Type of Content: Q&A

What legislation governs health data privacy?

The U.S. health privacy framework has been built on a foundation of federal laws and regulations, with the additional support of state-level rules and legislation. This section describes the current U.S. health data privacy framework and examines the successes and shortcomings of this framework in addressing key privacy issues.

The Federal Trade Commission (FTC) Act: Passed in 1914, the FTC Act "prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce." Applied in the healthcare context, this means that companies must not mislead consumers about what is happening with their health information.

The Privacy Act of 1974: Establishes a code of fair information practices for the collection, maintenance, use, and dissemination of information about individuals when that information is maintained in a federal system. Most importantly, the Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual.

Family Educational Rights and Privacy Act (FERPA): Passed in 1974, FERPA establishes specific guidelines for protecting the privacy of personal health information in students' educational records, such as vaccinations and nurse visits. Students and families may request access to these records at any time and schools must have written permission to release any of this information. These rights transfer to the student upon their eighteenth birthday.

The Federal Policy for the Protection of Human Subjects or the "Common Rule": The 1979 Belmont Report outlines basic ethical principles that should underpin biomedical and behavioral research for human subjects. This report set the foundation for the later 1991 Common Rule, a federal rule which outlines specific protections for at-risk groups like prisoners, children, and pregnant women.

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA): This 2002 legislation establishes laws to govern confidentiality protections for data collected by U.S. statistical agencies and units. According to the HHS State of Data Sharing Report, the National Center for Health Statistics and the Center for Behavioral Health Statistics and Quality are the two HHS entities covered under CIPSEA. CIPSEA was recently replaced by a newer version of the law under the Foundations for Evidence-Based Policymaking Act of 2018, which aimed to expand access to CIPSEA-related datasets.

The Health Insurance Portability and Accountability Act (HIPAA): Passed in 1996, HIPAA was designed to create a federal floor for the privacy and security of personal health information, which HIPAA defines as data that "includes the individual's past, present, or future mental or physical condition, the provision of healthcare to an individual, and any past, present, or future payment for the provision of healthcare to the individual." HIPAA sets the standards for how entities covered by the law must transmit personal health information, which includes claims, enrollment, eligibility, payment, and coordination of benefits. *For more information on how HIPAA covers patient data, please visit the "HIPAA and Patient Data" page.*

Genetic Information Nondiscrimination Act (GINA): Passed in 2008, GINA aims to prevent discrimination based on a person's genetic information by employers and health insurers. Companies are not allowed to make decisions related to eligibility, premium costs, or coverage based on this information. The law specifically stipulates that *employers, employment agencies, training programs, and labor organizations* may not:

- Discriminate based on genetic information which includes refusing employment based on genetic information, limit, segregate, or classify individuals based on their genetic information.
- Request, purchase, or acquire genetic information from an employee except in certain circumstances such as receiving written permission from the employee or as required to monitor specific substances in the workplace.

What states have enacted statewide laws to govern health data privacy?

- **Maine**: Maine's 2019 Act to Protect the Privacy of Online Consumer Information "prevents the use, sale, or distribution of a customer's personal information by internet providers without the express consent of the customer." Personally identifiable information or other customer behavior could now only be released to other third parties with the express consent of that consumer.
- **California:** California's Consumer Privacy Act seeks to regulate the privacy of consumer-generated data by allowing consumers to opt-in or opt-out of sharing specific pieces of consumer health and mobile data.

What proposed laws exist that aim to govern privacy?

In recent years a number of bills have been introduced to help better govern consumer data, and specifically, consumer health data.

The Protecting Personal Health Data Act: Senators Amy Klobuchar (D-MN) and Lisa Murkoski (R-AK) introduced the Protecting Personal Health Data Act in June 2019 to protect consumer

health data through better regulations for consent, opt-out, and access to personal health data. The proposal also includes an amendment to create a National Task Force on Health Data Protection which would evaluate and provide input to address cybersecurity risks and privacy concerns associated with consumer products that handle personal health data. The task force would also monitor the development of security standards for consumer devices, services, applications, and software.

In addition to the Protecting Personal Health Data Act, two different laws were introduced in the Commerce Committee to help regulate consumer access to data. They are the following:

The Consumer Online Rights Privacy Act (COPRA): Introduced by Senator Maria Cantwell (D-WA), this bill aims to establish a set of foundational rights for consumers and protect them from harmful data practices. The legislation would grant consumers a right to access their data, the right to control the movement of their data (especially as it moves to third parties), and the right to correct or delete their data. COPRA also ensures that there are heightened data standards for sensitive data such as biometric or geolocation data, and creates new enforcement powers for the FTC.

United States Consumer Data Privacy Act: Being developed by Senator Roger Wicker (R-MS) and the Commerce Committee, this bill puts new authority into the hands of the FTC and state attorneys general. The law would create a national data privacy standard that will supersede state privacy laws and would be similar to the European General Data Protection Regulation. The act does include a right of access but does encourage consumer control over their data by requesting that it be corrected, deleted, or made portable. The law also encourages consumers to consent or opt-out of data practices in a clear way.

Additional bills have also been introduced in the wake of COVID-19 to better manage and regulate privacy among applications and services that request patient data. These include:

Exposure Notification Privacy Act: Introduced by Senator Maria Cantwell (D-WA) and Senator Bill Cassidy (R-LA), the bill would require affirmative consent and anonymized, aggregated data for mobile applications that use contact tracing during disease outbreaks. The bill also ensures that operators of these apps work with public health authorities and directly restrict data collection to the minimum amount necessary. The app operator must also delete the data of a patient if that patient requests this deletion.

Paul's Note: Reference previous newscan spreadsheet to review key privacy updates: https://docs.google.com/spreadsheets/d/10T60oo1I6xKKN4Ymc4zKBPXpF8JAIM1snkKg_OncNYg/edit#gid=0

Type of Content: Q&A