JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · HEALTHCARE

HIPAA IT Setup Guide for Medical and Dental Practices

How to set up the computers, network, email, backups and vendors in a small medical or dental office so patient data stays safe and the practice keeps running. Each step says plainly whether HIPAA **requires** it today, HHS **recommends** it, or it is only **proposed**.

By Umair Akhtar, Founder & President, JPert INC

Published November 1, 2026
Last reviewed November 1, 2026

About a 15-minute read

JPert INC
1934 Old Gallows Road, Suite 360, Vienna, VA 22182
703-576-8200 · jpert.com

Free to share. The latest version is always at https://jpert.com/white-papers/medical-dental-practice-it-setup

Scan for the latest version

The short version

- The HIPAA Security Rule in force today **requires a written risk analysis**. It is the item federal regulators cite most often when they penalize practices.
- The big HIPAA update you may have heard about is **still only a proposal**. It was published January 6, 2025, and the federal agenda now projects a final rule around July 2027.
- You do not need to wait for it. Multi-factor sign-in, encryption, an up-to-date device list, a separate network for medical devices, and tested offline backups are already what HHS recommends for small practices.
- Every IT company or cloud service that can touch patient data needs a signed **Business Associate Agreement** before it does.

Who this is for and how to read it

This white paper is for owners, practice administrators and office managers of medical and dental practices with roughly 5 to 100 staff and no full-time IT department. It is written so a non-technical reader can follow it and hand it to whoever manages their technology.

Every recommendation is labeled so you know how firm it is:

- REQUIRED The HIPAA Security Rule requires it today (45 CFR Part 164, Subpart C).
- RECOMMENDED Official HHS or NIST guidance recommends it for small practices, or it is how HIPAA's flexible requirements are normally met.
- PROPOSED It appears in the January 2025 proposed rule and is not yet law.

We link every point to the official source at the end. This is general guidance, not legal advice. Talk to your attorney about your specific situation.

The rules that apply today

The HIPAA Security Rule

The Security Rule protects *electronic* patient information (ePHI). It is organized into three groups of safeguards: administrative (policies, training, risk analysis), physical (the building, workstations and devices) and technical (sign-in, audit logs, encryption). Its current text dates from 2003, with the last changes in 2013.

Some items are "required" and others are "addressable." **Addressable does not mean optional.** For an addressable item, such as encryption, a practice must either put it in place or write down why it is not reasonable and what equivalent step it took instead. For laptops, email and backups, it is very hard to argue that encryption is unreasonable.

The proposed update (not final)

On January 6, 2025, HHS published a proposed overhaul of the Security Rule. It would, among other things, make almost every item required, require encryption and multi-factor authentication, require a written technology inventory and network map, require the ability to restore key systems within 72 hours, and require yearly compliance audits, vulnerability scans every six months and a yearly penetration test.

As of November 2026, **none of that is final**. The federal regulatory agenda lists the rule as a long-term action with a projected final rule around July 2027, and HHS says the current rule stays in effect until then. If it is finalized as proposed, practices would get about 240 days (60 days to take effect plus 180 days to comply). The final version may also differ from the proposal.

Our advice: do not treat the proposal as a deadline, and do not ignore it either. Most of what it proposes is already in HHS's free guidance for small practices and in the fixes regulators ask for in settlements. Building to it now means no scramble later.

The free HHS playbook for small practices

HHS and industry experts publish *Health Industry Cybersecurity Practices* (HICP, 2023 edition) under Section 405(d) of the Cybersecurity Act of 2015. It names the five threats that hit healthcare hardest: phishing and other social engineering, ransomware, loss or theft of equipment or data, insider data loss (accidental or deliberate), and attacks on network-connected medical devices. Its Technical Volume 1 is written for small organizations, which HICP defines as roughly 1 to 10 physicians.

Federal law (Public Law 116-321, passed in 2021) tells HHS to consider whether a practice had "recognized security practices" such as HICP in place for the prior 12 months when it decides penalties. Following HICP is not a free pass, but it counts.

