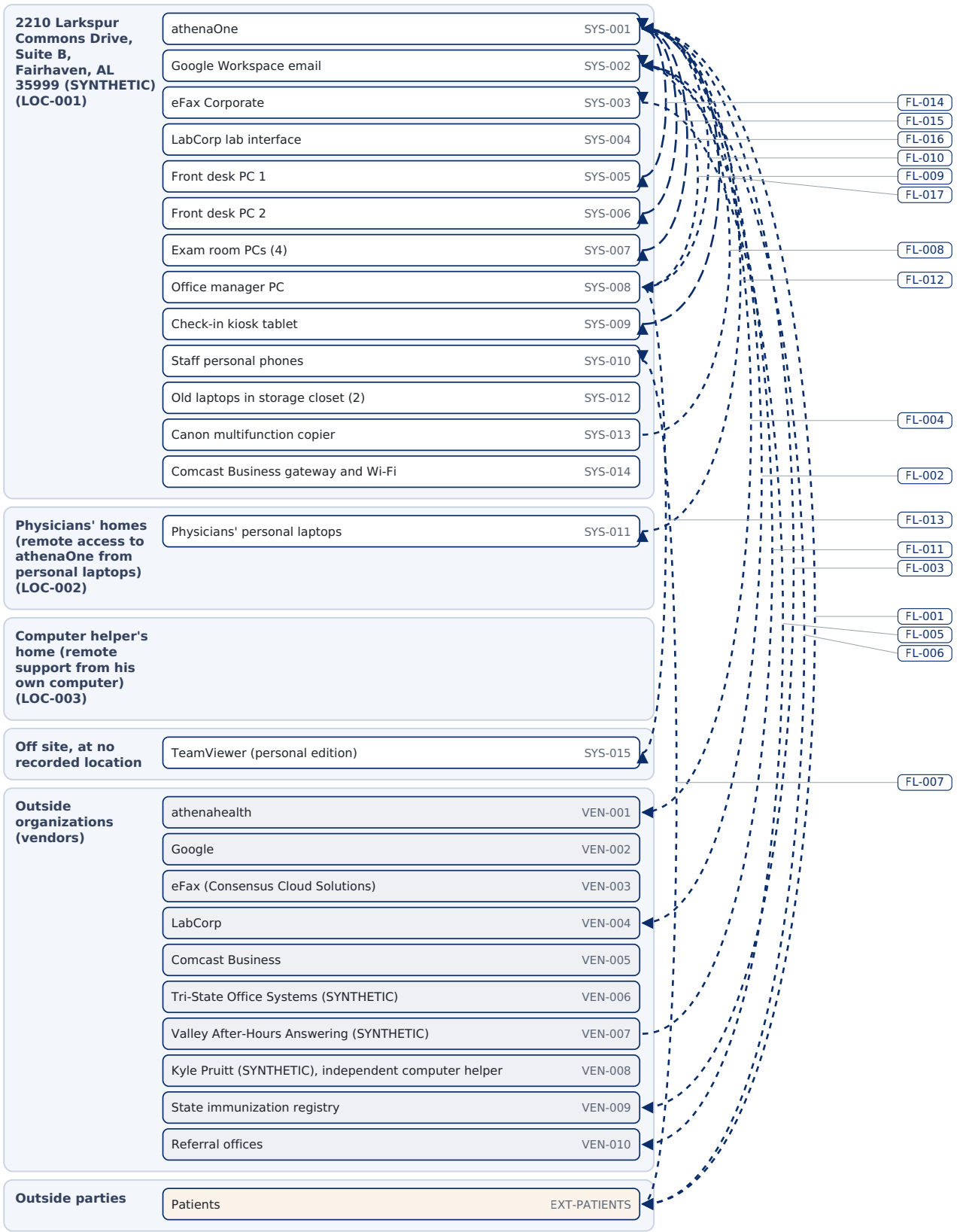
System	Attribute	Recorded	Basis
	Where it is physically or logically located	Helper's home	Reported, S-2
	What patient information it holds or reaches	Screen access to everything the PC can reach	Reported, S-2
	Who uses it	Computer helper	Reported, S-2
	Who maintains it	Computer helper	Reported, S-2
	How users sign in to it	Unattended access with a fixed password, no 2FA	Reported, S-2

H-2. Locations

Location	Identifier	Basis
2210 Larkspur Commons Drive, Suite B, Fairhaven, AL 35999 (SYNTHETIC)	LOC-001	Visited by ePHIShield (ePHIShield analyst, 2026-10-21)
Physicians' homes (remote access to athenaOne from personal laptops)	LOC-002	Not visited and not evaluated remotely (ePHIShield analyst, 2026-10-21); location reported, S-9
Computer helper's home (remote support from his own computer)	LOC-003	Not visited and not evaluated remotely (ePHIShield analyst, 2026-10-21); location reported, S-9

H-3. Information flows

The diagram and the table below show the same recorded flows. A flow appears only when someone recorded it, with how it is known; nothing is inferred. A picture of what was recorded is not, by itself, an assessment of how well those flows are protected; that is the subject of the risk analysis in Part D.



Lanes and placement come only from recorded locations, hosting and vendors. Nothing is inferred; a flow appears only when recorded. Arrowheads show direction; a two-way flow has one at each end. Each flow's label is in the column at the right, joined to its arc.

Recorded systems, locations and flows of patient information.

Flow	From	To	What moves	Channel	Direction	How it is known
FL-001	athenaOne (SYS-001)	Patients (EXT-PATIENTS)	Visit summaries, messages, forms	athena patient portal	Both ways	Reported: Office manager
FL-002	athenaOne (SYS-001)	LabCorp (VEN-004)	Lab orders and results	athena lab interface	Both ways	Reported: Office manager
FL-003	athenaOne (SYS-001)	State immunization registry (VEN-009)	Immunization administration records	athena registry interface	Both ways	Reported: Office manager
FL-004	athenaOne (SYS-001)	athenahealth (VEN-001)	Claims and remittances	athena clearinghouse	Both ways	Reported: Office manager
FL-005	eFax Corporate (SYS-003)	Referral offices (VEN-010)	Referrals, records	fax	Both ways	Reported: Office manager
FL-006	Google Workspace email (SYS-002)	Patients (EXT-PATIENTS)	School/ daycare forms, shot records (attachments)	ordinary email	Both ways	Reported: Office manager
FL-007	Staff personal phones (SYS-010)	Patients (EXT-PATIENTS)	Appointment logistics, sometimes child first names	SMS	Both ways	Reported: Office manager
FL-008	Canon multifunction copier (SYS-013)	Google Workspace email (SYS-002)	Scanned intake forms and outside records	scan-to-email (SMTP)	One way	Reported: Computer helper (office manager's nephew)
FL-009	Google Workspace email (SYS-002)	Office manager PC (SYS-008)	Scans saved locally before upload	download to Scans folder	One way	Reported: Computer helper (office manager's nephew)
FL-010	Office manager PC (SYS-008)	athenaOne (SYS-001)	Scanned documents	browser upload	One way	Reported: Office manager
FL-011	Valley After-Hours Answering (SYNTHETIC) (VEN-007)	Google Workspace email (SYS-002)	After-hours call messages with child name and complaint	ordinary email	One way	Reported: Office manager
FL-012	Physicians' personal laptops (SYS-011)	athenaOne (SYS-001)	Clinical documentation	https browser session	Both ways	Reported: Office manager
FL-013	TeamViewer (personal edition) (SYS-015)	Office manager PC (SYS-008)	Remote control session	TeamViewer	Both ways	Reported: Computer helper (office manager's nephew)
FL-014	Front desk PC 1 (SYS-005)	athenaOne (SYS-001)	Scheduling, check-in and billing work in the record	athenaOne in the browser	Both ways	Observed: ePHIShield analyst (on-site visit)

