Tiered Technology Framework and Assessment Checklist

HITECH on a Shoestring: Modernizing Practice IT Without Losing the Human Touch | v1.1, November 2026 | © 2026 Kenny Collaborative LLC

Operational guidance, not legal, compliance or financial advice. Confirm requirements with your compliance advisor or attorney.

What this is	A framework that shows what good practice technology looks like in four pillars, which items are required, recommended or optional, and what each typically costs by category. The same rows become a checklist for your practice and a 30/90/180-day roadmap. It names no products.
Time	About 10 minutes to mark the Required rows. About 45 minutes for every row.
Order	1. Read the Framework tab. 2. Mark each row on the My practice tab: Done, Partial, Missing or Not applicable. Add an owner and a target date. 3. Open the Roadmap tab. It fills itself from your answers, Required items first. 4. Use Tabs 3 to 5 as working checklists: offboarding, systems inventory and cyber coverage questions.
Which cells to edit	Light purple cells are yours to fill in. Light gray cells calculate; do not edit them. Row P1-02 on My practice is filled in as an example. Clear it before you start.

The tiers

Required	A HIPAA Security Rule standard or implementation specification applies. That includes addressable specifications: you implement them, or document why an equivalent measure is reasonable and put that measure in place. Addressable does not mean optional.
Best practice	Federal guidance (the HHS Cybersecurity Performance Goals) or common standards recommend it, and the proposed Security Rule update may require it.
Optional	It can help, but it is not required. Score it with the Human Filter Worksheet before you buy it.
On a budget	Not a tier. The On a budget column on the Framework tab gives the lowest-cost route that still meets the need. On the session slides, the On a budget marker refers to this column.

The four pillars

Secure infrastructure	Identity and single sign-on, devices, backups, training and coverage. Rows P1-01 to P1-15.
Clinical systems	The EMR and every system that touches PHI. Rows P2-01 to P2-08. Selection and contracts are covered in session #306, The EMR Dozen.
Patient engagement	Phones, reminders, scheduling, intake and the website. Rows P3-01 to P3-06. The BAA rule from Pillar 2 applies to every vendor here that holds PHI.
Business intelligence	A few numbers with owners, from reports you already have. Rows P4-01 to P4-03.
AI, across all pillars	AI is a capability inside every layer, not a fifth pillar. Rows AI-01 and AI-02.

About the sources

Regulatory basis	HIPAA Security Rule citations (45 CFR Part 164, Subpart C) were checked against the eCFR as of October 23, 2026. (R) marks a required implementation specification and (A) an addressable one; "standard" marks a standard with no separate specification.
Proposed change	Notes marked NPRM refer to the proposed Security Rule update published January 6, 2025. It is not final and is not binding. The current rule remains in force. Federal agenda listings in 2026 moved final action to 2027 or later.
Typical cost	Category-level ranges in US dollars at list price, checked in November 2026 against vendor pricing pages and published small-business pricing surveys. Ranges span several vendors. Prices change; get current quotes before you budget. The productivity suite examples name Google Workspace and Microsoft 365 together because the session compares them; no other products are named.
Free federal tools	HHS Security Risk Assessment Tool (healthit.gov, current version 3.6). HHS Cybersecurity Performance Goals (hphcyber.hhs.gov). 405(d) Health Industry Cybersecurity Practices (405d.hhs.gov).

Framework

HITECH on a Shoestring: Modernizing Practice IT Without Losing the Human Touch | v1.1, November 2026 | © 2026 Kenny Collaborative LLC

Operational guidance, not legal, compliance or financial advice. Confirm requirements with your compliance advisor or attorney.

