

HIPAA Compliance Checklist for Virginia Practices

For Doctors' Offices, Dental Practices & Med Spas

SIM Technology Solutions • Healthcare IT & Compliance Guide • Updated September 2026

HIPAA & COMPLIANCE

HIPAA doesn't expect a solo practitioner's office to look like a hospital IT department, but it does hold doctors' offices, dental practices, and med spas to the same core safeguards. This checklist covers the administrative, technical, and physical safeguards examiners and auditors actually look for, plus the data retention and disposal rules practices in Virginia most often get wrong.

How to use this: Work through each section with whoever owns IT and compliance in your practice (that may be you). Unchecked items are your punch list. Nothing here is legal advice. For anything involving your specific facts, especially retention questions for closed charts or multi-state operations, loop in healthcare counsel.

1. Administrative Safeguards

- ☐ A Security Risk Analysis (SRA) has been completed in the last 12 months and is documented, not just talked about
- ☐ A named Privacy Officer and Security Officer are designated (can be the same person in a small practice)
- ☐ Signed Business Associate Agreements (BAAs) are on file for every vendor that touches PHI, including your EHR/practice management vendor, IT provider, billing company, cloud backup, imaging vendor, and answering service
- ☐ Workforce members complete HIPAA security awareness training at onboarding and at least annually, with signed acknowledgment on file
- ☐ A written sanctions policy exists for staff who violate PHI handling policies
- ☐ A documented incident response / breach response plan exists and has been reviewed in the last year
- ☐ Access to PHI is reviewed periodically and revoked promptly when staff leave or change roles

2. Technical Safeguards

- ☐ Every staff member has a unique login, with no shared or generic accounts on EHR, email, or practice systems
- ☐ Multi-factor authentication (MFA) is enforced on email, EHR/practice management software, and any remote access
- ☐ PHI is encrypted at rest (on servers, workstations, laptops) and in transit (email, file transfers)
- ☐ Systems automatically log off or lock after a period of inactivity

- ☐ Endpoint protection is in place on every device, ideally Endpoint Detection & Response (EDR), not just consumer antivirus
- ☐ Audit logs are enabled and actually reviewed periodically for unusual access to patient records
- ☐ Backups run on a regular schedule, are encrypted, and are tested with an actual restore, not just confirmed as "completed" in a log

3. Physical Safeguards

- ☐ Workstations that can access PHI are positioned so screens aren't visible to patients or passersby
- ☐ Server/network equipment is in a locked, access-controlled space
- ☐ Laptops and portable devices with PHI are encrypted and secured when not in use
- ☐ There's a documented process for wiping or destroying devices and media before disposal or resale
- ☐ Visitor and after-hours access to areas containing PHI is controlled and, ideally, logged

4. Data Retention Guidelines

This is the part most practices get wrong, mainly because two different sets of rules apply depending on what you're retaining.

HIPAA's own rule: 6 years for documentation, not charts

HIPAA itself (45 CFR §164.316 and §164.530) requires **administrative and compliance documentation** to be kept for **6 years** from the date created, or from when it was last in effect, whichever is later. This covers your:

- Security Risk Analyses and remediation plans
- Policies and procedures (a policy in effect for 8 years must be kept 14 years total: 8 active plus 6 after retirement)
- Signed Business Associate Agreements
- Staff training records and acknowledgments
- Breach notification documentation and incident reports
- Access/audit logs and PHI disclosure authorizations

Patient charts: governed by Virginia state law, not HIPAA

HIPAA does not set a retention period for the medical record itself; that's state law. For practices in Virginia:

Record type	Minimum retention	Authority
Physician records – adult patient	6 years from the last patient encounter (up to 12 years from creation)	Va. Code §54.1-2910.4
Physician records – minor patient	Until age 18, or 6 years from last encounter, whichever is later	Va. Code §54.1-2910.4

Record type	Minimum retention	Authority
Hospital records – adult patient	5 years following discharge	12VAC5-410-370
Hospital records – minor patient	5 years after the patient turns 18	12VAC5-410-370
Birth and death records	10 years	Va. Code §32.1-274

Dental practices and med spas generally follow the physician standard above unless a specific board regulation says otherwise. Confirm with your licensing board if you're unsure. If you've transferred a record to another provider or given a copy to the patient, you're not required to keep retaining the original beyond your own documentation needs.

Secure disposal

- ☐ Paper records are cross-cut shredded or handled by a bonded document destruction vendor with a certificate of destruction
- ☐ Electronic PHI is wiped using a method that meets NIST media sanitization guidance before a device is resold, recycled, or discarded, not just deleted
- ☐ Destruction of both paper and electronic records is logged: what was destroyed, when, and by whom

5. Breach Notification: Know Your Clock

Who you must notify	Timeline
Affected individuals	Without unreasonable delay, no later than 60 days after discovery
HHS Office for Civil Rights – 500+ affected	At the same time as individual notice (within 60 days)
HHS Office for Civil Rights – under 500 affected	Logged and reported annually, within 60 days of year-end
Media	Required if the breach affects more than 500 residents of a single state or jurisdiction

Not sure where your practice actually stands?

SIM Technology Solutions runs Security Risk Analyses, manages BAAs, and builds the documentation trail healthcare practices need, without you having to become a compliance officer on top of running your practice. **Call 703-594-9226** or email info@simtsolutions.com for a walkthrough of where the gaps are.