Flow	From	To	What moves	Channel	Direction	How it is known
FL-015	Front desk PC 2 (SYS-006)	athenaOne (SYS-001)	Scheduling, check-in and billing work in the record	athenaOne in the browser	Both ways	Observed: ePHIShield analyst (on-site visit)
FL-016	Exam room PCs (4) (SYS-007)	athenaOne (SYS-001)	Clinical documentation	athenaOne in the browser	Both ways	Observed: ePHIShield analyst (on-site visit)
FL-017	Check-in kiosk tablet (SYS-009)	athenaOne (SYS-001)	Check-in and demographics	athenaOne app, signed in under a front-desk account	Both ways	Observed: ePHIShield analyst (on-site visit)

H-4. Open items for the flow record

Reference	Open item	Detail
SG-856ecb5f	Suggestion dismissed (closed)	Intake (ephi-flows): claims or billing information leaves the practice. Dismissed by A. Reviewer (SYNTHETIC): SYNTHETIC REHEARSAL. Already recorded as FL-004; no second flow recorded.
SG-f7efc350	Suggestion dismissed (closed)	Intake (ephi-flows): referral information leaves the practice. Dismissed by A. Reviewer (SYNTHETIC): SYNTHETIC REHEARSAL. Already recorded as FL-005; no second flow recorded.
SG-4a0fea2f	Suggestion dismissed (closed)	Intake (ephi-flows): information is sent to patients. Dismissed by A. Reviewer (SYNTHETIC): SYNTHETIC REHEARSAL. Already recorded as FL-001; no second flow recorded.
SG-e632105f	Suggestion dismissed (closed)	Comcast Business is a recorded vendor with no recorded flow. Dismissed by A. Reviewer (SYNTHETIC): SYNTHETIC REHEARSAL. Internet service only; carries traffic, stores no patient information.
SG-8eb82ecf	Suggestion dismissed (closed)	LabCorp lab interface holds patient information and has no recorded flow in or out. Dismissed by A. Reviewer (SYNTHETIC): SYNTHETIC REHEARSAL. athena's channel for the recorded athenaOne to LabCorp flow of lab orders and results; not a separate store.
SYS-012	Patient information held not established	Old laptops in storage closet (2) (SYS-012): Unknown; possibly the prior EHR's local data or exports

H-5. Risk register

Threat	Source	Start L/I	Effect	Step	Likelihood	Impact	Risk	Adjustments
Unattended personal remote-access tool on the office PC	Adversarial: external, through a third-party remote tool	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Front-desk PC running Windows 10 past end of support (included in: exploited unpatched or unsupported systems)	Adversarial: external, malware	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Password-only remote access to athena and Gmail	Adversarial: external, credential theft	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Waiting-room tablet signed in to the EHR all day	Adversarial: opportunistic visitor	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Texts and the practice Gmail app on unmanaged personal phones	Non-adversarial: workforce error; adversarial: device theft	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Two retired unencrypted laptops in an unlocked closet (included in: disposal or reuse of equipment and media)	Adversarial: opportunistic theft; accidental: disposal process failure	Reviewer	—	—	High	High	High	Reviewer-set (basis in Part D)
Lost or stolen device	Adversarial/ Environmental — theft or loss	Moderate / High	+1	+2	Very High	High	High	remote-access step not counted twice
Disposal or reuse of equipment and media	Accidental — process failure	Moderate / High	+1	+2	Very High	High	High	None

Threat	Source	Start L/I	Effect	Step	Likelihood	Impact	Risk	Adjustments
Inappropriate access by a staff member	Adversarial — insider	Moderate / High	+0.34	+1	High	High	High	None
Access retained after someone leaves	Adversarial — former insider	Moderate / High	+1	+2	Very High	High	High	None
Phishing and stolen email credentials	Adversarial — external criminal actor	High / High	+0.65	+1	Very High	High	High	remote-access step not counted twice
Ransomware	Adversarial — external criminal actor	High / Very High	+0.53	+1	Very High	High	High	impact set to High (from Very High) (reviewer)
Shared sign-in without individual attribution	Structural — control design	High / Moderate	+0.33	+1	Very High	High	High	impact set to High (from Moderate) (reviewer)
Interception or misdirection in transit	Adversarial/ Accidental	Moderate / High	+0.53	+1	High	High	High	None
Exploited unpatched or unsupported systems	Adversarial — external	High / High	+0.07	0	High	High	High	None
Shared physical and network secrets never changed	Adversarial: former insider or opportunistic outsider	Reviewer	—	—	Moderate	High	Moderate	Reviewer-set (basis in Part D)
Patient information kept by services with no agreement on record (included in: vendor compromise)	Adversarial or accidental: third party	Reviewer	—	—	Moderate	High	Moderate	Reviewer-set (basis in Part D)
Fire, flood, storm or power loss	Environmental	Low / High	+0.65	+1	Moderate	High	Moderate	None

Threat	Source	Start L/I	Effect	Step	Likelihood	Impact	Risk	Adjustments
Unauthorized physical access	Adversarial — external or unescorted visitor	Moderate / High	+0.3	0	Moderate	High	Moderate	None
Vendor compromise	Adversarial — third party	Moderate / High	0	0	Moderate	High	Moderate	None
Misdirected fax never assessed; no working incident procedure	Non-adversarial: workforce error	Reviewer	—	—	High	Moderate	Moderate	Reviewer-set (basis in Part D)
Policy binder states controls that do not exist	Non-adversarial: reliance on inaccurate documentation	Reviewer	—	—	Moderate	Moderate	Moderate	Reviewer-set (basis in Part D)
Permanent data loss	Structural/ Accidental	Moderate / Very High	+0.53	+1	High	Moderate	Moderate	impact set to Moderate (from Very High) (reviewer)
Visible or unattended screens	Accidental — workforce	High / Moderate	+1	+2	Very High	Moderate	Moderate	None

Figures as recorded in the register. A risk recorded by ePHIShield's reviewer has no starting point or safeguard effect: its likelihood and impact are the reviewer's.

H-6. Documents reviewed

Document	Relied on for
HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)	§164.308(a)(1)(ii)(C), §164.308(a)(2), §164.308(a)(5)(i), §164.308(a)(6)(i), §164.310(b), §164.312(a)(2)(iv)
athenaOne active user list (printed during on-site visit)	§164.308(a)(3)(ii)(C), §164.312(a)(1), §164.312(a)(2)(i)
athenahealth service agreement with BAA addendum (PDF, 2019)	§164.308(b)(1), §164.308(b)(3), §164.314(a)(1), §164.314(a)(2)(i)

H-7. Unresolved items

21 open items, 15 material (also listed in Part A). An established deficiency is not itself listed here: it is a finding with a corrective step in Part G, though a requirement with a deficiency may still have open questions, which are. A verification request asks for evidence of something reported; it is not a correction. An item the record already settles (a professional ruling or reading, or a standard not met whatever the answer) is kept here with that disposition and its reason, and is not counted as open.