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
P1-01	Secure infrastructure	**Unique login for every person**	Required	Gives each workforce member their own account so every action can be traced to one person.	• No shared logins on any system that holds PHI • One central account per person (the productivity suite) used to sign in to other apps where possible • Accounts created and disabled by a named owner	164.312(a)(2)(i) unique user identification (R); 164.312(d) person or entity authentication (R)		Included in the productivity suite	Use the suite accounts as the single sign-on for every app that supports it	Separate logins per app with no central off switch	30 days
P1-02	Secure infrastructure	**Multi-factor authentication on every account**	Best practice	Requires a second factor at sign-in so a stolen password alone does not open the account.	• On for every user, admin accounts first • Authenticator app or passkey rather than text message where possible • Backup codes stored by the account owner	CPG Essential: multifactor authentication	NPRM would require MFA for access to systems that hold ePHI, with limited exceptions	$0 (built into both suites and free authenticator apps)	Free authenticator app on each staff member's phone	Hardware keys for every user before basic MFA is on	30 days
P1-03	Secure infrastructure	**Productivity suite (email, files, chat, calendar) under a BAA**	Required	Hosts practice email, files and messaging on business accounts covered by a business associate agreement (BAA).	• Business or enterprise plan, never consumer accounts • BAA accepted in the admin console before PHI is stored • Only the services the BAA lists are used for PHI • Examples of this category: Google Workspace or Microsoft 365	164.308(b)(1) business associate contracts (R); 164.314(a)		About $7, $14 or $22 per user per month across the three common small-business tiers (both suites, list price, annual plan)	The lowest tier that includes the BAA and the admin controls you will use	Paying for the top tier for features nobody uses	30 days
P1-04	Secure infrastructure	**Patient communication on practice accounts only**	Required	Keeps email and messages with patients inside practice-owned, BAA-covered accounts.	• No personal email, texting or messaging apps for patient communication • Shared group inbox for front desk and scheduling • Messages stay with the practice when staff leave	164.308(b)(1) (R); 164.312(a)(1) access control (standard)		$0 beyond P1-03	Shared group address in the productivity suite	A separate messaging app per clinician	30 days
P1-05	Secure infrastructure	**Password manager for shared and admin logins**	Best practice	Stores the logins that cannot be individual (payer portals, vendor admin accounts) in one place with access by role.	• Every shared login is listed, stored and owned • Access granted by role and removed at offboarding • Passwords rotated when someone with access leaves	164.308(a)(5)(ii)(D) password management (A); CPG Essential: unique credentials		About $2–8 per user per month; some business plans are priced flat for a small team	Business vault for shared and admin logins only; browser password manager for staff	An enterprise vault for every staff member before shared logins are inventoried	90 days
P1-06	Secure infrastructure	**Managed devices with encryption and remote wipe**	Best practice	Lets the practice enforce screen locks and encryption, and wipe a lost or departing device.	• Every device that opens PHI is enrolled and encrypted • Screen lock and automatic logoff set centrally • Remote wipe tested once • Devices wiped before disposal or reuse	164.312(a)(2)(iv) encryption (A); 164.312(a)(2)(iii) automatic logoff (A); 164.310(d)(2)(i)–(ii) disposal and media re-use (R); CPG Essential: strong encryption	NPRM would make encryption of ePHI at rest and in transit required, with limited exceptions	About $50 per device per year for browser-based laptops; device management is included in the top small-business tier of either suite	Refurbished business laptops on a managed, browser-based operating system, about $250–300 each	Full endpoint security suites on laptops that only run a browser	180 days
P1-07	Secure infrastructure	**Supported operating systems and automatic updates**	Best practice	Keeps every device on an operating system that still receives security updates, installed automatically.	• No device on an unsupported operating system • Automatic updates on, with a set restart window • Built-in malware protection on	164.308(a)(5)(ii)(B) protection from malicious software (A); CPG Essential: mitigate known vulnerabilities	NPRM would require patching on set timelines	$0 to about $300 per device (convert or replace)	Convert older hardware to a supported, browser-based operating system	Replacing every device at once	90 days
P1-08	Secure infrastructure	**Backup of practice files outside any single device**	Required	Keeps a retrievable copy of practice data that survives a lost device, deletion or ransomware.	• No practice data lives only on one computer or drive • Version history on, and a restore tested once a year • A written plan for restoring critical systems	164.308(a)(7)(ii)(A) data backup plan (R); 164.308(a)(7)(ii)(B) disaster recovery plan (R)	NPRM would require restoring critical systems and data within 72 hours	Usually included in suite storage; separate cloud-to-cloud backup about $2–4 per user per month	Suite cloud storage with version history	A local storage drive as the only copy	90 days
P1-09	Secure infrastructure	**Offboarding procedure, same day as HR**	Required	Removes every system access the day someone leaves, using one checklist.	• One checklist used for every departure (Tab 3) • Main account suspended first; apps that require suite sign-in lock out • Apps with their own passwords removed one by one; shared logins rotated; devices collected and wiped	164.308(a)(3)(ii)(C) termination procedures (A); CPG Essential: revoke credentials for departing workforce members	NPRM would require access removed no later than one hour after employment ends	$0	The checklist on Tab 3	Offboarding handled only by HR or a PEO	90 days

