HIPAA Safeguards Covered by PDX IT Gold

PDX Information Technology Services | pdxittech.com | Portland, Oregon area

Which HIPAA Security Rule safeguards (45 CFR Part 164, Subpart C) PDX IT services under the Gold plan cover today, and how.

Practice name:	Completed by:	Date:

Included in the PDX IT Gold plan

- ✓ Free initial IT assessment
- ✓ No setup fee
- ✓ EDR (endpoint detection and response) malware protection
- ✓ Dark web monitoring
- ✓ Automated monitoring and patching
- ✓ After-hours support
- ✓ VoIP phone support
- ✓ HIPAA-related support at no extra cost
- ✓ Signed Business Associate Agreement (BAA)

Support is provided on a best-effort basis; the plan does not include service level agreements or guaranteed response times.

How to use this worksheet

- Every HIPAA Security Rule safeguard is listed. Covered (green) means PDX IT services under the Gold plan handle it today. Not covered (red) means it is not part of the Gold plan and remains with your practice.
- For each item, check Yes if it is in place at your practice, No if it is not yet set up, or N/A if it does not apply. Use Notes for follow-ups or questions for PDX IT.
- Citations refer to Title 45 of the Code of Federal Regulations (CFR), Part 164.

Section 1: Administrative safeguards

45 CFR 164.308. Policies, people and planning that manage how ePHI is protected.

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Risk analysis (Required) 45 CFR 164.308(a)(1)(ii)(A) Accurate, thorough assessment of risks to the confidentiality, integrity and availability of ePHI.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Risk management (Required) 45 CFR 164.308(a)(1)(ii)(B) Security measures that reduce identified risks to a reasonable and appropriate level.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Sanction policy (Required) 45 CFR 164.308(a)(1)(ii)(C) Consequences for workforce members who do not follow security policies.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Information system activity review (Required) 45 CFR 164.308(a)(1)(ii)(D) Regular review of audit logs, access reports and security incident reports.	Covered	Automated monitoring of managed computers plus review of Microsoft 365 sign-in and audit activity as part of Microsoft 365 account administration.	☐	☐	☐	
Assigned security official (Required) 45 CFR 164.308(a)(2) One named person responsible for security policies and procedures.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Workforce authorization and/or supervision (Addressable) 45 CFR 164.308(a)(3)(ii)(A) Staff who work with ePHI, or where it can be accessed, are authorized or supervised.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Workforce clearance procedure (Addressable) 45 CFR 164.308(a)(3)(ii)(B) Process to confirm a person's access to ePHI is appropriate before granting it.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Termination procedures (account access removal) (Addressable) 45 CFR 164.308(a)(3)(ii)(C) Remove accounts and access promptly when someone leaves.	Covered	When you tell us someone has left, we disable their Microsoft 365 account, reset access and remove them from managed systems.	☐	☐	☐	
Access authorization (Addressable) 45 CFR 164.308(a)(4)(ii)(B) Policy for who approves access to systems that hold ePHI.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Access establishment and modification (Addressable) 45 CFR 164.308(a)(4)(ii)(C) Process to set up, review and change user access as roles change.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Security reminders (Addressable) 45 CFR 164.308(a)(5)(ii)(A) Ongoing security updates and awareness reminders for staff.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Protection from malicious software (Addressable) 45 CFR 164.308(a)(5)(ii)(B) Anti-malware tools to detect, guard against and report malware.	Covered	EDR (endpoint detection and response) malware protection on managed computers, plus automated patching.	☐	☐	☐	
Log-in monitoring (Addressable) 45 CFR 164.308(a)(5)(ii)(C) Monitor log-in attempts and report discrepancies.	Covered	Microsoft 365 sign-in monitoring as part of Microsoft 365 account administration, plus dark web monitoring for exposed staff credentials.	☐	☐	☐	
Password management (Addressable) 45 CFR 164.308(a)(5)(ii)(D) Procedures for creating, changing and protecting passwords.	Covered	Password and MFA policies set through Microsoft 365 account administration; dark web monitoring alerts us to leaked credentials so passwords can be reset.	☐	☐	☐	
Security incident response and reporting (Required) 45 CFR 164.308(a)(6)(ii) Identify, respond to, reduce harm from and document security incidents.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Data backup plan (Required) 45 CFR 164.308(a)(7)(ii)(A) Create and keep retrievable exact copies of ePHI.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Disaster recovery plan (Required) 45 CFR 164.308(a)(7)(ii)(B) Procedures to restore any loss of data.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Emergency mode operation plan (Required) 45 CFR 164.308(a)(7)(ii)(C) Keep critical processes running and ePHI protected during an emergency.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Testing and revision of contingency plans (Addressable) 45 CFR 164.308(a)(7)(ii)(D) Periodically test backup and recovery plans and update them.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Applications and data criticality analysis (Addressable) 45 CFR 164.308(a)(7)(ii)(E) Rank which systems and data matter most for recovery.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Periodic evaluation (Required) 45 CFR 164.308(a)(8) Periodic technical and non-technical review of your security program, including after changes.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Business associate agreement with PDX IT (Required) 45 CFR 164.308(b)(1) and (b)(3) Signed agreements with vendors that create, receive, keep or send ePHI for you.	Covered	PDX IT signs a Business Associate Agreement (BAA) with your practice. Covers PDX IT only, not your other vendors.	☐	☐	☐	

