ZENOPS PRACTICAL GUIDE

A MEDICAL PRACTICE CHECKLIST FOR

HIPAA SECURITY
RISK ANALYSIS CHECKLIST

A working checklist for documenting ePHI risks, safeguards, and next actions

SCOPE • ASSESS • DOCUMENT • IMPROVE

Matthew Bowley
CEO, Zenops, Inc.

2026 Edition

HOW TO USE THIS CHECKLIST

Turn review work into evidence

This checklist is designed for a medical practice, clinic, or small healthcare organization that needs a practical way to organize a HIPAA Security Rule risk analysis. It helps the team document scope, ePHI locations, threats, vulnerabilities, safeguards, risk decisions, and follow-up actions in one working packet.

A completed checklist is not a certification and does not by itself establish HIPAA compliance. Use it with the current Security Rule, your organization's facts, applicable state and contractual requirements, and advice from qualified privacy, security, or legal professionals when needed.

DO NOT INCLUDE PATIENT DATA Use system names, record identifiers, screenshots with sensitive details removed, and summaries. Do not paste actual patient information into this checklist.

The working sequence

1. Define the assessment scope, participants, method, and review period.
2. Identify where ePHI is created, received, maintained, or transmitted, including vendors and remote access.
3. Record reasonably anticipated threats and vulnerabilities, then evaluate likelihood and potential impact.
4. Document existing safeguards and the evidence that supports each conclusion.
5. Turn material findings into an owned, dated risk-management plan and approve the next review date.

Status key

Status	Use when
Complete	The practice reviewed the item and retained enough evidence to support the conclusion.
Partial	Some control or evidence exists, but coverage, consistency, or documentation is incomplete.
No	The safeguard or process is absent, not operating, or not yet verified.
N/A	The practice documented why the item does not apply to its environment.
Action needed	A risk or evidence gap needs an owner, priority, and due date.

SECTION 1

Practice profile and assessment method

Start by making the boundaries and decision rules visible.

A reviewer should be able to tell what organization, locations, systems, people, vendors, and time period this assessment covers. If something is outside the boundary, write down why and where it is handled instead.

Field	Entry
Practice / legal entity	_____
Locations included	_____
Assessment lead	Name / title: _____
Participants	Clinical: _____ Operations: _____ IT: _____ Vendor: _____
Assessment period	Start: _____ End: _____
Last review / next review	Last: _____ Next: _____
Scope statement	_____ _____
Method / rating scale	_____

Scope readiness

	Review item	Status / notes
☐	The assessment sponsor or practice leader approved the scope and participants.	Yes / Partial / No / N/A Notes: _____
☐	All practice locations, departments, and remote-work arrangements were considered.	Yes / Partial / No / N/A Notes: _____
☐	Covered-entity and business-associate relationships were identified for the services in scope.	Yes / Partial / No / N/A Notes: _____
☐	The review period and any changes since the last review are documented.	Yes / Partial / No / N/A Notes: _____
☐	The risk-rating method, definitions, and approval threshold are written down.	Yes / Partial / No / N/A Notes: _____
☐	The practice has a secure location for the completed assessment and supporting evidence.	Yes / Partial / No / N/A Notes: _____

PRACTICAL TEST If a new EHR, clinic location, telehealth service, cloud application, medical device, or vendor could change how ePHI is handled, treat that change as a trigger to revisit the analysis.

SECTION 2

Identify ePHI, systems, and data movement

You cannot assess a risk that the practice has not located.

Inventory the places where ePHI is created, received, maintained, or transmitted. Include systems that staff may not think of as clinical systems: email, shared drives, file-transfer tools, scanned documents, mobile devices, backups, printers, fax services, payment or billing systems, and vendor portals.