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
1 (U-03715C)	Front desk PCs 1 and 2, Exam room PCs (4), Office manager PC	material question (reviewer)	Whether Windows Defender is running and current on every practice PC	Material	Office manager, with the IT provider	Get-MpComputerStatus output for each PC (AMServiceEnabled, RealTimeProtectionEnabled, signature age)	Open
2 (U-07CFF3)	Front desk PC 1, Exam room PCs (4), Office manager PC, Comcast Business gateway and Wi-Fi	material question (reviewer)	The patch state of the PCs other than the Windows 10 front-desk PC, and of the gateway	Material	Office manager, with the IT provider and Comcast Business	Windows Update history or Get-HotFix per PC, and the gateway firmware version from the Comcast Business portal	Open (also settles: §164.308(a)(1)(ii)(B) “Who handles security updates for your computers, server, and network equipment, and do you know when those were last updated or checked?”)
3 (U-29EC2A)	Physicians' personal laptops	material question (reviewer)	Whether the physicians' personal laptops hold downloaded ePHI and are encrypted	Material	Each physician, for their own laptop	Per laptop, a screenshot of the Downloads folder and the browser download history for athena, and the output of manage-bde -status (Windows) or fdesetup status (macOS)	Open
4 (U-2B56C8)	Old laptops in storage closet (2)	material question (reviewer)	What the two retired closet laptops hold	Material	Office manager (acting security lead); inspection by an IT provider under a written agreement	The dated offline inspection of each laptop (drive removed or external boot): user profiles, prior-EHR data folders and exports, recorded on the inventory	Open (also settles: Old laptops in storage closet (2))

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
5 (U-3BD72F)	Canon multifunction copier	material question (reviewer)	What credential and image cache the leased copier holds, and how its drive is handled at lease return	Material	Office manager, with Tri-State Office Systems	A copier admin panel screenshot of the scan-to-email account and drive overwrite or encryption setting, the dealer's statement of drive handling at lease return, and the lease end date	Open
6 (U-3F7A54)	athenaOne; Google Workspace email	material question (reviewer)	Whether athenaOne and Gmail keep audit logs, and for how long	Material	Office manager (athenaOne practice admin)	An athenaOne admin access-report sample with athena's retention statement, and the Google Workspace admin audit-log page for this edition	Open (also settles: §164.312(b))
7 (U-4055CA)	eFax Corporate	material question (reviewer)	The facts of the 2025 misdirected fax needed for the breach assessment	Material	Office manager, with counsel	What the form contained, who received it, when the practice learned of it and the recipient's statement, documented with counsel's view	Open
8 (U-51E8F5)	Staff personal phones	material question (reviewer)	Whether staff phones are encrypted and passcode-locked, and whether departed staff still hold parent text threads	Material	Office manager	Per phone, the lock-screen passcode setting and OS version; a count of staff who text parents; written attestations from departed staff that the threads were deleted	Open
9 (U-64BC86)	eFax Corporate; Valley After-Hours Answering (SYNTHETIC)	material question (reviewer)	Whether an agreement exists with eFax and with Valley After-Hours Answering (none was produced when requested on site)	Material	Office manager	The eFax account admin page showing the plan and any BAA acceptance; a signed Valley agreement or the vendor's written statement that none exists	Open
10 (U-8A4F79)	Office manager PC; TeamViewer (personal edition)	material question (reviewer)	Whether the TeamViewer access was used by anyone other than the helper	Material	Office manager (reading the log herself, not only through the helper)	The TeamViewer incoming-connection log on the office manager PC and the helper's TeamViewer account device list	Open

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
11 (U-8B270E)	Staff personal phones; Google Workspace email	material question (reviewer)	How staff confirm a number or address belongs to the child's parent or guardian before texting or emailing	Material	Office manager	The office manager's answer, checked against how athena's guarantor and contact fields are used before a message is sent	Open
12 (U-F6C7B9)	athenaOne	material question (reviewer)	Whether the departed MA's athenaOne account was used after August 2025	Material	Office manager (athenaOne practice admin), with athenahealth support	The athenaOne access log for that user from the departure date until the account is disabled	Open
13 (U-F22AD3)	§164.308(a)(3)(i) · practice-wide	verification requested	Requested once (round 2); no document was received. The answer stands as reported, not verified.	Material	The HIPAA security official	Provide: Role/permission matrix; EHR user list with roles	Open
14 (U-98AA29)	§164.308(a)(3)(ii)(C) · practice-wide	not answered	Not established after 4 attempt(s), first with the HIPAA security official and then by another route (ask for the document: Termination checklist; or check termination checklist; or ask the practice administrator instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established. Established parts are kept: How quickly, at the last actual departure; Who performs each step. Contradicted by an established fact, so not established: EHR login disabled. The rest is unknown.	Material	The practice administrator	Answer: When someone leaves, what happens to their EHR login, email, building keys or codes, and any practice-owned device? Who does it and how quickly?	Settled (A. Reviewer (SYNTHETIC), 2026-10-21: ePHIShield ruled the requirement not adequate on this record (Part F); the correction is in Part G)

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
15 (U-71A0A5)	§164.308(a)(5)(i) · practice-wide	not answered	Not established after 2 attempt(s), first with the practice administrator and then by another route (ask the HIPAA security official instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.	Material	The HIPAA security official	Answer: Do the owners, physicians, and managers complete the same training?	Open
16 (U-683B98)	§164.308(a)(7)(ii)(A) · practice-wide	not answered	Not established after 3 attempt(s), first with the IT provider and then by another route (ask the practice administrator, for the vendor's documentation or a vendor contact who can answer instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.	Material	The practice administrator	Answer: Is at least one copy kept somewhere separate from the office and isolated from the network?	Open

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
17 (U-B80A67)	§164.306(a) · practice-wide	verification requested	The answer to “List every system, application, or service where patient information is stored or processed electronically — EHR, practice management, billing, imaging, lab interfaces, patient portal, email, texting, fax service, backups, and cloud storage.” rests on the practice's statement; no document or observation supports that answer.	Not material	The practice administrator	Provide: System or asset inventory	Open
18 (U-928FE8)	§164.308(a)(1)(ii)(A) · practice-wide	verification requested	The answer to “Has the practice experienced any lost or stolen device, ransomware, email compromise, patient information sent to the wrong person, or other security incident in the last three years?” rests on the practice's statement; no document or observation supports that answer.	Not material	The HIPAA security official	Provide: Incident log or records	Open
19 (U-E748D9)	§164.308(a)(3)(ii)(A) · practice-wide	not answered	Not established after 2 attempt(s), first with the practice administrator and then by another route (check student or contractor agreements; or ask the HIPAA security official instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.	Not material	The HIPAA security official	Answer: Are students, temporary staff, or contractors supervised when working in areas where patient information is visible?	Open

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
20 (U-4C910F)	§164.308(a)(6)(i) · practice-wide	verification requested	A document was reviewed and rejected by ePHIShield's reviewer: SYNTHETIC REHEARSAL. The binder's incident procedure is a template with no names or contacts; the office manager's own account of what happens (call her, then the helper or athena) and the informally handled 2025 misfax do not follow it. The answer rests on the practice's statement.	Not material	The practice administrator	Provide: Incident response procedure	Settled (A. Reviewer (SYNTHETIC), 2026-10-21: ePHIShield ruled the requirement not adequate on this record (Part F); the correction is in Part G) (also settles: §164.308(a)(6)(i) “Read the practice's incident procedure. Which of the things the rule names does it actually cover, and what would happen if someone followed it exactly?”)
21 (U-526536)	§164.308(a)(7)(i) · practice-wide	not answered	Not established after 2 attempt(s), first with the HIPAA security official and then by another route (ask for the document: Contingency / disaster recovery plan; or ask the practice administrator instead). Referred for professional review; this answer is treated as unknown and on its own does not count against the safeguard, whose status rests on what is established.	Not material	The practice administrator	Answer: If the office lost its systems to fire, flood, ransomware, or extended power loss, is there a written plan for continuing patient care and recovering the records?	Not pursued (the standard is not met whatever the answer: every required specification beneath it is an established deficiency (§164.308(a)(7)(ii)(A), §164.308(a)(7)(ii)(B), §164.308(a)(7)(ii)(C)))

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
22 (U-449B22)	§164.308(a)(7)(ii)(D) · practice-wide	not answered	Not asked: it depends on whether the answer to “If the office lost its systems to fire, flood, ransomware, or extended power loss, is there a written plan for continuing patient care and recovering the records?” (§164.308(a)(7)(i)), which was not established. This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established. Settle the earlier question first.	Not material	The HIPAA security official	Answer: Has the contingency plan ever been tested or walked through, and when?	Open
23 (U-6F1AA2)	§164.308(b)(1) · practice-wide	verification requested	Requested once (round 2); no document was received. The answer stands as reported, not verified.	Not material	The practice administrator	Provide: Vendor list	Open

