ZENOPS PRACTICAL GUIDE

A MEDICAL PRACTICE GUIDE TO

CYBERSECURITY
STARTER GUIDE

A practical field guide for protecting patients, systems, staff, and trust

PATIENTS • PEOPLE • PRACTICE

Matthew Bowley
CEO, Zenops, Inc.

2026 Edition

ABOUT THIS GUIDE

How to use this book

This guide is for physicians, practice managers, office leaders, clinical staff, and technology partners who need a practical starting point for protecting a small or midsize medical practice. It focuses on the everyday controls that reduce avoidable disruption and make the practice easier to protect.

You do not need a large security team to make progress. You need clear ownership, a short list of priorities, and habits that protect access to patient information and the systems people rely on to deliver care.

> **CORE IDEA** Cybersecurity is part of patient safety and practice continuity. Protect the systems people need to care for patients, communicate, bill, and recover.

A note on scope

This is an educational field guide, not legal, medical, compliance, or insurance advice. HIPAA obligations depend on your role, contracts, services, and facts. If your practice is a HIPAA covered entity or business associate, use this guide with your privacy or security lead and qualified counsel. Confirm state requirements, payer rules, contracts, and breach-notification duties before relying on a decision.

Contents

CHAPTER 1

Start with the Patient and the Practice

The goal is not perfect security. The goal is a practice that can keep caring for people when something goes wrong.

Medical practices are small operating systems. Scheduling, registration, clinical documentation, prescriptions, lab and imaging results, billing, referrals, patient messages, and staff communication all depend on technology. A cyber event can become a care-delivery problem quickly.

Name what must keep working

Start with services, not products. Ask what the practice must be able to do on a normal day and what it must still do during a technology outage or security event.

1. Register and identify patients safely
2. Access the clinical record or a safe downtime substitute
3. Communicate with patients and care partners
4. Prescribe, order, receive, and review clinical information
5. Process claims, payments, payroll, and urgent vendor support
6. Restore systems without guessing what is trustworthy

> **PATIENT-SAFETY TEST** For each important system, ask: if it were unavailable for one hour, one day, or one week, what would the practice do?

Make ownership visible

A practice may use an EHR vendor, a managed IT provider, a billing company, a lab partner, a cloud phone system, and a payment processor. Those partners may operate important controls, but the practice still needs an owner who can ask questions, approve decisions, and coordinate during an incident.

7. Executive or physician sponsor: sets priorities and accepts risk
8. Practice or operations lead: coordinates workflow and downtime decisions
9. Privacy/security lead or outside advisor: guides safeguards and incident handling
10. System owners: know how each service is configured and supported
11. All staff: protect accounts, report concerns, and follow downtime steps

CHAPTER 2

Understand What You Are Responsible For

Start with the rules that apply to your practice, then build a reasonable plan around the risks you can see.

The HIPAA Security Rule establishes standards for protecting electronic protected health information, or ePHI, with administrative, physical, and technical safeguards. If the Security Rule applies to your organization, risk analysis is a foundational step: identify where ePHI lives, what could harm its confidentiality, integrity, or availability, and what safeguards are reasonable for your environment.

Ask four scope questions

12. Is the practice a HIPAA covered entity, a business associate, or both in different activities?
13. Which systems, devices, people, and vendors create, receive, maintain, or transmit ePHI?
14. Which contracts require a business associate agreement or specific security terms?
15. Which state, payer, professional, insurance, or contractual rules add obligations?

RISK-ANALYSIS RULE A policy binder is not a risk analysis. The analysis should connect threats and vulnerabilities to the systems, information, people, and safeguards in your actual practice.

Use frameworks as organizing tools

The HHS Healthcare and Public Health Cybersecurity Performance Goals are voluntary practices designed to help healthcare organizations prioritize high-impact improvements. NIST Cybersecurity Framework 2.0 provides a flexible way to organize work around Govern, Identify, Protect, Detect, Respond, and Recover. Use these frameworks to structure conversations and track progress; do not treat a framework checklist as a legal certification.