Technology and ePHI inventory

System / process	ePHI or critical data	Where / who / vendor	Owner / evidence
EHR / practice management	_____	_____	_____
Email / calendar / messaging	_____	_____	_____
Patient portal / telehealth	_____	_____	_____
Billing / claims / payments	_____	_____	_____
Lab / imaging / medical devices	_____	_____	_____
File storage / scanning / fax	_____	_____	_____
Backups / disaster recovery	_____	_____	_____
Endpoints / mobile / remote access	_____	_____	_____
Network / Wi-Fi / printers	_____	_____	_____
Other system or workflow	_____	_____	_____

Inventory prompts

	Review item	Status / notes
☐	The inventory covers ePHI at rest, in use, and in transit, not only the primary EHR.	Yes / Partial / No / N/A Notes: _____
☐	Cloud services, hosted systems, APIs, integrations, and remote-support tools are listed.	Yes / Partial / No / N/A Notes: _____
☐	Local files, downloads, exports, spreadsheets, scanned documents, fax queues, and printed output were considered.	Yes / Partial / No / N/A Notes: _____
☐	Backups, snapshots, archives, disaster-recovery copies, and removable media were considered.	Yes / Partial / No / N/A Notes: _____
☐	Medical devices and building or security systems that connect to the practice network were considered.	Yes / Partial / No / N/A Notes: _____
☐	Shadow systems, personal devices, texting tools, and unsanctioned applications were considered.	Yes / Partial / No / N/A Notes: _____
☐	Each system has an owner, business purpose, location, and vendor or business-associate relationship where relevant.	Yes / Partial / No / N/A Notes: _____

SECTION 3

Map data flows and trust boundaries

Follow the handoffs that create exposure between people, systems, and vendors.

A simple data-flow map can be a drawing, a table, or an annotated network diagram. It should show how ePHI moves between the practice, workforce members, patients, service providers, and external systems. Record the safeguards at each handoff and the owner responsible for the connection.

KEEP IT USEFUL The map does not need to be a network-engineering diagram. It needs to help a reviewer see where ePHI travels, where access is granted, and where a failure could affect confidentiality, integrity, or availability.

From	To	Medium / integration	ePHI?	Safeguard / owner
_____	_____	_____	Yes / No	_____
_____	_____	_____	Yes / No	_____
_____	_____	_____	Yes / No	_____
_____	_____	_____	Yes / No	_____
_____	_____	_____	Yes / No	_____
_____	_____	_____	Yes / No	_____

Data-flow review

	Review item	Status / notes
☐	The practice can identify how patients, clinicians, staff, and vendors access each critical system.	Yes / Partial / No / N/A Notes: _____
☐	External email, portal, text, fax, file-transfer, and API paths were considered.	Yes / Partial / No / N/A Notes: _____
☐	Remote access paths identify the person or vendor, authentication method, device, and approval owner.	Yes / Partial / No / N/A Notes: _____
☐	The practice documented where data is copied, exported, cached, printed, or retained during a workflow.	Yes / Partial / No / N/A Notes: _____
☐	Trust boundaries and high-risk handoffs have an owner and a safeguard review.	Yes / Partial / No / N/A Notes: _____
☐	The map was updated for recent changes or the practice documented why no change was needed.	Yes / Partial / No / N/A Notes: _____

SECTION 4

Identify threats and vulnerabilities

Write down what could go wrong before deciding how much risk remains.

Consider reasonably anticipated threats and the conditions that could allow them to succeed. A threat is an event or actor; a vulnerability is a weakness or gap that could be exploited or could make the event more harmful. Record both. Avoid treating a control list as proof that the analysis is complete.