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
P1-10	Secure infrastructure	**Security awareness training on a schedule**	**Required**	Trains every workforce member on phishing, passwords and reporting, at hire and on a schedule.	• Training at hire and at least yearly, with sign-off • Periodic security reminders between trainings • A named person reviews results	164.308(a)(5)(i) security awareness and training (standard); 164.308(a)(5)(ii)(A) security reminders (A); CPG Essential: basic cybersecurity training	NPRM would require training at least every 12 months	$0 with free federal material; about $1–4 per user per month for a paid platform with phishing simulation	Free HHS and 405(d) material plus a yearly sign-off	A paid platform with no one assigned to review results	180 days
P1-11	Secure infrastructure	**Risk analysis, dated, at least yearly**	**Required**	Documents where PHI lives, the risks to it, and what the practice is doing about each risk.	• Written, dated and signed by the owner • Repeated yearly and after major changes • Each risk has an owner and a planned fix	164.308(a)(1)(ii)(A) risk analysis (R); 164.308(a)(1)(ii)(B) risk management (R)	NPRM would add specific written content and tie the analysis to an asset inventory and network map	$0 (HHS Security Risk Assessment Tool)	HHS Security Risk Assessment Tool, desktop app or spreadsheet version	Paying for an assessment you never act on	90 days
P1-12	Secure infrastructure	**Recognized security practices documented for 12 months**	**Best practice**	Keeps evidence that the practice followed recognized security practices, which HHS must consider in enforcement.	• SRA report, training records and a yearly CPG self-check kept in one folder • Evidence covers the prior 12 months	HITECH Act section 13412, added by Pub. L. 116-321 (2021)		$0	One shared folder holding the SRA report and a yearly CPG self-check		Later
P1-13	Secure infrastructure	**Network: separate guest and practice Wi-Fi, business router**	**Best practice**	Keeps patient and guest devices off the network that practice devices use.	• Guest Wi-Fi separate from practice Wi-Fi • Business-grade router with current firmware and a changed admin password • Someone named can log in to the router	CPG Enhanced: network segmentation	NPRM would require network segmentation	About $150–700 one-time for a business-grade router, or about $20–30 per month as an internet-provider managed Wi-Fi add-on	A guest network on equipment you already own	Enterprise gear the practice cannot administer	180 days
P1-14	Secure infrastructure	**Cyber liability coverage, limits reviewed**	**Optional**	Transfers part of the cost of a breach, ransomware event or vendor outage to an insurer.	• The four questions on Tab 5 answered in writing • Required security controls on the application are actually in place • Limits reviewed at each renewal	Not a HIPAA requirement		Quote-based and varies widely. Small businesses often see about $1,000–4,500 per year for a $1M limit; medical practices often pay more	A cyber rider on an existing business policy, after reading the sublimits	Buying coverage without reading the regulatory and breach-response limits	180 days
P1-15	Secure infrastructure	**Single sign-on through the productivity suite**	**Best practice**	Lets staff sign in to the EMR and other apps with their practice Google or Microsoft account instead of a separate password.	• On in every app that supports it, starting with the EMR • Password login turned off where the app allows it, so suspending one account locks the person out • Apps that cannot use it are marked on Tab 4 and removed by hand at offboarding	Supports 164.312(d) person or entity authentication (R) and 164.308(a)(3)(ii)(C) termination procedures (A); CPG Essential: multifactor authentication; revoke credentials for departing workforce members	NPRM would require MFA and access removal within one hour; single sign-on carries both to every connected app	Often included; some vendors offer it only on a higher tier	Use the sign-in option the app already includes, and ask about it before you sign a contract	Upgrading to a premium tier only to get single sign-on, when it could have been negotiated at signing	90 days

