
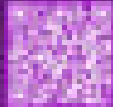


## HIPAA applies to 3 categories of individuals/entities:

HIPAA APPLIES TO 3 CATEGORIES OF INDIVIDUALS/ENTITIES:  
Covered Entity (CE), Business Associate (BA), and members of a CE or BA workforce  
(45 C.F.R. § 160.103)

**1 Are you a HIPAA-Covered Entity?**  
*(Only if you fall into one of these 3 categories)*

- Healthcare providers who bill or receive payment for healthcare in the normal course of business through the electronic transmission of covered transactions (i.e., billing third party payers and fund transfers)
- Healthcare data clearinghouses which process health data
- Health plans which furnish payment for care (e.g., health insurers and self-administered employer-sponsored plans with 50+ participants)

**2 Are you a Business Associate?**  
*(Only if you fall into one of these 3 categories)*

- Persons (other than a member of a CE workforce) or entities that perform services on behalf of a CE involving more than incidental access to (creating/receiving/maintaining/transmitting) Protected Health Information (PHI)
- Subcontractors of a BA whose services involve access to PHI
- Entities offering Personal Health Devices (PHDs) to individuals on behalf of a CE

**3 Are you a Part 2 Program (42 C.F.R. Part 2)?**

Part 2 applies to substance use disorder (SUD) records identifying patients (including presence on a facility, diagnosis, prognosis, or treatment received) maintained by a federally assisted program providing substance abuse education, prevention, training, treatment, rehabilitation, or research.

Part 2 programs are often CEs and are subject to both HIPAA and Part 2.


*Note: "Federally assisted" includes programs receiving federal funds, providers contracted, authorized, licensed, or registered with federal agencies (including CMS and DEA), and any program with IRS tax-exempt status.*

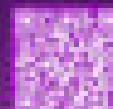
**4 If you are a CE (including a Part 2 Program) or BA, what are your obligations under HIPAA?**  
**45 C.F.R. Part 160 and Part 164 (Privacy Rule, Security Rule, and Breach Notification Rule)**

- Appoint a privacy officer to develop, implement, and maintain organizational privacy policies and procedures
- Appoint a security officer to develop, implement, and maintain policies and procedures to maintain the integrity of electronic Protected Health Information (ePHI)
- Provide annual HIPAA training to new hires and online workforce (employees and independent contractors alike)
- Perform and document annual risk assessments of physical and electronic security measures protecting ePHI (including data on computers, information systems, and mobile devices)
- Implement technical, physical, and administrative safeguards to prevent the misuse of ePHI/PHI and ensure its confidentiality, integrity, and availability
- Develop security incident investigation protocol and breach notification processes
- Respond immediately to potential security incidents and self-report confirmed breaches
- Implement internal privacy, security, and breach response policies and procedures and distribute to workforce for review and written acknowledgement

**Adella Katz**  
attorney  
[akatz@nelsonhardiman.com](mailto:akatz@nelsonhardiman.com)

Contact Us  
**877.248.8423**





## How to Ensure Your Organization is Compliant with Privacy Laws

### Short Term Considerations for Traditional Healthcare Providers (Covered Entities under HIPAA)

As a HIPAA-covered entity, it's absolutely critical to make sure that your marketing practices and use of client data (both PHI and non-PHI) take into account existing federal law (HIPAA, 45 C.F.R. Part 16), the new wave of FTC enforcement, and the rapidly evolving state privacy laws in the states in which your organization targets consumers online.

Make sure your internal and online website privacy policies are actually taking account of your real practices (consistency and transparency is key!).

- Your website privacy policy must actually reflect how you collect, store, share, and sell consumer information - PHI and non-PHI.
- Information related to PHI may, in combination with PHI, be protected by HIPAA (or state privacy laws).

Any providers who believe that HIPAA compliance protects them from compliance with ALL state and federal privacy laws other than HIPAA should disavow themselves of that notion.

- Remember that (b)(3)(ii) providers are subject to comprehensive state privacy laws - each has a different threshold based on number of consumers' information shared or sold, amount of annual revenue, etc.
- However, just because PHI itself is protected by HIPAA and may exempt you from compliance with certain state privacy laws, this does NOT mean that your online marketing practices are exempt from compliance! The marketing itself and tracking technologies used may be subject to state privacy laws and FTC scrutiny.

## IMPORTANT QUESTIONS TO KEEP IN MIND

- Do your marketing team communicate with legal and IT?
- Do you know who is drafting your website privacy policies and terms and conditions? Do you know how often they are updated?
- Do you know what your website's privacy policy says? What is promised to consumers? Are those promises being kept?
- Do you know which tracking tools are being used on your website? (e.g., pixels, cookies, etc.)
- Is your compliance department keeping track of the interactions between consumers and your company's website?
- Do you know (b)(3) information is being collected and (b)(3)?
- Is your marketing periodically audited for privacy compliance?

### Additional Resources from the FTC

- Protecting the privacy of health information - Update's Best Practices from FTC report: <https://www.ftc.gov/press-release/protecting-privacy-health-information-covers-what-advertisers-do-when>
- FTC rules and letter guide to the heart of the new tracking technologies used to harvest health information: <https://www.ftc.gov/press-release/ftc-issues-new-tracking-technologies-used-harvest-health-information>
- Stay safe Security 4 Rules for Business: <https://www.ftc.gov/press-release/stay-safe-security-4-rules-business>

**Adella Katz**

ATTORNEY  
[akatz@nelsonhardiman.com](mailto:akatz@nelsonhardiman.com)

Contact Us:  
877.248.8423