People and process

	Review item	Status / notes
☐	Phishing, business-email compromise, credential theft, or an unexpected MFA prompt.	Yes / Partial / No / N/A Notes: _____
☐	Shared accounts, generic credentials, weak passwords, or unapproved password storage.	Yes / Partial / No / N/A Notes: _____
☐	Access remaining after termination, role change, contractor departure, or vendor offboarding.	Yes / Partial / No / N/A Notes: _____
☐	Excessive access, unreviewed administrator privileges, or weak separation of duties.	Yes / Partial / No / N/A Notes: _____
☐	A staff member sending ePHI to the wrong recipient, device, number, or application.	Yes / Partial / No / N/A Notes: _____
☐	Inconsistent security training, unclear reporting, or fear of reporting mistakes quickly.	Yes / Partial / No / N/A Notes: _____
☐	A workaround, manual process, or exception that is common but not documented or approved.	Yes / Partial / No / N/A Notes: _____

Technology and configuration

	Review item	Status / notes
☐	Unsupported operating systems, devices, applications, or medical equipment.	Yes / Partial / No / N/A Notes: _____
☐	Unpatched software, exposed services, known vulnerabilities, or weak default configurations.	Yes / Partial / No / N/A Notes: _____
☐	Missing MFA, weak authentication, unmanaged devices, or insecure remote access.	Yes / Partial / No / N/A Notes: _____
☐	Insufficient endpoint protection, network separation, encryption, logging, or monitoring.	Yes / Partial / No / N/A Notes: _____
☐	Email forwarding, external sharing, mobile access, or cloud settings that are not reviewed.	Yes / Partial / No / N/A Notes: _____
☐	Backups that are unprotected, incomplete, inaccessible, or not tested through a restore.	Yes / Partial / No / N/A Notes: _____
☐	Single points of failure in the EHR, network, phone, or vendor service.	Yes / Partial / No / N/A Notes: _____

Physical, environmental, and third-party

	Review item	Status / notes
☐	Lost, stolen, unattended, or improperly disposed laptops, phones, tablets, drives, or paper records.	Yes / Partial / No / N/A Notes: _____
☐	Unauthorized physical access to work areas, server/network equipment, medication areas, or records storage.	Yes / Partial / No / N/A Notes: _____
☐	Fire, flood, power loss, temperature, construction, or other environmental disruption.	Yes / Partial / No / N/A Notes: _____
☐	A vendor or business associate that handles ePHI without clear responsibilities, evidence, or escalation paths.	Yes / Partial / No / N/A Notes: _____
☐	A subcontractor, integration, support tool, or managed service that is not visible in the inventory.	Yes / Partial / No / N/A Notes: _____
☐	Unclear notification, backup, recovery, data-return, deletion, or exit obligations in a vendor relationship.	Yes / Partial / No / N/A Notes: _____

DO NOT SKIP AVAILABILITY A risk analysis is not only about unauthorized disclosure. Consider how ransomware, outage, equipment failure, or vendor unavailability could affect safe care and access to ePHI.

SECTION 5

Review safeguards and supporting evidence

Document what is actually in place, not what a policy or vendor brochure says should be in place.

For each safeguard, record the current state and the evidence that supports it. Evidence may include a policy, configuration export, access review, ticket, training record, backup report, restore test, vendor agreement, network diagram, or interview note. Keep evidence references specific enough that another reviewer can find them.

Domain	Safeguard to verify	Status	Evidence
Administrative	Security policies and procedures are approved, available, and reviewed.	C / P / N / N/A	_____
Administrative	Risk management actions have owners, dates, status, and approval for accepted risk.	C / P / N / N/A	_____
Administrative	Workforce access is approved, changed, and removed through a defined process.	C / P / N / N/A	_____
Administrative	Security awareness and role-specific training are assigned and documented.	C / P / N / N/A	_____
Administrative	Security incident reporting, response, and escalation procedures are documented.	C / P / N / N/A	_____