No. (ID)	Requirement and scope	Uncertainty	What is unresolved	Materiality	Owner	Evidence that settles it	Disposition
24 (U-4A9D27)	§164.310(b) · practice-wide	verification requested	A document was reviewed and rejected by ePHIShield's reviewer: SYNTHETIC REHEARSAL. The binder is an uncustomized 2017 template that the practice never adopted; the record shows shared Windows accounts, the Windows screen lock turned off on the front and exam PCs, and a password on a sticky note at the front desk, which the template's workstation rules do not describe. The answer rests on the practice's statement.	Not material	The practice administrator	Provide: Acceptable use / workstation use policy	Settled (A. Reviewer (SYNTHETIC), 2026-10-21: ePHIShield ruled the requirement not adequate on this record (Part F); the correction is in Part G)
25 (U-24090B)	§164.312(c)(2) · practice-wide	not answered	Not established before the reporting date after 4 attempt(s). This answer is treated as unknown; on its own it does not count against the safeguard, whose status rests on what is established.	Not material	ePHIShield (professional review)	ePHIShield reviews what was recorded and decides what must still be asked	Open

H-8. Sources

- 45 CFR Part 164, Subpart C (Security Rule), as revised October 1, 2025.
- 45 CFR Part 160 (general administrative requirements, definitions).
- HHS Office for Civil Rights, Guidance on Risk Analysis Requirements under the HIPAA Security Rule.
- HHS Security Series Paper 6, Basics of Risk Analysis and Risk Management.
- HHS Security Risk Assessment Tool, User Guide v3.6.1.
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments (Sept. 2012).

Technical schedules

Schedules H-9 and H-10 (and H-11 where combined work is recorded) are the audit trail: each reference in this report and the record identifier it carries, and the evidence behind each status, question by question. They are for the assessor, an auditor or a regulator; the practice does not need them to act on the report.

H-9. Traceability

Each client reference used in this report and the identifier it carries in the assessment record, so any statement can be traced to its source.

Reference	Kind	Record identifier	Source
Unattended personal remote-access tool on the office PC	Risk	SR-001	An outsider who obtains the helper's TeamViewer credentials, or the helper's own compromised computer, takes control of the office manager's PC and reaches athena and locally saved scans.
Front-desk PC running Windows 10 past end of support	Risk	SR-002	Malware exploits a Windows 10 weakness that may go unpatched on the front-desk PC, which is signed in to athena all day under a shared account.
Password-only remote access to athena and Gmail	Risk	SR-003	Someone who phishes or guesses a physician's password signs in to athenaOne or Gmail from anywhere and reads or changes patient records.
Waiting-room tablet signed in to the EHR all day	Risk	SR-005	A parent or visitor using the check-in tablet navigates out of check-in and views or changes other patients' information.
Texts and the practice Gmail app on unmanaged personal phones	Risk	SR-007	Appointment texts naming a child, and the practice mailbox reached through the Gmail app, stay on personal phones the practice does not manage, including the phones of staff who have left, where the practice cannot reach, wipe or account for them. (A text sent to the wrong number is rated under interception or misdirection in transit.)
Two retired unencrypted laptops in an unlocked closet	Risk	SR-008	A retired laptop that may hold the prior record system's data leaves the practice's control unsanitized: taken from the unlocked closet by a visitor, vendor or cleaner, or discarded or given away with no wipe, since no disposal process exists.
Lost or stolen device	Risk	T-DEVICE	Laptop, tablet, phone, or portable drive containing ePHI is lost or stolen
Disposal or reuse of equipment and media	Risk	T-DISPOSE	ePHI is disclosed through improperly disposed or reused hardware, media, or leased copiers
Inappropriate access by a staff member	Risk	T-INSIDER	Workforce member accesses or discloses patient records without a permitted purpose
Access retained after someone leaves	Risk	T-ORPHAN	Departed workforce member retains active access to ePHI systems

Reference	Kind	Record identifier	Source
Phishing and stolen email credentials	Risk	T-PHISH	Workforce member discloses credentials to a phishing message, allowing unauthorized access to email containing ePHI
Ransomware	Risk	T-RANSOM	Ransomware encrypts practice systems and backups, rendering patient records unavailable and potentially exfiltrated
Shared sign-in without individual attribution	Risk	T-SHARED	Shared or generic logins prevent attribution of access to patient records to an individual, so misuse is harder to investigate and attribute
Interception or misdirection in transit	Risk	T-TRANSMIT	ePHI is intercepted or misdirected during unprotected electronic transmission
Exploited unpatched or unsupported systems	Risk	T-UNPATCHED	Unsupported or unpatched systems are exploited to gain access to the practice network
Shared physical and network secrets never changed	Risk	SR-006	A former employee, a cleaning-crew member or a visitor who knows the alarm code, the posted Wi-Fi password or the gateway's default admin password enters after hours or joins the network that carries the practice PCs; the copier's stored Gmail app password gives mailbox access to whoever reaches the copier's settings.
Patient information kept by services with no agreement on record	Risk	SR-010	A service that receives and keeps the practice's patient information every day uses, keeps or discloses it outside the practice's control, or has a security incident it is not obliged to report, so the practice never learns of it and cannot assess or notify.
Fire, flood, storm or power loss	Risk	T-DISASTER	Fire, flood, storm, or extended power loss damages systems and interrupts access to patient records
Unauthorized physical access	Risk	T-PHYS	Unauthorized person gains physical access to workstations or server equipment holding ePHI
Vendor compromise	Risk	T-VENDOR	A business associate suffers a compromise exposing the practice's ePHI, or handles it without adequate assurances
Misdirected fax never assessed; no working incident procedure	Risk	SR-004	A misdirected fax or email is handled informally, so a reportable breach goes unassessed and unreported.
Policy binder states controls that do not exist	Risk	SR-009	Staff or the practice rely on the binder's statements, for example that all ePHI is encrypted, and wrongly treat a lost device or emailed record as secured, so a notifiable breach is not assessed or reported.