Keep evidence of decisions

Keep a dated risk analysis, action plan, exceptions, review notes, training records, restore-test results, vendor answers, and incident exercises. The value is not paperwork for its own sake. It is being able to show what the practice knew, what it decided, who owned the next step, and when the decision would be revisited.

CHAPTER 3

Find Your Digital Front Door

You cannot protect what you cannot name, and you cannot recover what you have not mapped.

Create a plain-language inventory of the practice's technology and information flows. Include systems operated by vendors. Mark what is connected to what, where ePHI moves, and which accounts can reach each system.

Minimum inventory

16. EHR, practice management, scheduling, e-prescribing, labs, imaging, and clinical devices
17. Patient portal, telehealth, texting, email, fax, and call systems
18. Billing, claims, payment, payroll, HR, accounting, and document storage
19. Laptops, desktops, tablets, phones, servers, routers, printers, and medical devices
20. Cloud services, remote access tools, backups, security tools, and shared accounts
21. Vendors, business associates, support contacts, agreements, and renewal dates

Map the trust boundaries

Area	What to document	Questions to ask
People	Staff, clinicians, contractors, vendors	Who needs access, and who approves it?
Systems	Applications, devices, networks, portals	What depends on what?
Information	ePHI, billing, credentials, backups	Where is it stored, sent, and deleted?
Recovery	Downtime tools, backups, contacts	What can be restored, and how fast?

Look for shadow systems

Staff may use personal email, consumer file sharing, unapproved texting, spreadsheets, or browser extensions when the official workflow is slow. Treat these as signals that a process needs improvement, not as reasons to shame people. Ask what job the workaround is doing, then provide a safer path and retire the workaround.

INVENTORY RULE Every important system should have a business owner, a technical contact, a data description, an access path, a backup or downtime story, and a review date.

CHAPTER 4

Protect Accounts and Devices

Strong identity and well-maintained devices stop many problems before they become patient-impacting events.

Most practices should begin with account and device basics before buying more tools. The controls below are simple to explain, measurable, and useful across the EHR, email, cloud services, remote support, and administrator accounts.

Account fundamentals

22. Use unique accounts for each person. Avoid shared administrator credentials.
23. Turn on multi-factor authentication for email, remote access, administrators, cloud services, and any system that supports it.
24. Use least privilege: give people the access needed for the job, then remove it when the job changes.
25. Review privileged access and inactive accounts on a recurring schedule.
26. Use a managed password manager or another approved method for storing credentials.
27. Have a documented joiner, mover, and leaver process for staff and vendors.

Device fundamentals

28. Install supported operating systems and apply security updates on a defined schedule.
29. Use centrally managed endpoint protection and confirm that it reports health and alerts.
30. Encrypt laptops and mobile devices, use screen locks, and limit local storage of ePHI.
31. Separate guest Wi-Fi from practice systems and use strong, unique network credentials.
32. Control remote support tools and record who can use them, when, and for what purpose.
33. Maintain a replacement plan for unsupported hardware, network equipment, and medical devices.

> **MFA PRIORITY** If you can make only one identity improvement this week, start with email and administrator accounts. Those accounts often unlock many other systems.

Make the safe action the easy action

Staff are more likely to follow a control when it fits the workflow. Use single sign-on where appropriate, make reporting easy, provide a clear exception path, and remove unnecessary steps. Security that slows care without a plan for the real workflow will be bypassed.

CHAPTER 5

Secure Email, Portals, and Patient Information

Patient information often leaves the EHR through ordinary communication channels. Protect the handoffs.

Email and messaging are common paths for phishing, business email compromise, misdirected information, and accidental disclosure. A secure workflow combines technical settings, clear operating rules, and a culture where staff can pause and ask for help.

Make suspicious messages reportable

34. Give every staff member one obvious way to report a suspicious email, text, or call.
35. Teach staff to verify urgent payment, password, wire, gift-card, and record requests using a known contact path.
36. Use phishing-resistant habits: pause, inspect the sender and link, and do not approve an unexpected MFA prompt.
37. Treat unusual requests from a clinician, executive, vendor, or patient as worth verifying.

