HIPAA: Its Importance and How to Stay Compliant

An Introduction to HIPAA

HIPAA is one of the most important federal laws governing healthcare, yet it is also one of the most commonly misunderstood. Whether you are a licensed clinician, an administrator, or a business owner offering telehealth or wellness services, HIPAA applies to you. Compliance is not optional, it is a legal requirement that protects your patients, your business, and your license. Understanding HIPAA means understanding how to handle patient information safely and ethically.

What Is HIPAA and What Does It Protect?

HIPAA stands for the Health Insurance Portability and Accountability Act, a federal law created to protect patient privacy and secure medical information. HIPAA applies to all “covered entities” (clinics, telehealth providers, pharmacies, insurers, etc.) and “business associates” (contractors, software vendors, billing companies, marketing firms that access health data, etc.).

One of the most important parts of HIPAA is the protection of PHI, Protected Health Information.

What is PHI?

PHI is any piece of information that can identify a patient AND relates to their past, present, or future health or healthcare services.

PHI can exist in any format:

- Written
- Digital
- Verbal
- Photos/scans/video/audio
- Text messages/emails
- EHR/telehealth platforms
- Even casual conversations if patient details are shared

Examples of PHI identifiers include:

(PHI only requires one of these identifiers + any health information)

Direct identifiers:

- Name
- Address
- Email
- Telephone number
- Social security number
- Medical record number
- Insurance information
- Account or invoice numbers
- Biometric identifiers
- Full-face photos or identifiable images
- Device identifiers (serial numbers, MAC addresses, etc.)
- IP addresses or location data tied to a person
- Patient ID numbers
- Voice prints/recordings

Indirect identifiers (PHI when combined with health data):

- Dates (birth, appointment, discharge, death)
- Zip codes
- Employer or workplace
- Unique health conditions

- Medication lists
- Case details that can identify someone in context (“my last patient today who is a 27-year-old marathon runner with Crohn’s...")

PHI Also Includes Information Related To:

- Medical history
- Diagnoses
- Treatment plans
- Symptoms or intake answers
- Clinical notes
- Medication prescriptions
- Insurance claims
- Billing or payment for medical services
- Communications between a patient and healthcare provider

Even if no name is mentioned, if the patient could *reasonably* be identified — it's PHI.

For example:
“I saw an 11-year-old yesterday with Down Syndrome whose mom owns the bakery downtown”
Still PHI, because the patient could be identified.

If you wouldn’t say it to the patient in a crowded room, do not post it, text it, email it, or mention it publicly.

Proper Handling of HIPAA Information and Common Pitfalls

HIPAA compliance is not just about using the right software—it is about behavior, decision-making, and awareness. To stay compliant:

Communication

- Use encrypted platforms for telehealth, messaging, and file sharing
- Do not discuss patient information over text, social media, or personal email
- Never talk about a patient in public areas (hallways, waiting rooms, elevators, etc.)

Workspace and Access

- Keep charts, screens, and devices out of the view of unauthorized individuals
- Do not leave patient files or open EHR screens unattended
- Use unique logins, never share accounts or passwords

Technology

- Use devices with password protection, screen locks, and encryption
- Avoid storing PHI on personal devices whenever possible
- Use only approved storage/submission methods, not Dropbox, iMessage, Google Docs, etc., unless a BAA is in place

Common Pitfalls to Avoid

- Discussing cases where others can overhear
- Printing or downloading patient information and leaving it unsecured
- Using screenshots or photos of patient records
- Talking about patients casually with friends or co-workers

If you’re ever unsure if something is HIPAA-safe, assume it is not and verify before proceeding.

What to do in the Event of a Breach

A breach is any situation where PHI is accessed, shared, or exposed without proper authorization, whether intentional or accidental. If a breach occurs:

1. Stop the breach immediately (disable access, shut down access, secure the system, etc.)
2. Document what happened in detail
3. Notify your compliance officer or supervisor immediately
4. File required legal notifications, some breaches must be reported to the Department of Health & Human Services (HHS)
5. Notify affected patients if necessary under federal breach notification rules
6. Implement corrective action to prevent recurrence (training, policy change, technology adjustment, etc.)

There is no such thing as a harmless breach. HIPAA requires that all breaches be taken seriously and handled appropriately.

Final Reminder: HIPAA is Everyone's Responsibility

HIPAA compliance is not just for physicians or administrators, it applies to every person who interacts with patient information, including support staff, social media managers, and business owners. Protecting PHI is both a legal requirement and a reflection of respect for the people we serve. Maintaining compliance is not just about avoiding penalties—it is about building trust, ensuring safety, and upholding the integrity of healthcare.

By staying informed and proactive, we can provide excellent care while keeping patient information secure.