HHS also publishes ten voluntary "Essential" cybersecurity goals for healthcare: fix known vulnerabilities, email security, multi-factor authentication, basic training, strong encryption, removing access when people leave, basic incident planning, unique logins, separate admin accounts, and security requirements for vendors. The steps below cover all ten.

Step 1: Risk analysis and a list of everything you own

REQUIRED HIPAA requires "an accurate and thorough assessment" of the risks to patient data, followed by a plan to reduce those risks (45 CFR 164.308(a)(1)). It must cover all ePHI wherever it lives: your practice management and EHR systems, imaging, email, laptops, phones, backups and cloud services. Update it when something important changes, such as a move, a new system or a security incident.

HHS does not require a particular method. Small and medium practices can use the free HHS Security Risk Assessment Tool (version 3.7), which keeps your answers on your own computer. Using it does not guarantee compliance, but it gives you a structure.

RECOMMENDED Keep a list of every device, program and cloud service, who uses it and whether it touches patient data. Include X-ray sensors, panoramic and CBCT machines, lab equipment, printers, scanners, phones and the Wi-Fi equipment. Record how each device is wiped when it is retired. HICP recommends this for small practices, and the

proposed rule would require a written inventory and network map updated every 12 months PROPOSED .

Step 2: Accounts, passwords and multi-factor sign-in

- REQUIRED **Everyone gets their own login.** No shared front-desk or "doctor" accounts. Unique user IDs are a required item (164.312(a)(2)(i)), and they are how your audit logs show who looked at what.
- REQUIRED **An emergency access plan.** Write down how staff reach patient records if a system or the usual login fails (164.312(a)(2)(ii)).
- RECOMMENDED **Multi-factor sign-in (MFA) on email, remote access and the EHR.** HICP's very first small-practice email item says to turn on MFA before allowing email access, and it also calls for MFA on remote access and VPNs. MFA is one of HHS's Essential goals and would become required under the proposal PROPOSED . Prefer an authenticator app or security key over text messages.
- RECOMMENDED **Long passwords, not complicated ones.** Current NIST guidance (SP 800-63B, Revision 4) says passwords used alone should be at least 15 characters, should be checked against lists of leaked passwords, and should not be forced to change on a schedule unless there is a sign they were stolen. Give staff a password manager.
- RECOMMENDED **Admin accounts are separate.** Day-to-day work happens on a standard account. Only a few people hold administrator rights, on a separate login. This is another HHS Essential goal.
- RECOMMENDED **Access matches the job and ends on the last day.** Front-desk staff do not need billing exports; a hygienist does not need payroll. When someone leaves, turn off their accounts, remote access and door codes the same day. HIPAA lists termination procedures as an addressable item, and HHS lists it as an Essential goal.
- RECOMMENDED **Screens lock automatically.** Automatic logoff is an addressable HIPAA item. Set exam-room and front-desk computers to lock after a few minutes, and use quick badge or PIN unlock so staff do not disable it.

Step 3: Email

Phishing is the first of HICP's five threats, and email is where most break-ins start.

- RECOMMENDED Turn on the spam, malware and impersonation filtering your email service includes, and tag messages that come from outside the practice.
- RECOMMENDED Use encrypted email for any message to someone outside the practice that contains patient information.
- RECOMMENDED Publish SPF, DKIM and DMARC records for your domain so criminals cannot easily send email that looks like it came from you.
- RECOMMENDED Run phishing practice tests. HICP suggests simulations as often as monthly for small practices. Thank people who report suspicious email; never shame someone who clicked.
- RECOMMENDED Confirm any request to change bank details, pay an invoice or buy gift cards by calling a number you already have.

Your email provider must sign a Business Associate Agreement if email contains patient information (see Step 7).