Domain	Safeguard to verify	Status	Evidence
Administrative	Downtime, contingency, backup, and disaster-recovery procedures are documented and tested.	C / P / N / N/A	_____
Administrative	Business associates and relevant suppliers are identified and reviewed.	C / P / N / N/A	_____
Physical	Facility access, workstations, records storage, and equipment areas are protected.	C / P / N / N/A	_____
Physical	Devices and media are received, moved, reused, sanitized, and disposed of securely.	C / P / N / N/A	_____
Physical	Environmental controls and power or connectivity dependencies are understood.	C / P / N / N/A	_____
Technical	Users have unique accounts; privileged access is separated and reviewed.	C / P / N / N/A	_____
Technical	MFA is enabled for email, remote access, administrator accounts, and other high-risk systems where supported.	C / P / N / N/A	_____
Technical	Access follows least privilege and is reviewed on a defined schedule.	C / P / N / N/A	_____
Technical	Supported systems are patched and vulnerabilities are tracked through closure or documented exception.	C / P / N / N/A	_____
Technical	Endpoints, servers, mobile devices, and medical devices have appropriate protection and monitoring.	C / P / N / N/A	_____
Technical	ePHI is protected in transit and at rest where the risk and system support it.	C / P / N / N/A	_____
Technical	Email, portal, remote-support, external-sharing, and mobile-access settings are reviewed.	C / P / N / N/A	_____
Technical	Audit controls and logs are enabled for systems where access or activity needs review.	C / P / N / N/A	_____
Technical	Backups are protected from ordinary compromise or deletion and restore testing is documented.	C / P / N / N/A	_____
Technical	Network, Wi-Fi, remote access, and internet-exposed services are configured and reviewed.	C / P / N / N/A	_____

EVIDENCE RULE If the practice cannot locate the evidence, record the item as unverified or partial rather than assuming the safeguard is operating.

SECTION 6

Rate and document material risks

Use a consistent method, then explain the judgment behind the rating.

The HIPAA Security Rule does not require one specific scoring formula. The example below is a practical way to make decisions repeatable. Your practice may use another method if it documents the definitions, applies them consistently, and explains why a risk is prioritized, mitigated, transferred, avoided, or accepted.

Example likelihood scale

Score	Meaning
1 - Rare	Unlikely in the current environment; strong safeguards and few exposure paths.
2 - Unlikely	Possible but not expected; exposure or weakness is limited.
3 - Possible	Credible event or recurring weakness; reasonable opportunity exists.
4 - Likely	Expected or has occurred in the practice or a comparable environment.
5 - Almost certain	Active exposure, repeated event, or very weak control conditions.

Example impact scale

Score	Meaning
1 - Limited	Minimal effect on confidentiality, integrity, availability, operations, or patient care.
2 - Minor	Contained effect with limited disruption, exposure, or recovery effort.
3 - Moderate	Material operational, privacy, security, financial, or patient-care effect.
4 - Major	Significant disruption, broad exposure, extended outage, or difficult recovery.
5 - Severe	Potentially widespread or prolonged effect on ePHI, safe care, or the practice.

RATING REMINDER A score is not the analysis. The rationale, evidence, affected ePHI, current safeguards, and treatment decision are what make the record useful.

Risk record 1

Asset / process	_____
Threat / vulnerability	_____ _____
ePHI affected	Confidentiality / Integrity / Availability / Not applicable
Current safeguards and evidence	_____ _____
Likelihood / impact / rating	Likelihood: ____ Impact: ____ Inherent risk: ____ Residual risk: ____
Rationale	_____ _____
Treatment decision	Mitigate / Transfer / Avoid / Accept with approval / Further analysis
Owner / due date / status	Owner: _____ Due: _____ Status: _____

Risk record 2

Asset / process	_____
Threat / vulnerability	_____ _____
ePHI affected	Confidentiality / Integrity / Availability / Not applicable
Current safeguards and evidence	_____ _____
Likelihood / impact / rating	Likelihood: ____ Impact: ____ Inherent risk: ____ Residual risk: ____
Rationale	_____ _____
Treatment decision	Mitigate / Transfer / Avoid / Accept with approval / Further analysis
Owner / due date / status	Owner: _____ Due: _____ Status: _____