Coverage reflects PDX IT services under the Gold plan; the client remains responsible for its own HIPAA compliance program. Planning aid, not legal advice.

Section 2: Physical safeguards

45 CFR 164.310. Protecting your office, workstations, devices and media.

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Contingency operations (Addressable) 45 CFR 164.310(a)(2)(i) Facility access to support restoring data during an emergency.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Facility security plan (Addressable) 45 CFR 164.310(a)(2)(ii) Protect the facility and equipment from unauthorized access, tampering and theft.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Access control and validation procedures (Addressable) 45 CFR 164.310(a)(2)(iii) Control and validate a person's access to facilities based on role, including visitors.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Maintenance records (Addressable) 45 CFR 164.310(a)(2)(iv) Record repairs and changes to physical security (doors, locks, walls, hardware).	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Workstation use (Required) 45 CFR 164.310(b) Rules for how workstations that access ePHI are used and where they are placed.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Workstation security (Required) 45 CFR 164.310(c) Physical safeguards that limit workstation access to authorized users.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Disposal (Required) 45 CFR 164.310(d)(2)(i) Securely wipe or destroy ePHI and the hardware or media it is stored on.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Media re-use (Required) 45 CFR 164.310(d)(2)(ii) Remove ePHI from electronic media before it is reused.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Accountability (hardware and media tracking) (Addressable) 45 CFR 164.310(d)(2)(iii) Record the movement of hardware and media and who is responsible for it.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Data backup and storage before moving equipment (Addressable) 45 CFR 164.310(d)(2)(iv) Make a retrievable exact copy of ePHI before equipment is moved.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Section 3: Technical safeguards

45 CFR 164.312. Technology controls on systems that store or send ePHI.

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Unique user identification (Required) 45 CFR 164.312(a)(2)(i) Every user has their own login name or number. No shared accounts.	Covered	Individual named Microsoft 365 accounts for each user, set up and maintained through Microsoft 365 account administration.	☐	☐	☐	
Emergency access procedure (Required) 45 CFR 164.312(a)(2)(ii) A way to get needed ePHI during an emergency.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Automatic logoff (Addressable) 45 CFR 164.312(a)(2)(iii) Sessions lock or end after a set period of inactivity.	Covered	Screen lock and sign-in timeout settings applied to managed computers and Microsoft 365.	☐	☐	☐	
Encryption and decryption (data at rest) (Addressable) 45 CFR 164.312(a)(2)(iv) Encrypt stored ePHI on servers, laptops, phones and backups.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Audit controls (Required) 45 CFR 164.312(b) Hardware, software or procedures that record and examine activity in systems with ePHI.	Covered	Microsoft 365 audit logging kept turned on and reviewed as part of Microsoft 365 account administration, plus automated monitoring of managed computers.	☐	☐	☐	
Integrity controls (Required) 45 CFR 164.312(c)(1) Policies that protect ePHI from improper change or destruction.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Mechanism to authenticate ePHI (Addressable) 45 CFR 164.312(c)(2) A way to confirm ePHI has not been changed or destroyed without authorization.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Person or entity authentication (Required) 45 CFR 164.312(d) Verify that a person or system seeking access is who they claim to be.	Covered	Multi-factor authentication (MFA) set up and enforced on Microsoft 365 accounts.	☐	☐	☐	