Step 4: Computers, phones and updates

- RECOMMENDED **Encrypt every laptop, desktop and phone that can hold patient data.** Encryption is addressable today and would be required under the proposal PROPOSED . It also protects you after a theft: under the HIPAA Breach Notification Rule, properly encrypted data is "secured," so losing an encrypted laptop is generally not a reportable breach. Virginia's breach law has a similar exception for encrypted data.
- RECOMMENDED **Patch at least monthly.** HICP recommends patching at least monthly if updates are not automatic. Fixing known vulnerabilities is the first HHS Essential goal.
- RECOMMENDED **Replace unsupported systems.** HICP says to replace operating systems that no longer get security updates. Windows 10 support ended October 14,

2025. If a machine cannot upgrade yet (for example, one that runs an older imaging program), Microsoft sells Extended Security Updates for a limited time, and that machine should be isolated on the network until it is replaced.

- RECOMMENDED **Endpoint protection that someone actually watches.** HICP calls for antivirus and endpoint protection on every computer. Alerts that nobody reviews do not stop an attack.
- REQUIRED **Wipe or destroy drives before disposal or reuse.** Disposal and media re-use are required physical safeguards (164.310(d)). Keep a record of what was wiped and when.

Step 5: Network, Wi-Fi and medical devices

A flat network, where the guest Wi-Fi, the X-ray sensor and the billing computer all sit together, lets one infected device reach everything. HICP's small-practice network guidance is to separate them.

- RECOMMENDED **Separate networks** (often called segments or VLANs) for: staff computers and servers; medical and imaging devices; phones, cameras, TVs and other smart devices; and guest Wi-Fi. Network segmentation is an HHS Enhanced goal and would be required under the proposal PROPOSED .
- RECOMMENDED **Guest Wi-Fi never touches the practice network.** Patients and vendors get their own network with internet access only.
- RECOMMENDED **Use WPA3 Wi-Fi security** where your equipment supports it, with a strong passphrase that changes when staff leave. The Wi-Fi Alliance requires WPA3 on all newly certified devices.
- RECOMMENDED **A business firewall with intrusion prevention**, kept updated, and replaced when the manufacturer stops supporting it.
- RECOMMENDED **No remote desktop open to the internet.** HICP and CISA both say to turn off direct inbound remote desktop access and use a VPN or secure remote-access service with MFA instead. Exposed remote desktop is a common way ransomware gets in.

- RECOMMENDED **Lock the network closet** and disable unused network jacks in waiting rooms and empty offices. Facility access controls are an addressable HIPAA item.

Medical and dental equipment makers are responsible for device security under FDA rules, but the practice is responsible for how those devices sit on its network. Keep them on their own segment, change default passwords, and ask the vendor how they deliver security updates and remote support.

Step 6: Backups and getting back up and running

REQUIRED HIPAA requires a data backup plan, a disaster recovery plan and an emergency mode operation plan (164.308(a)(7)). That means you can get exact copies of patient data back, you know how you will restore systems, and you know how the practice keeps seeing patients while systems are down.

- RECOMMENDED **Keep at least one copy offline or locked** so ransomware cannot change or delete it. HHS's ransomware guidance says to back up frequently and consider offline backups, and CISA's ransomware guide says the same.
- RECOMMENDED **Encrypt backups**, including cloud backups, as HICP recommends.
- RECOMMENDED **Test a restore** on a schedule and write down how long it took. Testing is an addressable HIPAA item, and an untested backup is a guess.
- RECOMMENDED **Rank your systems.** Decide what comes back first: usually the practice management or EHR system, then imaging, then email. HIPAA lists this "criticality analysis" as addressable.
- PROPOSED The proposal would require written procedures to restore critical systems and data within 72 hours. That is a sensible target to plan for now.

Cloud-based practice software does not remove the need for a backup plan. Check what your vendor backs up, how long it keeps it, and how you would get your data back if you left or the vendor had an outage.

Step 7: Vendors and Business Associate Agreements

REQUIRED Any outside company that creates, receives, stores or transmits patient data for you is a business associate and must sign a Business Associate Agreement (BAA) first (164.308(b), 164.314). That includes your IT company, cloud EHR or practice management vendor, email and file storage provider, backup service, and any software vendor with remote access.

HHS's cloud guidance is clear on two points practices often miss:

- A cloud provider that stores patient data is a business associate **even if the data is encrypted and the provider does not have the key**.
- Using a cloud service for patient data without a BAA is itself a HIPAA violation.