Reference	Kind	Record identifier	Source
Permanent data loss	Risk	T-DATALOSS	Hardware failure or accidental deletion causes permanent loss of patient records
Visible or unattended screens	Risk	T-SCREEN	Patient information is exposed to patients or visitors through unattended or visible workstation screens
§164.306(a)	Finding	F-RC-164_306-a	CU-P8b-164.306(a)
§164.308(a)(1)(ii)(A)	Finding	F-RC-164_308-a-1-ii-A	CU-P8b-164.308(a)(1)(ii)(A)
§164.308(a)(1)(ii)(B)	Finding	F-RC-164_308-a-1-ii-B	CU-P8b-164.308(a)(1)(ii)(B)
§164.308(a)(1)(ii)(C)	Finding	F-RC-164_308-a-1-ii-C	CU-P8b-164.308(a)(1)(ii)(C)
§164.308(a)(1)(ii)(D)	Finding	F-RC-164_308-a-1-ii-D	CU-P8b-164.308(a)(1)(ii)(D)
§164.308(a)(2)	Finding	F-RC-164_308-a-2	CU-P8b-164.308(a)(2)
§164.308(a)(3)(i)	Finding	F-RC-164_308-a-3-i	CU-P8b-164.308(a)(3)(i)
§164.308(a)(3)(ii)(A)	Finding	F-RC-164_308-a-3-ii-A	CU-P8b-164.308(a)(3)(ii)(A)
§164.308(a)(3)(ii)(C)	Finding	F-RC-164_308-a-3-ii-C	CU-P8b-164.308(a)(3)(ii)(C)
§164.308(a)(4)(ii)(C)	Finding	F-RC-164_308-a-4-ii-C	CU-P8b-164.308(a)(4)(ii)(C)
§164.308(a)(5)(i)	Finding	F-RC-164_308-a-5-i	CU-P8b-164.308(a)(5)(i)
§164.308(a)(5)(ii)(A)	Finding	F-RC-164_308-a-5-ii-A	CU-P8b-164.308(a)(5)(ii)(A)
§164.308(a)(5)(ii)(B)	Finding	F-RC-164_308-a-5-ii-B	CU-P8b-164.308(a)(5)(ii)(B)
§164.308(a)(5)(ii)(C)	Finding	F-RC-164_308-a-5-ii-C	CU-P8b-164.308(a)(5)(ii)(C)
§164.308(a)(5)(ii)(D)	Finding	F-RC-164_308-a-5-ii-D	CU-P8b-164.308(a)(5)(ii)(D)
§164.308(a)(6)(i)	Finding	F-RC-164_308-a-6-i	CU-P8b-164.308(a)(6)(i)
§164.308(a)(6)(ii)	Finding	F-RC-164_308-a-6-ii	CU-P8b-164.308(a)(6)(ii)
§164.308(a)(7)(i)	Finding	F-RC-164_308-a-7-i	CU-P8b-164.308(a)(7)(i)
§164.308(a)(7)(ii)(A)	Finding	F-RC-164_308-a-7-ii-A	CU-P8b-164.308(a)(7)(ii)(A)
§164.308(a)(7)(ii)(B)	Finding	F-RC-164_308-a-7-ii-B	CU-P8b-164.308(a)(7)(ii)(B)
§164.308(a)(7)(ii)(C)	Finding	F-RC-164_308-a-7-ii-C	CU-P8b-164.308(a)(7)(ii)(C)
§164.308(a)(7)(ii)(D)	Finding	F-RC-164_308-a-7-ii-D	CU-P8b-164.308(a)(7)(ii)(D)
§164.308(b)(1)	Finding	F-RC-164_308-b-1	CU-P8b-164.308(b)(1)
§164.308(b)(3)	Finding	F-RC-164_308-b-3	CU-P8b-164.308(b)(3)
§164.310(a)(1)	Finding	F-RC-164_310-a-1	CU-P8b-164.310(a)(1)
§164.310(a)(2)(i)	Finding	F-RC-164_310-a-2-i	CU-P8b-164.310(a)(2)(i)
§164.310(a)(2)(ii)	Finding	F-RC-164_310-a-2-ii	CU-P8b-164.310(a)(2)(ii)
§164.310(a)(2)(iii)	Finding	F-RC-164_310-a-2-iii	CU-P8b-164.310(a)(2)(iii)
§164.310(b)	Finding	F-RC-164_310-b	CU-P8b-164.310(b)
§164.310(c)	Finding	F-RC-164_310-c	CU-P8b-164.310(c)

Reference	Kind	Record identifier	Source
§164.310(d)(1)	Finding	F-RC-164_310-d-1	CU-P8b-164.310(d)(1)
§164.310(d)(2)(i)	Finding	F-RC-164_310-d-2-i	CU-P8b-164.310(d)(2)(i)
§164.310(d)(2)(ii)	Finding	F-RC-164_310-d-2-ii	CU-P8b-164.310(d)(2)(ii)
§164.310(d)(2)(iii)	Finding	F-RC-164_310-d-2-iii	CU-P8b-164.310(d)(2)(iii)
§164.312(a)(1)	Finding	F-RC-164_312-a-1	CU-P8b-164.312(a)(1)
§164.312(a)(2)(i)	Finding	F-RC-164_312-a-2-i	CU-P8b-164.312(a)(2)(i)
§164.312(a)(2)(ii)	Finding	F-RC-164_312-a-2-ii	CU-P8b-164.312(a)(2)(ii)
§164.312(a)(2)(iii)	Finding	F-RC-164_312-a-2-iii	CU-P8b-164.312(a)(2)(iii)
§164.312(a)(2)(iv)	Finding	F-RC-164_312-a-2-iv	CU-P8b-164.312(a)(2)(iv)
§164.312(b)	Finding	F-RC-164_312-b	CU-P8b-164.312(b)
§164.312(c)(1)	Finding	F-RC-164_312-c-1	CU-P8b-164.312(c)(1)
§164.312(c)(2)	Finding	F-RC-164_312-c-2	CU-P8b-164.312(c)(2)
§164.312(d)	Finding	F-RC-164_312-d	CU-P8b-164.312(d)
§164.312(e)(1)	Finding	F-RC-164_312-e-1	CU-P8b-164.312(e)(1)
§164.312(e)(2)(i)	Finding	F-RC-164_312-e-2-i	CU-P8b-164.312(e)(2)(i)
§164.312(e)(2)(ii)	Finding	F-RC-164_312-e-2-ii	CU-P8b-164.312(e)(2)(ii)
§164.314(a)(1)	Finding	F-RC-164_314-a-1	CU-P8b-164.314(a)(1)
§164.314(a)(2)(i)	Finding	F-RC-164_314-a-2-i	CU-P8b-164.314(a)(2)(i)
Item 1	Action plan step	R-RC-164_308-a-3-ii-C-10	164.308(a)(3)(ii)(C)#1
Item 2	Action plan step	REC-SR-010-C	SR|SR-010#contain
Item 3	Action plan step	REC-SR-001-C	SR|SR-001#contain
Item 4	Action plan step	REC-SR-005-C	SR|SR-005#contain
Item 5	Action plan step	REC-SR-008-C	SR|SR-008#contain
Item 6	Action plan step	REC-SR-004-C	SR|SR-004#contain
Item 7	Action plan step	REC-SR-006-C	SR|SR-006#contain
Item 8	Action plan step	R-RC-164_308-a-2-7	164.308(a)(2)#0
Item 9	Action plan step	R-RC-164_308-a-3-i-8	164.308(a)(3)(i)#0
Item 10	Action plan step	R-RC-164_308-a-3-ii-C-9	164.308(a)(3)(ii)(C)#0

Reference	Kind	Record identifier	Source
Item 11	Action plan step	R-RC-164_308-a-4-ii-C-11	164.308(a)(4)(ii)(C)#0
Item 12	Action plan step	R-RC-164_308-a-5-ii-B-14	164.308(a)(5)(ii)(B)#0
Item 13	Action plan step	R-RC-164_308-a-5-ii-B-15	164.308(a)(5)(ii)(B)#1
Item 14	Action plan step	R-RC-164_312-a-1-36	164.312(a)(1)#0
Item 15	Action plan step	R-RC-164_312-a-2-i-37	164.312(a)(2)(i)#0
Item 16	Action plan step	R-RC-164_312-a-2-iv-39	164.312(a)(2)(iv)#0
Item 17	Action plan step	R-RC-164_312-d-41	164.312(d)#0
Item 18	Action plan step	R-RC-164_312-d-42	164.312(d)#1
Item 19	Action plan step	REC-SR-003	SR|SR-003
Item 20	Action plan step	R-RC-164_308-b-1-50	164.308(b)(1)#0
Item 21	Action plan step	R-RC-164_308-b-3-51	164.308(b)(3)#0
Item 22	Action plan step	R-RC-164_314-a-1-59	164.314(a)(1)#0
Item 23	Action plan step	R-RC-164_314-a-2-i-60	164.314(a)(2)(i)#0
Item 24	Action plan step	REC-SR-010	SR|SR-010
Item 25	Action plan step	R-RC-164_308-a-1-ii-A-1	164.308(a)(1)(ii)(A)#0
Item 26	Action plan step	R-RC-164_308-a-1-ii-B-3	164.308(a)(1)(ii)(B)#0
Item 27	Action plan step	R-RC-164_308-a-1-ii-C-5	164.308(a)(1)(ii)(C)#0
Item 28	Action plan step	R-RC-164_308-a-1-ii-D-6	164.308(a)(1)(ii)(D)#0
Item 29	Action plan step	R-RC-164_308-a-5-i-12	164.308(a)(5)(i)#0
Item 30	Action plan step	R-RC-164_308-a-5-ii-A-13	164.308(a)(5)(ii)(A)#0
Item 31	Action plan step	R-RC-164_308-a-5-ii-C-17	164.308(a)(5)(ii)(C)#0