Protect the message path

38. Use the patient portal or an approved secure messaging method for sensitive clinical information.
39. Confirm addresses, attachments, recipients, and minimum-necessary content before sending.
40. Use approved templates for common patient communications so staff do not improvise risky workflows.
41. Review auto-forwarding, shared inboxes, mobile access, retention, and external sharing settings.
42. Do not assume that a vendor's word 'secure' answers how messages are encrypted, logged, retained, and accessed.

> **TWO-CHANNEL RULE** For a high-risk request, verify through a second channel you initiate yourself. Do not use the phone number or reply path in the suspicious message.

Make reporting blame-free

A fast report is more valuable than a perfect first explanation. Tell staff what to do if they click a link, send information to the wrong person, lose a device, approve an unexpected prompt, or notice unusual activity. Early reporting gives the practice more options.

CHAPTER 6

Backups, Downtime, and Recovery

A backup is only useful if the practice can find it, trust it, and restore from it.

Plan for the practice to be without a key system. The trigger may be ransomware, a vendor outage, a network failure, a lost device, a power event, or a human mistake. Recovery planning is an operational exercise, not only an IT exercise.

Build a recovery story

43. Identify the systems required for safe care, communication, scheduling, and revenue operations.
44. Define a target recovery time for each critical service and what a safe degraded mode looks like.
45. Keep at least one backup or recovery copy protected from ordinary account compromise or deletion.
46. Test restores on a schedule and record what worked, what failed, and who fixes the gap.
47. Keep offline or printed downtime procedures, contact lists, forms, and instructions where staff can reach them.
48. Coordinate recovery assumptions with the EHR, billing, lab, imaging, phone, and IT providers.

Downtime decisions

Question	Write down the answer
Who declares downtime?	Name, backup, and decision trigger
How do clinicians access essential information?	Approved downtime record or vendor procedure
How do patients and partners reach us?	Phone, message, notice, and escalation path
How do we preserve new information?	Paper, local form, queue, and later reconciliation
Who coordinates restoration?	Practice lead, IT, vendors, and communications owner

RESTORE TEST A successful backup job is not the same as a successful restore. Test a real file, system, or workflow and record the result.

Learn from the test

After a downtime exercise, ask what slowed the team down: missing contacts, unclear authority, stale forms, unavailable devices, weak vendor support, or an assumption no one had tested. Fix the highest-impact gap first, then repeat the exercise.

CHAPTER 7

Work with Vendors and Business Associates

Your practice can outsource a service. It cannot outsource the need to understand the dependency.

Vendors may host ePHI, manage devices, connect systems, provide support, process claims, handle payments, or deliver medical devices. Review the relationship before access is granted and again when the service, contract, or risk changes.

Questions for a practical review

49. What information will the vendor handle, and for what purpose?
50. What access will the vendor have, from where, and for how long?
51. Is a business associate agreement required, and does the contract match the service?
52. How are MFA, logging, encryption, backups, vulnerability management, and support access handled?
53. How quickly will the vendor notify the practice about a suspected or confirmed incident?
54. How will data be returned, deleted, or preserved when the relationship ends?
55. What happens if the vendor is unavailable during an outage or incident?

Avoid the questionnaire trap

A completed questionnaire is not proof that a vendor is safe. Compare the vendor's answers to the access it actually receives, ask for evidence where the risk is high, and record open items with owners and dates. A smaller vendor may not have a large compliance team; that does not remove the need for clear answers and an agreed response path.

> **VENDOR RULE** Before a vendor gets access, know what it can reach, why it needs that access, who approves it, how it will be monitored, and how it will be removed.

Keep an exit plan

For every critical service, know how to export data, obtain records, contact support, continue basic operations, and transition to another service if needed. Exit planning is part of continuity planning, not a sign that you expect every vendor relationship to fail.

CHAPTER 8

Prepare for Incidents and Train the Team

The first minutes of an incident are easier when people already know who to call and what not to do.