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Transmission integrity controls (Addressable) 45 CFR 164.312(e)(2)(i) Make sure ePHI sent over a network is not improperly changed without detection.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Transmission encryption (Addressable) 45 CFR 164.312(e)(2)(ii) Encrypt ePHI sent by email, file transfer, remote access or other networks.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Section 4: Organizational requirements and documentation

45 CFR 164.314 and 164.316. Vendor agreements, written policies and record keeping.

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Business associate contract with PDX IT (Required) 45 CFR 164.314(a) Agreement requires the vendor to safeguard ePHI, report incidents and flow terms down to subcontractors.	Covered	Signed BAA between PDX IT and your practice. Agreements with your other vendors remain with your practice.	☐	☐	☐	
Group health plan requirements (if applicable) (Required) 45 CFR 164.314(b) Plan documents require the plan sponsor to safeguard ePHI. Mark N/A if not a group health plan.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Written policies and procedures (Required) 45 CFR 164.316(a) Reasonable and appropriate written policies and procedures for each safeguard.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Documentation in writing (Required) 45 CFR 164.316(b)(1) Policies, procedures, actions, activities and assessments kept in written or electronic form.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Time limit (six-year retention) (Required) 45 CFR 164.316(b)(2)(i) Keep documentation six years from creation or the date it was last in effect, whichever is later.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Availability (Required) 45 CFR 164.316(b)(2)(ii) Documentation is available to the people responsible for carrying out the procedures.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Updates (Required) 45 CFR 164.316(b)(2)(iii) Review documentation periodically and update it after environmental or operational changes.	Not covered	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Section 5: Proposed changes (not yet in effect)

Use this section to plan ahead. These items are not current requirements.

PROPOSED (HHS proposed rule, January 6, 2025) - not final; HHS currently targets July 2027 for final action. These items are not current legal requirements and may change before any final rule.

Safeguard	Covered by PDX IT Gold	How	Yes	No	N/A	Notes
Encryption of ePHI at rest and in transit, mandatory (Proposed) **Proposed revision to 45 CFR 164.312** Encryption would be required, with limited exceptions.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Multi-factor authentication (MFA) required (Proposed) **Proposed revision to 45 CFR 164.312** MFA for access to systems with ePHI, with limited exceptions.	**Covered**	MFA set up and enforced on Microsoft 365 accounts through Microsoft 365 account administration.	☐	☐	☐	
Annual compliance audit (Proposed) **Proposed revision to 45 CFR 164.308** Audit compliance with the Security Rule at least once every 12 months.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Restore critical systems and data within 72 hours (Proposed) **Proposed revision to 45 CFR 164.308** Written procedures to restore relevant electronic systems and data within 72 hours of a loss.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Written technology asset inventory and network map (Proposed) **Proposed revision to 45 CFR 164.308** Inventory of hardware, software and data plus a map of how ePHI moves through your systems, reviewed at least yearly.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Vulnerability scans every 6 months and annual penetration test (Proposed) **Proposed revision to 45 CFR 164.312** Automated scans at least every six months and a penetration test at least every 12 months.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	
Removal of required / addressable distinction (Proposed) **Proposed revision to 45 CFR 164.306 and Subpart C** All implementation specifications would become required, with specific limited exceptions.	**Not covered**	*Not part of PDX IT Gold services. Your practice owns this safeguard.*	☐	☐	☐	

Reviewed with PDX IT Services by:	Next review date:

Coverage reflects PDX IT services under the Gold plan; the client remains responsible for its own HIPAA compliance program. Planning aid, not legal advice.