Reference	Kind	Record identifier	Source
Item 32	Action plan step	R-RC-164_308-a-6-ii-23	164.308(a)(6)(ii)#0
Item 33	Action plan step	R-RC-164_308-a-7-i-24	164.308(a)(7)(i)#0
Item 34	Action plan step	R-RC-164_308-a-7-ii-A-25	164.308(a)(7)(ii)(A)#0
Item 35	Action plan step	R-RC-164_308-a-7-ii-A-26	164.308(a)(7)(ii)(A)#1
Item 36	Action plan step	R-RC-164_308-a-7-ii-B-27	164.308(a)(7)(ii)(B)#0
Item 37	Action plan step	R-RC-164_308-a-7-ii-B-28	164.308(a)(7)(ii)(B)#1
Item 38	Action plan step	R-RC-164_310-d-1-32	164.310(d)(1)#0
Item 39	Action plan step	R-RC-164_310-d-2-i-33	164.310(d)(2)(i)#0
Item 40	Action plan step	R-RC-164_310-d-2-ii-34	164.310(d)(2)(ii)#0
Item 41	Action plan step	R-RC-164_310-d-2-iii-35	164.310(d)(2)(iii)#0
Item 42	Action plan step	R-RC-164_312-a-2-iv-40	164.312(a)(2)(iv)#1
Item 43	Action plan step	R-RC-164_312-e-1-43	164.312(e)(1)#0
Item 44	Action plan step	R-RC-164_312-e-2-i-44	164.312(e)(2)(i)#0
Item 45	Action plan step	R-RC-164_312-e-2-ii-45	164.312(e)(2)(ii)#0
Item 46	Action plan step	R-RC-164_312-e-2-ii-46	164.312(e)(2)(ii)#1
Item 47	Action plan step	REC-SR-001	SR|SR-001
Item 48	Action plan step	REC-SR-002	SR|SR-002
Item 49	Action plan step	REC-SR-005	SR|SR-005
Item 50	Action plan step	REC-SR-007	SR|SR-007
Item 51	Action plan step	REC-SR-008	SR|SR-008
Item 52	Action plan step	R-RC-164_308-a-5-ii-D-48	164.308(a)(5)(ii)(D)#0

Reference	Kind	Record identifier	Source
Item 53	Action plan step	R-RC-164_308-a-5-ii-D-49	164.308(a)(5)(ii)(D)#1
Item 54	Action plan step	R-RC-164_308-a-7-ii-C-29	164.308(a)(7)(ii)(C)#0
Item 55	Action plan step	R-RC-164_310-a-1-52	164.310(a)(1)#0
Item 56	Action plan step	R-RC-164_310-a-1-53	164.310(a)(1)#1
Item 57	Action plan step	R-RC-164_310-b-30	164.310(b)#0
Item 58	Action plan step	R-RC-164_310-c-31	164.310(c)#0
Item 59	Action plan step	R-RC-164_312-a-2-iii-57	164.312(a)(2)(iii)#0
Item 60	Action plan step	REC-SR-004	SR|SR-004
Item 61	Action plan step	REC-SR-006	SR|SR-006
Item 62	Action plan step	R-RC-164_308-a-1-ii-A-2	164.308(a)(1)(ii)(A)#1
Item 63	Action plan step	R-RC-164_308-a-1-ii-B-4	164.308(a)(1)(ii)(B)#1
Item 64	Action plan step	R-RC-164_308-a-6-i-18	164.308(a)(6)(i)#0
Item 65	Action plan step	R-RC-164_308-a-6-i-19	164.308(a)(6)(i)#1
Item 66	Action plan step	R-RC-164_308-a-6-i-20	164.308(a)(6)(i)#2
Item 67	Action plan step	R-RC-164_308-a-6-i-21	164.308(a)(6)(i)#3
Item 68	Action plan step	R-RC-164_308-a-6-i-22	164.308(a)(6)(i)#4
Item 69	Action plan step	R-RC-164_312-a-2-ii-38	164.312(a)(2)(ii)#0
Item 70	Action plan step	R-RC-164_308-a-5-ii-B-16	164.308(a)(5)(ii)(B)#2
Item 71	Action plan step	R-SCAN-1	164.308(a)(1)(ii)(B)#scan
Item 72	Action plan step	R-RC-164_310-a-2-ii-55	164.310(a)(2)(ii)#0
Item 73	Action plan step	R-RC-164_310-a-2-iii-56	164.310(a)(2)(iii)#0

Reference	Kind	Record identifier	Source
Item 74	Action plan step	R-RC-164_312-c-1-58	164.312(c)(1)#0
Item 75	Action plan step	REC-SR-009	SR|SR-009
Item 76	Action plan step	R-RC-164_308-a-3-ii-A-47	164.308(a)(3)(ii)(A)#0
Item 77	Action plan step	R-RC-164_310-a-2-i-54	164.310(a)(2)(i)#0
Item E1	Action plan step	R-RC-164_308-a-7-ii-D-62	164.308(a)(7)(ii)(D)#0
Item E2	Action plan step	R-RC-164_312-b-63	164.312(b)#0
Item E3	Action plan step	R-RC-164_312-c-2-64	164.312(c)(2)#0

H-10. Evidence behind each status

Each row is one recorded question. Contribution is what it added to the status: supporting, adverse, unknown, or none (context and analysis inputs never count as control evidence). A contradicted answer is never supporting: where only part of it is contradicted, the uncontested parts are named. A mixed answer supports the safeguard in some parts and counts against it in others; both are named. Recorded gives the intake round the answer belongs to (intake round 1: Office manager (also billing); intake round 2: Computer helper (office manager's nephew), and, where the answer came in reply to a later written request within that round, the follow-up request it answered; the date is the date of the session in which it was recorded. Systems names the systems an answer was recorded for, and, where it differs by system, those on which it counts against the safeguard. An earlier answer that a later answer replaced is kept beneath it as superseded, with its source and what changed.

The Source and Documents columns cite the source key at the head of Schedule H-1 (S-n a source, D-n a document).

