Health Insurance Portability & Accountability Act (HIPAA)

The Gist: HIPAA contains detailed requirements related to the privacy of personal health information and the security of data, such as electronic health records.

Why it Matters: Health care is an area where innovative thinking is needed, and entrepreneurs could create industry-changing offerings. However, the healthcare industry is heavily regulated. There are many HIPAA privacy and security regulations that apply to new products or services in the health space. Fines and penalties for failing to comply with HIPAA can be high, and failure to comply will limit potential growth.

The Need to Know: HIPAA only applies to some businesses. Generally, HIPAA applies to health insurers, health care clearinghouses, medical service providers, and "business associates" of these entities. Being a third-party service provider in the healthcare sector often qualifies a company as a "business associate" that must be HIPAA compliant.

Businesses that fall under HIPAA must protect patient privacy and data security. All HIPAA privacy and security regulations cover "Protected Health Information" (PHI), which is any information held by a covered entity that can be linked to the patient (health status, tests conducted, payments, etc.).

On the privacy front, HIPAA requires covered entities to: secure an individual's consent before disclosing private information in some cases, disclose an individual's medical information to the individual within 30 days if requested by the individual; update any inaccuracies in an individual's medical record; notify individuals of their uses of PHI; appoint a privacy official and contact person for privacy complaints; and disclose PHI to law enforcement as required, such as in suspected child abuse cases.

In terms of security, HIPAA requires covered entities to implement safeguards around the administrative, physical, and technical uses of patient data, specifically for electronic health records. There are set security standards for each, which apply to covered entities. The HITECH Act updated security rules to require covered entities to notify the Department of Health & Human Services (HHS) of any data breaches impacting more than 500 individuals, in addition to notifying all impacted individuals.

For more information on HIPAA, check out the HHS Health privacy page.