FAQ

Common Security Questions

Straight answers to the HIPAA security questions mental health & behavioral health practices ask us most.

Plain-language answers, real citations
These are the questions we hear most often from solo practitioners and growing group practices. Answers are kept practical, with the underlying regulation noted where it helps. Your situation may differ — when in doubt, ask us.

The Basics

Who's covered · what counts · which rules apply

Q **I'm a solo therapist — does HIPAA really apply to me?** §160.103

A Almost certainly yes. You become a covered entity the moment you transmit health information electronically — submitting claims, checking eligibility, or billing electronically. Practice size doesn't exempt you; a one-person practice carries the same core obligations as a large group.

Q **What actually counts as protected health information (PHI)?** §160.103 · §164.514(b)

A Any individually identifiable health information you create, receive, or store — names, contact details, dates, record or account numbers, and other identifiers tied to a person's care or payment. In behavioral health, even the bare fact that someone is your patient can be PHI.

Q **What's the difference between the Privacy Rule and the Security Rule?** §164 Subparts E & C

A The Privacy Rule governs how you use and disclose PHI in any form — including paper records and spoken conversations. The Security Rule sets safeguards specifically for electronic PHI (ePHI). You must comply with both.

Email, Messaging & Everyday Tools

The apps you already use

Q **Is my regular Gmail or iCloud email HIPAA compliant?**

A No. Consumer email has no business associate agreement and isn't built for PHI. You need a business plan that will sign a BAA — such as Microsoft 365 or Google Workspace — with message encryption enabled.

Q **Is Microsoft 365 or Google Workspace compliant out of the box?**

A Not automatically. They *can* be compliant, but only when you're on a BAA-eligible plan, have actually signed the BAA, and have configured encryption, access controls, and audit logging. The tools enable compliance; they don't guarantee it.

Q **Can I text patients or use WhatsApp / iMessage?** §164.522(b)

A Standard SMS and consumer messaging apps aren't appropriate for PHI — no BAA and limited security. Use a secure messaging tool or patient portal. A patient may request texts after being warned of the risk, which you should document.

Q **Is Zoom okay for telehealth sessions?** §164.502(e)

A Only the healthcare / BAA-covered version configured for HIPAA — not the free consumer tier. Whatever platform you use, confirm a signed BAA covers it and that recordings and chat are handled securely.

Risk, Breaches & Penalties

What's required · what's at stake

Q **Do I really need a Security Risk Analysis every year?** §164.308(a)(1)(ii)(A)

A Yes. A current, documented SRA is the foundation of compliance and the single most commonly cited deficiency in OCR enforcement. Update it at least annually and whenever you make a significant change to systems, vendors, or operations.

Q **Does HIPAA actually require encryption?** §164.312(a)(2)(iv) · (e)(2)(ii)

A Encryption is "addressable," not optional. You must implement it where reasonable, or document why not and use an equivalent safeguard. In practice you should encrypt — properly encrypted PHI is also your breach "safe harbor."

Q **What happens if we have a breach?** §§164.400–414

A Run the four-factor risk assessment, then notify: affected individuals (within 60 days), HHS (500+ individuals within 60 days; smaller breaches reported annually), and prominent media for breaches affecting 500+ in a state. Document every step.

Q **How big are the penalties for non-compliance?**

A Civil penalties are tiered by culpability and adjusted yearly for inflation — ranging from roughly a hundred dollars to tens of thousands per violation, up to an annual cap (now over $2 million) per category. Willful neglect and knowing misuse carry the steepest exposure, including potential criminal penalties.

Records, Vendors & Special Cases

Storage · BAAs · behavioral health specifics

Q **Do I need a BAA with every vendor?** §164.502(e) · §164.308(b)

A With every *business associate* — any vendor that creates, receives, maintains, or transmits PHI for you: EHR, billing, scheduling, email, cloud storage, IT/MSP. Pure "conduits" that only transport sealed information (like the postal service) are the narrow exception.

Q **Is cloud storage allowed for patient records?** §164.502(e)

A Yes — with a signed BAA and proper safeguards such as encryption, access controls, and backups. The cloud provider becomes your business associate and shares responsibility for protecting the data.

Q **What's special about psychotherapy notes?** §164.508(a)(2)

A They're your private process notes, kept separate from the rest of the chart. Most disclosures — even to insurers — require a specific, standalone authorization, giving them stronger protection than ordinary records.

Q **How long do I have to keep HIPAA documentation?** §164.316(b)(2) · §164.530(j)

A HIPAA requires retaining its required documentation — policies, risk analyses, training logs, and the like — for six years. Clinical record retention is set separately by state law, which is often longer, so follow the stricter timeline.

Still Have Questions?

Every practice is a little different. We'll give you clear, specific answers for your setup — no jargon. Reach out for a free consultation.

CALL **631-388-4274**

EMAIL **support@a1plusai.com**

WEBSITE **a1plusai.com**

SERVING **New York & Long Island**