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.302	ce-type	reported	supporting	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.302	ephi-confirm	reported	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.306(a)	ephi-systems	reported	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.306(a)	ephi-locations	observed	none	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.306(a)	ephi-flows	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.306(a)	workforce-count	reported	supporting	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.306(b)	it-support-model	reported	supporting	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.306(b)	budget-constraints	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(a)(1)(ii)(A)	prior-sra	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(A)	known-vulnerabilities	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(A)	prior-incidents	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(B)	risk-mgmt-process	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)
§164.308(a)(1)(ii)(B)	patching	asked, unknown	unknown	S-12	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(B)	patching: earlier answer, superseded	superseded	none: superseded by the later answer	S-13	—	intake round 2; replaced intake round 2, follow-up request 2 (recorded 2026-10-21)	—	Stated: ehr: yes. Later evidence: the later answer (reported by the practice). Resolution: clarified by the analyst: SYNTHETIC REHEARSAL. The 'No' answered the parenthetical: the practice has no server; the system inventory lists none, and its record system, email and fax are cloud services..
§164.308(a)(1)(ii)(B)	vulnerability-scanning	reported	none	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(C)	sanction-policy	established deficient	adverse	S-13	D-2	intake round 2 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F); document evidence rejected by ePHIShield
§164.308(a)(1)(ii)(D)	log-review-practice	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(1)(ii)(D)	log-sources	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(2)	security-official	established deficient	adverse	S-11	D-2	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(a)(2)	security-official: earlier answer, superseded	superseded (overturned)	none: superseded by the later answer	S-14	D-2	intake round 1; replaced intake round 2, follow-up request 1 (recorded 2026-10-21)	—	Stated: name: Me (office manager); in writing: yes. Later evidence: Assignment is documented in writing: yes → no (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)). Resolution: the later answer stands.
§164.308(a)(3)(i)	role-access	reported	supporting	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: affirmative (Part F)
§164.308(a)(3)(i)	access-review	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(3)(ii)(A)	access-authorization-process	established deficient	adverse	S-10	—	intake round 1, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(3)(ii)(A)	supervision-nonstaff	asked, unknown	unknown	S-10	—	intake round 1, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(3)(ii)(C)	termination-checklist	contradicted	contradicted in part: EHR login disabled; not counted as support while the contradiction stands	S-10	—	intake round 1, follow-up request 3 (recorded 2026-10-21)	practice-wide	contradicted by the established answer to 164.308(a)(3)(ii)(C)|orphan-check (ehr)
§164.308(a)(3)(ii)(C)	termination-timeliness	reported	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(3)(ii)(C)	orphan-check	established deficient	adverse	S-11	D-1	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F)
§164.308(a)(3)(ii)(C)	addressable-164.308(a)(3)(ii)(C)	established deficient	adverse	S-11	D-1	intake round 2 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(a)(4)(ii)(C)	access-modify-process	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(4)(ii)(C)	addressable-164.308(a)(4)(ii)(C)	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(i)	training-program	established deficient	adverse	S-11	D-2	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(i)	training-program: earlier answer, superseded	superseded (overturned)	none: superseded by the later answer	S-10	—	intake round 1; replaced intake round 2, follow-up request 1 (recorded 2026-10-21)	—	Stated: all staff: yes; when: Annual, at the staff meeting; records kept: not sure. Later evidence: Every workforce member receives training: yes → no; When it happens (new hire, annual, both): “Annual, at the staff meeting” → “Never formally; binder says annual” (document read by ePHIShield: HIPAA Policy & Procedure Binder (template, purchased 2017, uncustomized)). Resolution: the later answer stands.
§164.308(a)(5)(i)	training-new-hire	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(i)	training-management	asked, unknown	unknown	S-10	—	intake round 1, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(A)	security-reminders	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)
§164.308(a)(5)(ii)(A)	addressable-164.308(a)(5)(ii)(A)	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(B)	antimalware	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-13	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(a)(5)(ii)(B)	antimalware-monitoring	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(B)	addressable-164.308(a)(5)(ii)(B)	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(C)	login-monitoring	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)
§164.308(a)(5)(ii)(C)	addressable-164.308(a)(5)(ii)(C)	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(D)	password-practices	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(D)	password-sharing	established deficient	adverse	S-11	—	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(5)(ii)(D)	password-sharing: earlier answer, superseded	superseded (overturned)	none: superseded by the later answer	S-10	—	intake round 1; replaced intake round 2, follow-up request 1 (recorded 2026-10-21)	—	Stated: No. Later evidence: answer: no → yes (observed by ePHIShield). Resolution: the later answer stands.
§164.308(a)(6)(i)	incident-policy	asked, unknown	unknown	S-13	D-2	intake round 2 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F); document evidence rejected by ePHIShield
§164.308(a)(6)(i)	incident-procedure-content	asked, unknown	unknown	S-13	D-2	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F); document evidence rejected by ePHIShield
§164.308(a)(6)(ii)	incident-log	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(6)(ii)	incident-detail	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(a)(7)(i)	contingency-plan	asked, unknown	unknown	S-10	—	intake round 1, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(A)	backup-what	asked, unknown	unknown	S-10	—	intake round 1, follow-up request 3 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(A)	backup-coverage	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)
§164.308(a)(7)(ii)(A)	backup-encrypted	asked, unknown	unknown	S-13	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(A)	backup-offsite	asked, unknown	unknown	S-13	—	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(B)	restore-procedure	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(B)	restore-tested	reported	none	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(B)	rto-expectation	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.308(a)(7)(ii)(C)	emergency-mode	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: adverse (Part F)
§164.308(a)(7)(ii)(D)	contingency-test	asked, unknown	unknown	S-12	—	—	practice-wide	—
§164.308(b)(1)	vendor-list	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(b)(1)	ba-agreements	context	none (read vendor by vendor)	S-11	D-3	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.308(b)(1)	ba-agreements: earlier answer, superseded	superseded (overturned)	none: superseded by the later answer	S-14	D-3	intake round 1; replaced intake round 2, follow-up request 1 (recorded 2026-10-21)	—	Stated: all signed: yes; where kept: In the binder or my email. Later evidence: A signed agreement exists for every vendor listed: yes → no; Where the agreements are kept: “In the binder or my email” → “athena PDF in office manager's email” (document read by ePHIShield: athenahealth service agreement with BAA addendum (PDF, 2019)). Resolution: the later answer stands.
§164.308(b)(1)	agreement: athenahealth	documented	supporting	S-11	D-3	agreement recorded 2026-10-21; terms read 2026-10-21	practice-wide	terms read by A. Reviewer (SYNTHETIC), 2026-10-21: compliant (reviewed: safeguards term, subcontractor term, incident-reporting term)
§164.308(b)(1)	agreement: Google	established deficient	adverse	S-15	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(1)	agreement: eFax (Consensus Cloud Solutions)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(1)	agreement: Tri-State Office Systems (SYNTHETIC)	established deficient	adverse	S-17	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(1)	agreement: Valley After-Hours Answering (SYNTHETIC)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(1)	agreement: Kyle Pruitt (SYNTHETIC), independent computer helper	established deficient	adverse	S-18	—	agreement recorded 2026-10-21	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.308(b)(3)	ba-currency	context	none (read vendor by vendor)	S-11	D-3	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.308(b)(3)	agreement: athenahealth	documented	supporting	S-11	D-3	agreement recorded 2026-10-21; terms read 2026-10-21	practice-wide	terms read by A. Reviewer (SYNTHETIC), 2026-10-21: compliant (reviewed: safeguards term, subcontractor term, incident-reporting term)
§164.308(b)(3)	agreement: Google	established deficient	adverse	S-15	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(3)	agreement: eFax (Consensus Cloud Solutions)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(3)	agreement: Tri-State Office Systems (SYNTHETIC)	established deficient	adverse	S-17	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(3)	agreement: Valley After-Hours Answering (SYNTHETIC)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.308(b)(3)	agreement: Kyle Pruitt (SYNTHETIC), independent computer helper	established deficient	adverse	S-18	—	agreement recorded 2026-10-21	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.310(a)(1)	facility-access	established deficient	mixed: supporting on premises are locked or alarmed outside business hours (the measure itself); adverse on premises are locked or alarmed outside business hours (people outside the workforce come and go unescorted)	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(1)	server-location	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(1)	shared-building	context	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(2)(i)	emergency-facility-access	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)
§164.310(a)(2)(i)	addressable-164.310(a)(2)(i)	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(2)(ii)	facility-security-measures	observed	supporting	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(2)(ii)	addressable-164.310(a)(2)(ii)	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.310(a)(2)(iii)	visitor-control	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.310(a)(2)(iii)	addressable-164.310(a)(2)(iii)	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(b)	workstation-use-policy	asked, unknown	unknown	S-13	D-2	intake round 2 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F); document evidence rejected by ePHIShield
§164.310(b)	remote-work	reported	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	requirement ruled not adequate by ePHIShield (A. Reviewer (SYNTHETIC), 2026-10-21; Part F)
§164.310(c)	screen-visibility	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(c)	unattended-workstations	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(1)	device-inventory	established deficient	adverse	S-11	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(1)	device-movement	context	none	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(2)(i)	disposal-process	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(2)(ii)	reuse-process	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(2)(iii)	movement-log	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.310(d)(2)(iii)	addressable-164.310(d)(2)(iii)	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.312(a)(1)	system-access-controls	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-11	D-1	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)
§164.312(a)(2)(i)	unique-ids	established deficient	mixed: supporting on every user has their own log-in (on the other systems recorded), any shared or generic accounts exist (on the other systems recorded); adverse on every user has their own log-in (on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1 and 4 more), any shared or generic accounts exist (on athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1 and 4 more)	S-11	D-1	intake round 2 (recorded 2026-10-21)	adverse on: athenaOne, Google Workspace email, eFax Corporate, Front desk PC 1, Front desk PC 2, Exam room PCs (4), Check-in kiosk tablet, Canon multifunction copier; recorded for 13 systems	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.312(a)(2)(i)	shared-account-detail	established deficient	adverse	S-13	—	intake round 2, follow-up request 1 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(ii)	emergency-access	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iii)	auto-logoff	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iii)	addressable-164.312(a)(2)(iii)	established deficient	adverse	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iv)	encryption-at-rest	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iv)	encryption-mobile	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iv)	encryption-portable	reported	none	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(a)(2)(iv)	addressable-164.312(a)(2)(iv)	established deficient	adverse	S-11	D-2	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(b)	audit-capability	asked, unknown	unknown	S-13	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.312(c)(1)	integrity-controls	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.312(c)(2)	integrity-mechanism	asked, unknown	unknown	S-13	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.312(d)	authentication-method	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)
§164.312(d)	remote-access-mfa	reported	none	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(e)(1)	transmission-methods	reported	none	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.312(e)(1)	email-phi	established deficient	adverse	S-10	—	intake round 1 (recorded 2026-10-21)	practice-wide	—
§164.312(e)(2)(i)	transmission-integrity	asked, unknown	unknown	S-13	—	intake round 2, follow-up request 2 (recorded 2026-10-21)	practice-wide	—
§164.312(e)(2)(i)	addressable-164.312(e)(2)(i)	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.312(e)(2)(ii)	transmission-encryption	established deficient	mixed: read by ePHIShield as partly establishing it (Part F)	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	read by ePHIShield: partial (Part F)
§164.312(e)(2)(ii)	wifi-security	observed	none	S-11	—	intake round 2 (recorded 2026-10-21)	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.312(e)(2)(ii)	wifi-security: earlier answer, superseded	superseded	none: superseded by the later answer	S-13	—	intake round 2; replaced later in the same round (recorded 2026-10-21)	—	Stated: guest network: yes; separated: not sure; who knows password: All staff; written on the break room whiteboard. Later evidence: the later answer (observed by ePHIShield). Resolution: clarified by the analyst: SYNTHETIC REHEARSAL. Clarified from the on-site observation recorded in the inventory: the guest Wi-Fi is on the same network as the practice PCs. 'Not sure' was the respondent's knowledge, not the observed configuration..
§164.312(e)(2)(ii)	addressable-16 4.312(e)(2)(ii)	established deficient	adverse	S-13	—	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.314(a)(1)	ba-contract-terms	context	none (read vendor by vendor)	S-11	D-3	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.314(a)(1)	agreement: athenahealth	documented	supporting	S-11	D-3	agreement recorded 2026-10-21; terms read 2026-10-21	practice-wide	terms read by A. Reviewer (SYNTHETIC), 2026-10-21: compliant (reviewed: safeguards term, subcontractor term, incident-reporting term)
§164.314(a)(1)	agreement: Google	established deficient	adverse	S-15	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(1)	agreement: eFax (Consensus Cloud Solutions)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(1)	agreement: Tri-State Office Systems (SYNTHETIC)	established deficient	adverse	S-17	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(1)	agreement: Valley After-Hours Answering (SYNTHETIC)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—

