NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

HIPAA Tech Basics for Medical and Dental Offices

HIPAA's Security Rule applies to every practice that handles electronic patient records, no matter how small, and there's a real technology side to it beyond the legal paperwork. This guide walks through the IT basics: unique logins, encryption, Business Associate Agreements, and risk assessments.

Why this matters for your practice

Size doesn't exempt you, and the technology side is something you can act on today.

Every practice is covered
Handling electronic patient records means the Security Rule applies, no matter how small you are.

A breach gets expensive fast
Notification requirements, potential fines, and patients who lose trust in the practice.

Most of it is just good IT
Unique logins, encryption, and backups protect the practice anyway, HIPAA or not.

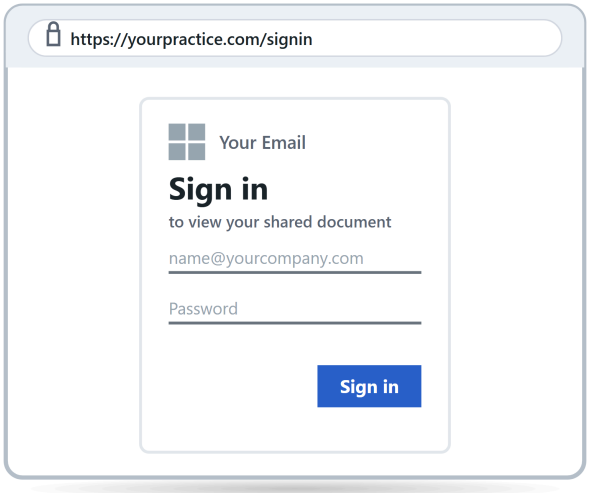
HIPAA tech basics for medical and dental offices

UNIQUE LOGINS

1 Every staff member needs their own login

No shared front-desk logins, no shared practice-management password.

WHAT TO DO
A unique login for every person is what makes an audit trail possible, who looked at which record, and when.



BAA

2 Every vendor who touches patient data needs a signed agreement

Your practice-management host, backup provider, email provider, and your IT company, all of them.

WHAT TO DO

It's called a Business Associate Agreement, and it's as much a vendor-management step as a legal one.



NAPLES COMPUTERS

★ Ready to shore up your HIPAA technical safeguards?

We'll review your logins, encryption, backups, and agreements, and document what's actually in place.

WHAT TO DO

Call 239-513-1960, especially before your next risk assessment.



The technical basics

- [ ] **Automatic screen lock**
  Workstations log off on their own when a staff member walks away
- [ ] **Encryption everywhere PHI lives**
  Laptops, phones, backups, and anything sent by email
- [ ] **Audit logs**
  A record of who accessed which patient file, and when

A few things worth knowing

- [ ] **No official "HIPAA certified" status**
  Be skeptical of any vendor who claims it, HHS doesn't certify products
- [ ] **Risk assessments, at least yearly**
  A documented look at where patient data lives, and what could expose it
- [ ] **Size doesn't exempt a practice**
  A two-provider office has the same technical requirements, just scaled down

Recap: HIPAA tech basics

- [ ] Unique logins for every staff member, never shared
- [ ] Encryption and automatic logoff, everywhere PHI lives
- [ ] Signed Business Associate Agreements with every vendor
- [ ] Risk assessments, at least once a year
- [ ] No official "HIPAA certified" status, be skeptical of vendors who claim it
- [ ] Ready to shore up your safeguards? Call Naples Computers

There's no official "HIPAA certified" credential for a product or vendor; HHS doesn't certify or endorse compliance products. Be skeptical of anyone who claims it, and keep records showing your safeguards are actually enforced, not just documented on paper.

NAPLES COMPUTERS

Running a medical or dental office? We'll help you shore up your technical safeguards.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**