Risk record 3

Asset / process	_____
Threat / vulnerability	_____ _____
ePHI affected	Confidentiality / Integrity / Availability / Not applicable
Current safeguards and evidence	_____ _____
Likelihood / impact / rating	Likelihood: ____ Impact: ____ Inherent risk: ____ Residual risk: ____
Rationale	_____ _____
Treatment decision	Mitigate / Transfer / Avoid / Accept with approval / Further analysis
Owner / due date / status	Owner: _____ Due: _____ Status: _____

SECTION 7

Turn findings into a risk-management plan

The analysis identifies risk; the plan decides what the practice will do about it.

Prioritize the risks that could most affect patient care, ePHI confidentiality, integrity, or availability. For each material finding, define the action, owner, due date, success measure, and evidence that will show the risk was reduced. If the practice accepts a risk, document who approved the decision and why.

Before closing the analysis

	Review item	Status / notes
☐	Every material risk has a treatment decision and an accountable owner.	Yes / Partial / No / N/A Notes: _____
☐	Priority reflects likelihood, impact, affected ePHI, patient-care impact, and current safeguards.	Yes / Partial / No / N/A Notes: _____
☐	Temporary exceptions have an expiration or review date and a compensating-control owner.	Yes / Partial / No / N/A Notes: _____
☐	Vendor or business-associate actions are assigned to a named practice owner.	Yes / Partial / No / N/A Notes: _____
☐	The plan includes evidence of completion, not only a task marked done.	Yes / Partial / No / N/A Notes: _____
☐	Leadership understands the highest remaining risks and the resources or decisions needed.	Yes / Partial / No / N/A Notes: _____

Findings and action register

ID / risk	Action / success measure	Owner	Priority	Due	Status
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____
_____	_____	_____	H / M / L	_____	_____

MAKE IT MEASURABLE Replace “improve security” with a result someone can verify: 100% of active accounts reviewed, all internet-facing systems patched, a successful restore test completed, or vendor access removed and evidenced.

SECTION 8

Validate, approve, and schedule the next review

A risk analysis is a living management record, not a file created once and forgotten.

Complete this closeout after the assessment lead has reviewed the evidence and the practice has decided how to handle material risks. Keep the completed checklist, supporting evidence references, approved action plan, and sign-off together in a controlled location.

Closeout review

	Review item	Status / notes
☐	The assessment covers all ePHI locations identified in the inventory and data-flow review.	Yes / Partial / No / N/A Notes: _____
☐	Threats, vulnerabilities, existing safeguards, likelihood, impact, and rationale are documented.	Yes / Partial / No / N/A Notes: _____
☐	The review considers administrative, physical, technical, vendor, and availability risks.	Yes / Partial / No / N/A Notes: _____
☐	Open evidence requests are assigned to owners and have due dates.	Yes / Partial / No / N/A Notes: _____
☐	Material risks have treatment decisions, approved exceptions, or a documented request for further analysis.	Yes / Partial / No / N/A Notes: _____
☐	The practice has recorded the next recurring review date and change-trigger conditions.	Yes / Partial / No / N/A Notes: _____

Review triggers

Trigger	Review action
New EHR, portal, telehealth, cloud, AI, billing, or messaging service	Revisit scope, data flow, vendor, access, and safeguards before or during implementation.
New location, merger, acquisition, or major staffing change	Update inventory, physical safeguards, roles, access, and recovery assumptions.
Security incident, suspected breach, ransomware, or significant outage	Reassess the affected risks and document lessons learned and corrective actions.
New medical device, network change, or internet-exposed service	Review asset ownership, segmentation, patching, monitoring, and support dependencies.
Material vendor, contract, BAA, or subcontractor change	Review data handling, access, notification, backup, exit, and evidence obligations.
Recurring review date	Reconfirm the environment, evidence, risk decisions, and action status; set the next date.