RECOMMENDED Keep a list of every vendor with access, what they can reach and when their BAA was signed. Ask each one how they protect your data, how fast they will tell you about an incident, and how you get your data back when the contract ends. Vendor security requirements are an HHS Essential goal. The proposal would add a yearly written check of each business associate's safeguards PROPOSED .

Step 8: When something goes wrong

REQUIRED HIPAA requires procedures to identify, respond to and document security incidents (164.308(a)(6)).

- RECOMMENDED **Write a one-page incident plan**: who to call (your IT provider, your cyber insurer, your attorney), how to disconnect an infected computer, and how to reach staff if email is down. Walk through it once a year with a short tabletop exercise, as HICP suggests.
- **Know the breach clock.** Under the HIPAA Breach Notification Rule, patients must be told without unreasonable delay and no later than 60 days after a breach is discovered. If 500 or more people are affected, you must also notify HHS within 60 days, and if more than 500 residents of a state are affected, the media as well. Smaller breaches go in a yearly report to HHS.

- **Ransomware is presumed to be a breach.** HHS's ransomware guidance says that when ransomware encrypts patient data, the data is considered "acquired," and a breach is presumed unless a documented assessment shows a low probability that it was compromised.
- **Virginia.** HIPAA-covered practices are exempt from Virginia's medical-information breach law (Va. Code 32.1-127.1:05), but Virginia's general breach law (Va. Code 18.2-186.6) can also apply when Social Security, driver's license or financial account numbers are exposed. Ask your attorney how both apply to you.
- **Report crimes.** Report cyber attacks and fraud to the FBI at ic3.gov.

Step 9: People, policies and the front desk

- REQUIRED **Name a security official** responsible for the program (164.308(a)(2)). In a small practice this is often the practice administrator, supported by your IT provider.
- REQUIRED **A sanction policy** for staff who break security rules, and **regular review of system activity** such as login and access logs (164.308(a)(1)).
- RECOMMENDED **Security training for everyone**, at hire and at least yearly, with attendance records. HIPAA lists a security awareness program as a standard, and HICP calls for annual training with records.
- RECOMMENDED **Short written policies** covering acceptable use, personal phones used for work, and how patient data is classified and shared. HICP lists these for small practices.
- RECOMMENDED **Workstations that face away from patients**, privacy screens at the front desk, and locked storage for paper and removable media. Workstation use and security are HIPAA standards.
- REQUIRED **Keep your documentation for six years**: policies, the risk analysis, training records and incident records (164.316).

One-page setup checklist

Area	What to have in place	Status today
Risk analysis	Written, covers all ePHI, updated after major changes, with a risk management plan	REQUIRED
Inventory	Every device, program and cloud service, including imaging and phones	RECOMMENDED PROPOSED
Logins	One login per person, emergency access plan	REQUIRED
MFA	On email, remote access, EHR and admin accounts	RECOMMENDED PROPOSED
Admin rights	Separate admin logins for a few people only	RECOMMENDED
Email	Filtering, external tags, encrypted sending, SPF/DKIM/DMARC	RECOMMENDED
Encryption	All laptops, desktops, phones and backups	Addressable today, PROPOSED as required
Updates	At least monthly; unsupported systems replaced or isolated	RECOMMENDED
Network	Separate segments for staff, medical devices, smart devices and guests; no exposed remote desktop	RECOMMENDED PROPOSED
Backups	Backup, disaster recovery and emergency mode plans; one offline or locked copy; tested restores	REQUIRED plans, RECOMMENDED method
Vendors	Signed BAA before any vendor touches patient data	REQUIRED

Area	What to have in place	Status today
Incidents	Written response procedures and a breach notification process	REQUIRED
People	Security official, training with records, sanction policy, log review	REQUIRED
Disposal	Drives wiped or destroyed before reuse or disposal, with records	REQUIRED

What enforcement looks like for small practices

The HHS Office for Civil Rights (OCR) runs a Risk Analysis Initiative focused on practices that never did a proper risk analysis. A few public examples from HHS:

- In April 2025, a small New York neurology practice, Comprehensive Neurology, agreed to pay $25,000 and accept two years of monitoring after a ransomware attack affected about 6,800 people. OCR found it had not done an accurate and thorough risk analysis.
- In April 2026, OCR announced four ransomware settlements totaling $1,165,000, including a women's health group ($320,000) and an imaging provider ($375,000).
- In October 2026, OCR announced that Shen Smiles, a Pennsylvania dental practice, agreed to pay $140,000; the case began with a patient's records request and found missing privacy policies, training and safeguards.

