Current Healthcare Legal and Regulatory Landscape

eHEALTH INITIATIVE

Health data – including health used for non-health-related purposes – is not regulated by a single national privacy framework. HIPAA is the primary federal law governing the use and disclosure of protected health information, but HIPAA covers an increasingly smaller slice of the health data pie. Other federal laws may apply, both to data regulated by HIPAA and to data outside of HIPAA's framework, and states have their own sets of often-more-restrictive laws. In short, the current legal landscape is a patchwork of laws, sometimes overlapping (and at times conflicting), with numerous gaps in comprehensive protections.

HIPAA

HIPAA's privacy, security and breach notification regulations are the most familiar, and most comprehensive, set of privacy protections in the U.S. for at least some health data. HIPAA governs a wide range of identifiable "protected health information" (PHI), which is broadly defined to include information related to current or past health status, treatment or payment for health care that identifies an individual and is created, held or transmitted by an entity covered by HIPAA. However, in terms of "who" is covered by the law, its scope is narrow: it applies to most health care providers (except those that do not accept health insurance), health plans and health care clearinghouses (referred to collectively as "covered entities"), and their contractors (known as "business associates").

When HIPAA applies, the Privacy Rule includes detailed provisions regarding how PHI, in digital, paper or other form, can be used and disclosed, such as for treatment, payment, public health and research, and specifies when an entity needs to obtain the prior authorization of the data subject. It also establishes rights for individuals, including the right to obtain a copy of PHI and to request amendments to this data. The Security Rule establishes baseline physical, technical and administrative safeguards that apply to electronic PHI, and the Breach Notification Rule requires notification of individuals and regulators in the event of breaches of PHI. HIPAA also defines de-identified data, and sets standards on how to achieve it, but places no limits on its use or disclosure, regardless of who controls the information.

A company that regularly stores and handles health information that is neither a covered entity nor a business associate is not governed by HIPAA. Such entities, often referred to as "non-covered entities," can include social-media platforms, health and wellness apps, smartphones, life insurers, retailers, credit-card companies and Internet search engines.

Other Federal Laws that Provide Privacy and Security Protections for Health Data

• The Common Rule applies to research on human subjects – which includes research done using identifiable personal data – conducted with the support of federal funding from certain agencies, including HHS, the Department of Veterans Affairs and the Department of Energy.

• "Part 2" regulations restrict the use and disclosure of patient records created by federally funded programs related to substance use disorders by prohibiting disclosure of such records without the express written consent of the patient, except in limited circumstances.

• The FDA does not regulate the use and exchange of health data per se, but it does regulate medical devices that often collect them. Further, the agency published guidance several years ago that informs manufacturers about how FDA applies its regulatory authority to certain software applications intended for use on mobile platforms, which would include mobile health technologies.

• The Federal Educational Rights and Privacy Act (FERPA) protects the privacy of student education records; education records, as defined by FERPA, are excluded from HIPAA's definition of PHI.

• The FTC also has broad authority over consumer data by way of provisions in the FTC Act that prohibit "unfair or deceptive acts or practices." This prohibition applies to all entities engaged in commerce, which would include the developers and marketers of mobile health technologies, social media sites and Internet search engines. However, the FTC Act does not contain a set of substantive privacy standards and it is often unclear whether certain uses of data might be deemed unfair or deceptive under the law.

State laws

State laws are often more restrictive than HIPAA, particularly with respect to sensitive health information. Many states have adopted privacy laws governing mental health, HIV and genetic testing data, which often require patient consent for the disclosure of information for purposes permitted under HIPAA, such as treatment, payment or quality improvement. Other state laws, such as California's Confidentiality of Medical Information Act (CMIA), apply to organizations that are not covered entities under HIPAA.

Outside the health care industry, the recently adopted California Consumer Privacy Act (CCPA) has raised the threshold for consumer privacy protection. An increasing number of other states have attempted to provide more comprehensive protections for digital data. For example, Illinois, Texas and Washington now have laws regulating the collection, use and disclosure of biometric information, and other states have proposed similar legislation. As of November 2019, 12 states are in various stages of passing legislation that in some way models itself after the CCPA.

International Law

The General Data Protection Regulation (GDPR), the sweeping European privacy law that went into effect in 2018, affects all individuals and entities that offer goods or services to citizens of the EU, or monitor their behavior there. In general, it requires consent before personal data – including health data – can be processed, although there are exceptions (such as for treatment, public health and some scientific research). The law requires a Data Protection Impact Assessment, and in some cases a regulatory review, for certain high-risk processing activities, such as, for example, health data processed in large numbers. The GDPR also provides strong rights to individuals, in addition to the right of consent, such as the right to erasure (otherwise known as the right to be forgotten) and rights to data portability.

New Federal Privacy Law?

Momentum is building for new federal privacy legislation, motivated by CCPA compliance concerns, potentially conflicting state law obligations, desire for harmonization with international law, and increasing public discomfort with the widespread collection of consumer data. Congressional committees have held hearings on data privacy and a number of privacy bills have been introduced, but as of now, no bills have made significant progress toward being enacted into law.

These privacy bills vary in their language as well as their scope; some are focused on cybersecurity, others on biosecurity, and most are not specific to health data. Of those that are, some focus exclusively on health data held by certain entities outside of HIPAA; other bills apply more broadly to all companies collecting personal data, or to particular actors in the digital data ecosystem, such as data brokers or companies offering services over the Internet or via mobile devices. Most of the bills with a broader focus than health data would exempt entities already covered by HIPAA. Many focus on requiring companies, even those without direct relationships with individuals (such as data brokers), to be more transparent with individuals regarding how their personal data is collected, used and disclosed, and to obtain prior express consent or authorization of data subjects. And a number of bills would vest enforcement of new privacy requirements with the FTC and would provide for steep penalties for violations and/or provide the Commission with greater resources (i.e.: staff and funding) to do its work.

About eHealth Initiative

eHealth Initiative (eHI) convenes executives from every stakeholder group in healthcare to discuss, identify and share best practices to transform the delivery of healthcare using technology and innovation. eHI, and its coalition of members, focus on education, research, and advocacy to promote the use and sharing of data to improve health care. Our vision is to harmonize new technology and care models in a way that improves population health and consumer experiences. eHI has become a go-to resource for the industry through its eHealth Resource Center. For more information, visit ehidc.org.