Write a short incident response plan that people can actually use. It should cover suspected phishing, lost devices, unauthorized access, malware, ransomware, misdirected patient information, vendor incidents, and service outages.

The first-response sequence

56. Report: tell the designated practice and technology contacts immediately.
57. Protect: stop interacting with the suspicious message or device; do not delete evidence.
58. Contain: follow the approved instructions for isolating a device or disabling an account.
59. Coordinate: bring in the IT provider, EHR/vendor contacts, privacy lead, leadership, counsel, and insurer as appropriate.
60. Communicate: use one source of truth and share only what is confirmed and necessary.
61. Recover: restore safely, reconcile records, and document lessons learned.

> **DO NOT GUESS** Do not promise a patient, payer, employee, or vendor that an incident is harmless before the practice completes an appropriate assessment.

Train for the real work

62. New-hire training: accounts, devices, privacy, reporting, and downtime basics
63. Recurring refreshers: phishing, MFA prompts, passwords, portable devices, and patient communications
64. Role-based practice: front desk, clinicians, billing, managers, and administrators face different scenarios
65. Tabletop exercises: a short scenario with a missing device, locked EHR, or vendor outage
66. After-action learning: share improvements without shaming the person who reported the issue

Make the plan findable

Keep the incident contacts, downtime steps, vendor escalation paths, and reporting instructions in more than one accessible place. If the EHR or email is unavailable, the practice should still know how to start the response.

CHAPTER 9

A 30-Day Medical Practice Action Plan

A month is enough time to create ownership, close a few high-impact gaps, and establish a repeatable rhythm.

Timing	Focus	Deliverable
Days 1-5	Ownership and inventory	Named sponsor, contacts, systems, devices, vendors, and critical workflows
Days 6-10	Risk baseline and MFA	Top risks, email/admin MFA, account review, and quick wins
Days 11-15	Patching and recovery	Update plan, endpoint coverage, backup review, and restore test
Days 16-22	Vendors and incident plan	Vendor review, escalation list, downtime steps, and response draft
Days 23-27	Training and exercise	Staff refresher, reporting path, and tabletop scenario
Days 28-30	Review and communicate	Open issues, owners, dates, leadership update, and next review

Days 1-10: see the whole picture

67. Name the practice sponsor, operations owner, privacy/security lead, and technology contacts.
68. Collect the EHR, billing, phone, lab, imaging, payment, email, and support vendor list.
69. List critical systems, devices, users, data, remote access paths, and shared accounts.
70. Turn on MFA for email, administrator, remote-access, and other high-impact accounts.
71. Write down the three highest-consequence gaps and one action for each.

Days 11-20: close the obvious gaps

72. Confirm supported software, patch ownership, endpoint protection, encryption, and screen locks.
73. Review backups and test one restore or one critical downtime workflow.
74. Review vendor access, business associate agreements, contacts, and incident-notification terms.
75. Draft the one-page incident response and downtime quick sheet.

Days 21-30: make it repeatable

76. Train staff on reporting, suspicious messages, unexpected MFA prompts, and lost devices.
77. Run a 30-minute tabletop exercise with leadership, front desk, clinicians, billing, and IT.
78. Document open risks, accepted exceptions, owners, due dates, and the next review date.
79. Share the plan in plain language so staff know what protection looks like in daily work.

NEXT STEP Pick one owner, one critical system, and one action. Put the review date on the calendar before the day ends.

APPENDIX A

Practice Security Baseline Checklist

Use this as a starting conversation. Mark each item Complete, In progress, Not applicable, or Needs an owner. The checklist is not a substitute for a practice-specific risk analysis.

Control area	Baseline question	Status / owner
Ownership	Is there a named practice owner and technology contact?	
Inventory	Are systems, devices, vendors, and ePHI flows documented?	
Identity	Are unique accounts, MFA, least privilege, and offboarding in place?	
Devices	Are supported, patched, protected, encrypted devices managed?	
Messaging	Are secure communication paths and reporting rules clear?	
Recovery	Are backups protected, tested, and paired with downtime steps?	
Vendors	Are access, BAAs, contacts, incident terms, and exit plans reviewed?	
Response	Do staff know how to report, contain, coordinate, and recover?	
Training	Is training recurring, role-based, and reinforced after exercises?	

