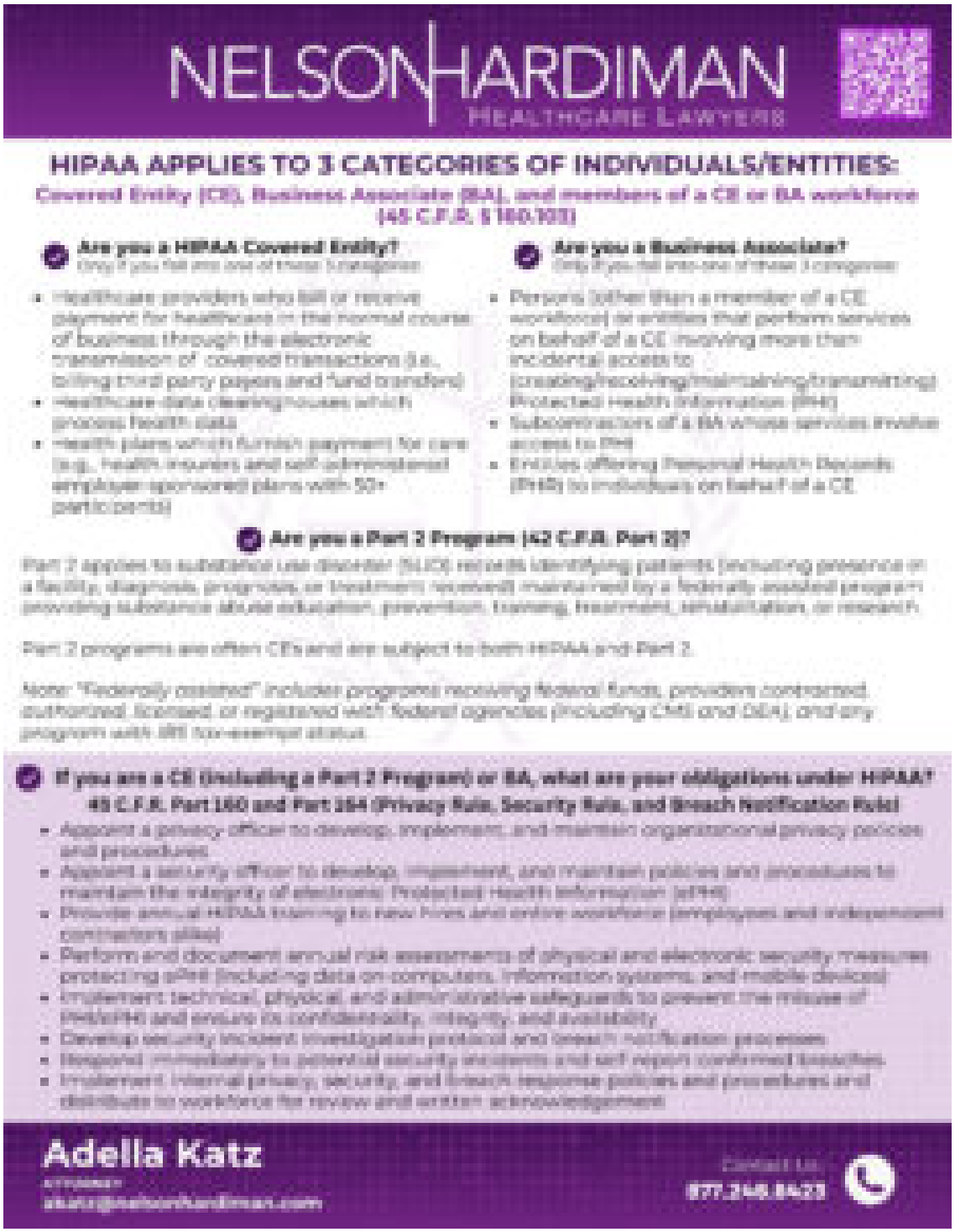
NELSON HARDIMAN
HEALTHCARE LAWYERS

HIPAA applies to 3 categories of individuals/entities:



NELSON HARDIMAN
HEALTHCARE LAWYERS

NELSON HARDIMAN
HEALTHCARE LAWYERS

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, 42 C.F.R. Part 2), 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 disabuse themselves of that notion.**

- Remember that not all 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

? Is your marketing team communicating with legal and IT?

? Do you know which tracking tools are being used on your website? (i.e., pixels, cookies, etc.)

? Do you know who is drafting your website privacy policies and terms and conditions? Do you know how often they are updated?

? Is your compliance department keeping track of the interactions between consumers and your company's website?

? Do you know what your website's privacy policy says? What is promised to consumers? Are those promises being kept?

? Do you know what information is being collected and how?

? Is your marketing periodically audited for privacy compliance?

Additional Resources from the FTC

- **Protecting the privacy of health information: A Baker's Dozen Takeaways from FTC cases** – https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-baker-s-dozen-takeaways-ftc-cases
- **FTC HBNR case letter puts it in the heart of the rules tracking technologies pose to personal health information** – letter makes it clear that developers of health apps and other online services that track user data using technologies like pixels and APIs are likely subject to the HBNR and must notify consumers and others of unauthorized disclosures of personal health information
- **Start with Security: A Guide for Business** – https://www.ftc.gov/business-guidance/resources/start-security-guide-business

Adella Katz
ATTORNEY
ak.atz@nelsonhardiman.com
CONTACT US
877.248.8423