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
P2-01	Clinical systems	**List of every system that touches PHI, with an owner**	Best practice	Shows every place patient data lives or passes through, and who is responsible for it.	• Every system on one list (Tab 4) • Each has an owner, a BAA status and an export route • Reviewed at least yearly with the risk analysis	Supports 164.308(a)(1)(ii)(A) risk analysis (R)	NPRM would require a written technology asset inventory and network map	$0	Tab 4 of this tool		30 days
P2-02	Clinical systems	**BAA for every system on that list**	Required	Puts a business associate agreement in place with every vendor that creates, receives, keeps or sends PHI for the practice.	• A signed or accepted BAA on file for each system that holds PHI • Add-ons and integrations checked separately • BAAs stored where the owner can find them	164.308(b)(1) business associate contracts (R); 164.314(a); CPG Essential: vendor cybersecurity requirements	NPRM would require written verification of business associates' safeguards at least yearly	$0	Request the vendor's standard BAA	Third-party add-ons assumed to be covered by the main vendor's BAA	90 days
P2-03	Clinical systems	**EMR with individual logins and role-based access**	Required	Gives each user their own EMR login with access limited to what their role needs.	• No shared EMR logins • Staff sign in with their practice Google or Microsoft account if the EMR supports it • Roles set for clinicians, front desk and billing; access changed when roles change	164.312(a)(1) access control (standard); 164.312(a)(2)(i) (R); 164.308(a)(4) information access management (standard)		Part of the EMR subscription; selection is covered in session #306, The EMR Dozen			30 days
P2-04	Clinical systems	**EMR audit log you can pull**	Required	Records who viewed or changed each record, so the practice can review activity and investigate.	• The owner knows how to run the audit report • Activity reviewed on a schedule • Log retained by the vendor for a stated period	164.312(b) audit controls (R); 164.308(a)(1)(ii)(D) information system activity review (R)		Usually included	Ask the vendor to show you how to run it before you need it		90 days
P2-05	Clinical systems	**Data export you control**	Best practice	Lets the practice take a full copy of its records in a documented format.	• Export terms in the contract: scope, format, timeline and fee • A sample export reviewed before signing	Contract term; not a HIPAA Security Rule requirement		Ask at signing; export fees vary by contract	Ask for a sample export and the export fee in writing	Export available only at termination, for a fee	90 days
P2-06	Clinical systems	**Fax into the chart**	Optional	Receives and sends faxes electronically so documents can be filed to the chart without paper.	• Covered by a BAA • Incoming faxes routed to a monitored queue, not one person's inbox	164.308(b)(1) (R) if the service handles PHI		About $10–50 per month at small-practice volumes; a BAA is often limited to higher tiers	Use the EMR's fax module if it has one; otherwise choose a plan by page volume	A separate fax service that files to personal email	Later
P2-07	Clinical systems	**Home exercise and remote monitoring integrated with the EMR**	Optional	Delivers home programs and collects patient-reported data between visits.	• One patient login, not two • Data flows into the chart • Covered by a BAA	164.308(b)(1) (R) if the service handles PHI		Varies; often included in or added to the EMR, otherwise quote-based	Use the EMR's own module before adding a separate app	A second patient app with its own login and its own BAA	Later
P2-08	Clinical systems	**Premium tiers and AI add-ons**	Optional	Adds features beyond the core EMR, including AI documentation tools.	• Each add-on scored with the Human Filter Worksheet • Covered by the BAA • A measure that decides whether to keep it	164.308(b)(1) (R) if the add-on handles PHI		Varies by vendor and tier	Run each through the Human Filter Worksheet	A tier that duplicates a tool you already pay for	Later