Requirement	Question	Evidence	Contribution	Source	Documents	Recorded	Systems	Ruling
§164.314(a)(1)	agreement: Kyle Pruitt (SYNTHETIC), independent computer helper	established deficient	adverse	S-18	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(2)(i)	ba-incident-reporting	context	none (read vendor by vendor)	S-11	D-3	intake round 2 (recorded 2026-10-21)	practice-wide	—
§164.314(a)(2)(i)	agreement: athenahealth	documented	supporting	S-11	D-3	agreement recorded 2026-10-21; terms read 2026-10-21	practice-wide	terms read by A. Reviewer (SYNTHETIC), 2026-10-21: compliant (reviewed: safeguards term, subcontractor term, incident-reporting term)
§164.314(a)(2)(i)	agreement: Google	established deficient	adverse	S-15	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(2)(i)	agreement: eFax (Consensus Cloud Solutions)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(2)(i)	agreement: Tri-State Office Systems (SYNTHETIC)	established deficient	adverse	S-17	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(2)(i)	agreement: Valley After-Hours Answering (SYNTHETIC)	not provided	unknown	S-16	—	agreement recorded 2026-10-21	practice-wide	—
§164.314(a)(2)(i)	agreement: Kyle Pruitt (SYNTHETIC), independent computer helper	established deficient	adverse	S-18	—	agreement recorded 2026-10-21	practice-wide	—

H-11. Historical source wording for combined work

This schedule is a historical record for the assessor. It is not part of the action plan and gives the practice no instruction. Where more than one step in the draft plan described the same act, the plan carries that act once, in Part G, and the other steps point to it. The wording each source step originally used is kept here, unchanged, so the combination can be audited. Nothing in the first four columns is work to perform, and nothing here records that any work has been done.

Google agreement: one act, carried at Item 2

Where it appears	Original wording (historical, not an instruction)	Text replaced in this report	How the report treats it
Item 2	Accept Google's Workspace business associate agreement in the admin console (a same-day administrator action).	None; not replaced	Carries the act (the instruction in Part G)
Item 24 (in the row with Item 20)	Stop placing new patient information in a service with no agreement until it has one: accept Google's Workspace business associate agreement in the admin console; obtain the eFax and Valley agreements, or move faxing to a plan that carries one and route after-hours messages to an address covered by one. The agreement step in the plan remains the contractual record; this step limits what reaches the services until then.	accept Google's Workspace business associate agreement in the admin console	Points to Item 2; the act is not repeated here
Item 20	Execute a business associate agreement with Google and Tri-State Office Systems (SYNTHETIC) (none is in place). Until each is executed, stop or limit what ePHI reaches that vendor. If the support of Kyle Pruitt (SYNTHETIC), independent computer helper continues, execute an agreement before any further access to ePHI; if the support ends, end the access instead. Each new or replacement agreement contains the terms §164.314(a)(2)(i) requires: the business associate complies with the applicable requirements of the Security Rule, ensures that its subcontractors that handle ePHI agree to the same, and reports to the practice any security incident of which it becomes aware, including breaches of unsecured protected health information as §164.410 requires (ePHIShield recommends a reporting period of no more than five calendar days). The executed agreement with athenahealth, read and found to contain the required terms, stands; it is not re-executed. Keep a register reconciling every vendor with ePHI access to its executed agreement. For eFax (Consensus Cloud Solutions) and Valley After-Hours Answering (SYNTHETIC): obtain the executed business associate agreement with eFax (Consensus Cloud Solutions) and Valley After-Hours Answering (SYNTHETIC) (none was produced when requested; whether one exists is not established); where none exists, execute one before any further disclosure.	Google's name in the opening instruction and in the list of evidence to keep	Points to Item 2; the act is not repeated here

Decision: the sources describe one act. Basis for treating them as one (baa accept): Google's Workspace business associate agreement is Google's standard click-through amendment, accepted by an administrator in the Workspace admin console; there is no negotiated contract to sign. Rationale: The reviewer's same-day step, the follow-on sub-point and the agreements project's Google portion all describe the one administrator act of accepting Google's standard

agreement; the project's word 'execute' is the engine's generic wording for an agreement not yet in force. Tri-State, the computer helper, eFax and Valley are different vendors and stay as separate work. Recorded by Synthetic rehearsal reviewer (ePHIShield analyst role), 2026-10-22 (record WE-001). The decision lapses and the question reopens if any source wording above changes.