Approval and record of review

Role	Name / signature	Date
Practice leader / sponsor	_____	_____
Privacy or security lead	_____	_____
IT / managed service / technical reviewer	_____	_____
Next scheduled review	_____	_____

RETAIN THE RECORD Keep the checklist, risk records, action register, evidence references, approvals, and material updates together. Do not store the working file with live patient data.

APPENDIX A

Evidence request list

Use this as a starting point; tailor it to the systems and workflows in scope.

Evidence should help a reviewer understand what the practice does, what is configured, what was tested, and who is accountable. Redact patient information and secrets before attaching or linking evidence.

Evidence area	Examples to request	Received / location
Governance	Current policies, standards, exception approvals, review records, risk-management plan	_____
Scope and inventory	System inventory, asset list, network or data-flow map, application list	_____
Identity and access	User list, privileged access list, MFA coverage, access review, termination tickets	_____
Endpoint and network	Patch status, endpoint protection, firewall/Wi-Fi review, remote-access list	_____
EHR and cloud	Vendor security documentation, configuration review, audit/log settings, sharing settings	_____
Backup and recovery	Backup reports, retention settings, restore test, downtime procedures, contact list	_____
Incident response	Incident plan, escalation tree, tabletop notes, reporting and notification workflow	_____
Workforce	Training assignments, completion records, phishing reporting process, onboarding/offboarding steps	_____
Physical safeguards	Facility access, workstation security, device/media handling, disposal records	_____
Third parties	BAAs, contracts, vendor reviews, service descriptions, incident and exit commitments	_____
Vulnerability management	Scanning results, remediation tickets, unsupported-system plan, exception records	_____

EVIDENCE HYGIENE Evidence should prove the control without creating a new exposure. Prefer redacted exports, summaries, configuration views, and ticket references over screenshots containing patient data or credentials.

APPENDIX B

Glossary and official resources

Use the sources below to deepen the review and confirm current guidance.

Glossary

ePHI: Electronic protected health information created, received, maintained, or transmitted by a covered entity or business associate.

Risk analysis: An accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Risk management: The process of implementing security measures to reduce identified risks and vulnerabilities to a reasonable and appropriate level.

Threat: An event, actor, or circumstance that could cause harm to ePHI, systems, operations, or safe care.

Vulnerability: A weakness or gap that could be exploited by a threat or could increase the effect of an event.

Likelihood: The estimated chance that a threat will exploit a vulnerability or that an event will occur.

Impact: The potential effect on confidentiality, integrity, availability, operations, finances, compliance, or patient care.

Residual risk: The risk that remains after current safeguards and planned actions are considered.

Business associate: A person or organization that performs certain functions or services involving PHI for a covered entity, as defined by HIPAA.

Safeguard: An administrative, physical, or technical measure used to protect ePHI and support secure operations.

Official resources

HHS: The HIPAA Security Rule. Overview of administrative, physical, and technical safeguards for ePHI. https://www.hhs.gov/hipaa/for-professionals/security/index.html

HHS OCR: Guidance on Risk Analysis. Explains scope, threats, vulnerabilities, safeguards, and documentation considerations. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

HHS / ONC: Security Risk Assessment Tool. A resource intended to help small and medium-sized practices and business associates conduct a risk assessment; it is not a guarantee of compliance. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

HHS Cyber Gateway: Healthcare Cybersecurity Performance Goals. Voluntary healthcare-specific practices that can help prioritize high-impact improvements. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html

NIST Cybersecurity Framework 2.0. A flexible structure for organizing cybersecurity risk governance and management; it does not replace HIPAA requirements. https://www.nist.gov/cyberframework

HHS Security Rule Guidance Materials. Additional educational papers and guidance on risk analysis, administrative, physical, and technical safeguards. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

PUBLICATION NOTE Guidance, enforcement priorities, and technology change. Review current official sources and obtain qualified advice when a decision depends on your specific facts, contracts, or legal obligations.