The fines for small practices are often modest. The bigger cost is the years of monitored corrective action that come with them, on top of the downtime and patient trust lost in the attack itself. In its settlements, OCR repeatedly asks practices to map where patient data flows, keep the risk analysis current, review system activity, use strong authentication, encrypt patient data and train staff. Those are the steps in this white paper.

How JPert can help

JPert is a managed IT and cybersecurity company based in Vienna, Virginia, near Tysons. We set up and run IT for medical and dental practices across Northern Virginia, and we sign a Business Associate Agreement with every healthcare client. If you want a second opinion on where your practice stands, start with our free 5-minute HIPAA assessment, read about IT for healthcare practices, or book a free IT assessment.

Related reading from our Chronicles: HIPAA risk assessment guide, medical office network security, Business Associate Agreements explained and MFA for medical practices.

Sources

Every recommendation above comes from these official sources, checked on November 1, 2026:

- HIPAA Security Rule, 45 CFR Part 164, Subpart C (eCFR)
- HHS OCR: Guidance on Risk Analysis
- Federal Register: HIPAA Security Rule proposed rule, 90 FR 898 (January 6, 2025)
- HHS: Fact sheet on the proposed Security Rule changes
- Unified Agenda entry for the proposed rule (RIN 0945-AA22)
- HHS 405(d): Health Industry Cybersecurity Practices (HICP), 2023 edition
- HICP Technical Volume 1: Small health care organizations
- HHS: Healthcare and Public Health Cybersecurity Performance Goals
- NIST SP 800-66 Rev. 2: Implementing the HIPAA Security Rule (February 2024)
- NIST SP 800-63B Rev. 4: Authentication and passwords
- HealthIT.gov: Security Risk Assessment Tool
- HHS OCR: Ransomware and HIPAA fact sheet
- HHS: Breach Notification Rule
- HHS: Guidance on HIPAA and cloud computing

- CISA: #StopRansomware Guide
- Microsoft: Windows 10 end of support and Extended Security Updates
- Wi-Fi Alliance: Wi-Fi security and WPA3
- Va. Code 32.1-127.1:05 (medical information breach notification)
- Va. Code 18.2-186.6 (personal information breach notification)
- HHS press releases: Comprehensive Neurology (April 2025), four ransomware settlements (April 2026), Shen Smiles (October 2026)

This white paper is general information about IT and security practices, not legal advice. Regulations change; we review this paper when HHS publishes a final Security Rule or new guidance. See our editorial policy and corrections page.

FAQ

Common questions from practice owners

Is the new HIPAA Security Rule final?

No. HHS proposed major changes on January 6, 2025, but as of November 2026 they are still a proposal. The federal regulatory agenda projects a final rule around July 2027. The current Security Rule, including its required risk analysis, remains in effect today.

Does addressable mean optional under HIPAA?

No. For an addressable item such as encryption, a practice must either put it in place or write down why it is not reasonable and what equivalent step it took instead. For laptops, email and backups, encryption is almost always reasonable.

Does our IT company need to sign a Business Associate Agreement?

Yes, if it can access, store or transmit patient data. HHS guidance says IT providers and cloud services that handle ePHI are business associates, even if they only store encrypted data and do not hold the key. Sign the agreement before they touch patient data.

Where should a small practice start?

Start with a written risk analysis, which HIPAA requires. Then turn on multi-factor authentication for email and remote access, encrypt every laptop, and set up an offline or locked backup that you test. Those steps close the doors attackers use most.

Want us to check your setup against this guide? Book a free IT assessment with our Vienna, VA team at jpert.com/contact or call 703-576-8200. We will give you a plain-English list of what to fix first.