Evidence to keep

80. Current inventory and network or information-flow notes
81. Risk analysis, action plan, and accepted-risk decisions
82. Access-review and offboarding records
83. Patch, endpoint, backup, and restore-test evidence
84. Vendor review, BAA, support, and incident-contact records
85. Training attendance and tabletop exercise notes

APPENDIX B

Incident Response Quick Sheet

Post this where the practice can reach it during an outage. Fill in names, numbers, and vendor-specific instructions before relying on it.

Practice incident lead: _____ Backup: _____

IT / MSP contact: _____ Phone: _____

EHR / critical vendor support: _____ Account / contract: _____

Privacy / security lead: _____ Counsel / insurer: _____

If something suspicious happens

86. Stop. Do not keep clicking, replying, approving prompts, or deleting messages.
87. Report. Contact the practice incident lead and technology contact using a known path.
88. Protect. Follow instructions to isolate the device or secure the account.
89. Record. Note what happened, when, what device or account was involved, and what actions were taken.
90. Coordinate. Let the designated leads determine next steps and required notifications.

Downtime notes

Critical workflow affected: _____

Downtime procedure or form location: _____

How patients and partners will be contacted: _____

How new information will be reconciled after recovery: _____

> **REMEMBER** Early reporting is a protective action. A fast, honest report gives the practice more options.

APPENDIX C

Vendor and Business Associate Review

Use this form before approving a new critical service, renewing a high-impact vendor, or changing access. Tailor it to the service and risk.

Vendor / service: _____ Business owner: _____

Data handled: _____ Criticality: Low / Med / High

Access granted: _____ Review date: _____

Review questions

91. Is a business associate agreement required and executed?
92. Does the vendor use MFA, unique accounts, logging, encryption, and least privilege?
93. How are vulnerabilities, patches, backups, and subcontractors managed?
94. What is the incident-notification process and expected timing?
95. What support is available during an outage or security event?
96. How will data be returned, deleted, or preserved at the end of the relationship?
97. What open risk, evidence request, or contract change needs an owner and date?

Decision: Approve / Approve with conditions / Hold / Do not proceed

Conditions, owner, and due date: _____

ACCESS RULE No vendor access without a business purpose, an owner, an approved path, and a plan to remove it.

APPENDIX D

Glossary and Official Resources

Glossary

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

Covered entity: A HIPAA-regulated health plan, health care clearinghouse, or health care provider that meets the applicable definition.

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

Least privilege: Giving a person, device, or service only the access needed for the task.

MFA: Multi-factor authentication: using two or more different types of evidence to verify identity.

Ransomware: Malicious software or activity that blocks access to systems or data, often while demanding payment.

Risk analysis: A documented assessment of threats and vulnerabilities that could affect the confidentiality, integrity, or availability of ePHI.

RTO: Recovery time objective: the target time for restoring a service after disruption.

Tabletop exercise: A guided discussion that uses a realistic scenario to test roles, decisions, contacts, and procedures.

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 why risk analysis is a foundational step and what it should consider. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

HHS: Security Risk Assessment Tool. A resource for small and medium-sized practices to identify and assess risks. https://www.hhs.gov/hipaa/for-professionals/security/guidance/security-risk-assessment-tool/index.html

HHS Healthcare and Public Health Cybersecurity Performance Goals. Voluntary essential and enhanced practices for healthcare and public health organizations. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html

CISA: Healthcare and Public Health Cybersecurity. Healthcare-focused cybersecurity and resilience resources. https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

NIST Cybersecurity Framework 2.0. A flexible structure for governing, identifying, protecting, detecting, responding, and recovering from cybersecurity risk. https://www.nist.gov/cyberframework

HHS 405(d) Program. Healthcare and public health cybersecurity practices and publications. https://405d.hhs.gov/

> **NEXT STEP** Choose one critical system, one accountable owner, and one action. Put the next review date on the calendar.