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
P3-01	Patient engagement	**Practice-owned phone and texting under a BAA**	Best practice	Puts calls and texts with patients on practice numbers, not clinicians' personal phones.	• Practice numbers on a cloud phone system covered by a BAA • Texting from the practice number, logged • Numbers stay with the practice when staff leave	164.308(b)(1) (R) if PHI is handled		About $20–40 per user per month	A cloud phone system with a BAA and shared lines instead of a line per clinician	Clinicians texting patients from personal phones	90 days
P3-02	Patient engagement	**Appointment reminders**	Best practice	Reminds patients of visits by text, email or call to reduce no-shows.	• Sent from the one system that owns the schedule • Patients can confirm or cancel from the reminder	164.308(b)(1) (R) if a separate service handles PHI		Often included in the EMR; confirm before buying separately	Use the reminders built into the system that owns the schedule	Reminders sent from two systems	90 days
P3-03	Patient engagement	**Online self-scheduling and intake**	Optional	Lets patients book and complete intake before the first visit.	• Intake writes into the EMR without retyping • Booking rules prevent visits the practice cannot serve • Covered by a BAA	164.308(b)(1) (R) if the service handles PHI		Often included in the EMR; standalone intake or form services with a BAA about $30–130 per month	Intake that writes into the EMR	Booking that skips data capture and creates callbacks	Later
P3-04	Patient engagement	**AI voice agent for new-patient calls**	Optional	Answers or returns new-patient calls and books visits automatically.	• Piloted on one line with a measure (calls answered, visits booked, callbacks) • Collects what intake needs, not only a booking • Covered by a BAA	164.308(b)(1) (R) if the service handles PHI		Quote-based; pricing models vary	A time-limited pilot on one line before any long contract	An agent that books but leaves intake to the front desk	Later
P3-05	Patient engagement	**Check-in kiosk**	Optional	Lets patients check in and update forms on a device in the lobby.	• A named owner who maintains it • Locked to the check-in form • Hosting service covered by a BAA	164.308(b)(1) (R) for the hosting service if PHI; 164.310(c) workstation security (standard)		A tablet, about $150–400 one-time, plus the form service (see P3-03)	A tablet running a simple check-in form	A kiosk the practice must maintain with no named owner	Later
P3-06	Patient engagement	**Website hosted off-site, not on a local server**	Best practice	Runs the public website on a hosted service that patches itself, away from practice systems.	• Hosted, with security updates applied by the host • No PHI collected through ordinary web forms • Patient forms only through a BAA-covered service	CPG Essential: mitigate known vulnerabilities		About $15–40 per month for a hosted site builder; forms that collect PHI add about $30–130 per month with a BAA	A hosted site builder	Patient forms on the public website without a BAA	180 days

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
P4-01	Business intelligence	**A short list of weekly numbers, each with an owner and the decision it drives**	**Best practice**	Turns reports into decisions by tying each number to a person and an action.	• Five to eight numbers, reviewed weekly • Each has an owner and the decision it informs • Numbers nobody acts on are dropped	Not a HIPAA requirement		$0	A spreadsheet fed by standard EMR reports	Numbers nobody acts on	90 days
P4-02	Business intelligence	**Standard EMR reports**	**Best practice**	Uses the reports the EMR already includes before buying analytics.	• The owner can run each weekly report without help • Report definitions written down so numbers mean the same thing each week	Not a HIPAA requirement		Usually included	Learn the reports you already have		90 days
P4-03	Business intelligence	**Dashboard or analytics tier**	**Optional**	Combines data from several systems into one view.	• Answers a decision the spreadsheet cannot • Each metric has an owner • Covered by a BAA if it holds PHI	164.308(b)(1) (R) if the service handles PHI		Varies; quote-based	Keep the spreadsheet until it cannot answer a decision you face	A dashboard admired and never acted on	Later

ID	Pillar	Category	Tier	What it does	What good looks like	Regulatory basis or CPG goal	Proposed change (NPRM, not final)	Typical cost (Nov 2026)	On a budget	Bloat warning	Suggested horizon
AI-01	Across all pillars: AI	**Written AI use policy**	**Best practice**	Tells staff which AI tool is approved, what data can go into it, and who is responsible for the output.	• Names the approved tool and account type • States the PHI rule and the clinician's responsibility • Signed by staff at hire and yearly	Supports 164.308(a)(5)(i) training (standard) and 164.308(b)(1) (R)		$0	Tool 3, Sample AI Use Policy	A policy that names no approved tool	180 days
AI-02	Across all pillars: AI	**One approved AI tool, on a practice account under a BAA**	**Optional**	Gives staff a sanctioned AI tool so they do not use personal accounts for practice work.	• Signed in with a practice account, never a personal one • The specific AI feature is listed as covered by the BAA • Scored with the Human Filter Worksheet	164.308(b)(1) (R) if PHI is entered		AI is included at a base level in both suites' business plans; premium AI add-ons about $20–30 per user per month	The AI built into a productivity suite you already have under a BAA	Several AI tools, each with its own data terms	Later

Pillar 2 note

What a small practice needs from an EMR: a signed BAA; individual logins with role-based access; an audit log you can pull; a data export you control; integrations for billing, home exercise and fax. Selection, contracts and trade-offs: session #306, The EMR Dozen.

Pillar 4 example

Example weekly numbers (number / owner / decision it drives): Visits per therapist / Clinical director / Schedule templates and hiring. Arrival rate / Front desk lead / Reminder and outreach changes. New-patient lead to scheduled / Front desk / Callback priority. Unscheduled leads / Front desk / Same-day follow-up. A/R days / Billing / Payer follow-up.