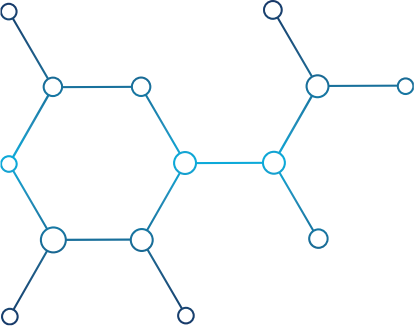
Health Privacy Principles for State Legislatures Regarding Use and Disclosure of Sensitive Personal Information by Non-medical Entities

ConnectedHealthInitiative



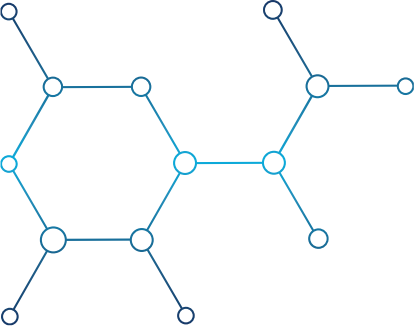
In the wake of the *Dobbs v. Jackson Women's Health Org*. decision, state and federal policymakers are responding with updates to health-related policy, including privacy, and seek the advice of industry to do so. Meanwhile, federal and state consumer protection enforcement agencies have recently prioritized the investigation of the collection, use, and transfer of sensitive personal information—including health data—occurring under existing law outside the scope of the Health Insurance Portability and Accountability Act (HIPAA).[1] In addition to federal and state consumer privacy laws, several states will have or already have comprehensive privacy laws to enforce.[2]

Policy makers now have twin imperatives: the development of consumer privacy law covering sensitive personal information and the protection of patients' access to digital health tools. Trade-offs between the two are made more pronounced given that, emerging from the global pandemic, reliance on virtual care and digital health tracking has only increased. Two years ago, a recent survey of the marketplace found about 350,000 digital health apps available across a wide range of app stores worldwide, with about 90,000 apps added to the stores in 2020 alone.[3] Surveys of consumer behavior also indicate that over 40 percent of Americans use wearable devices and apps to manage and monitor health metrics, and 90 percent of wearable device owners say they use them to track fitness and health.[4]

Mindful of these trends, state policymakers have a strong interest in safeguarding their constituents' access to innovative digital health options while tailoring the rules around collection, processing, transfer, and sale—as well as law enforcement's access to—sensitive personal information.

We urge state policymakers to consider the following principles as they seek to balance the protection of consumers' sensitive personal information against misuse or unauthorized access with the vital need for consumer access to digital health tools:

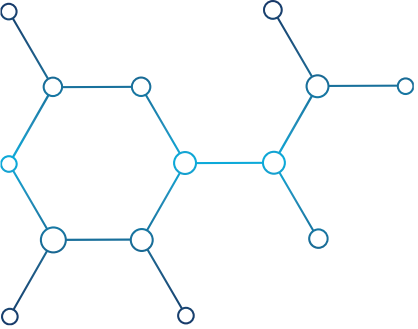
1. **Support a community-based approach to protecting consumers' sensitive personal information.** Protecting patients' access to reproductive health and their data requires a coordinated effort across the entire health care community, including digital health developers, health IT services companies, electronic health records (EHR) vendors, health system administrators, health information management professionals, and compliance and legal teams. For example, typically, if reproductive health information originating with a clinician in Washington is available via a health information exchange (HIE) to practitioners or other entities in Idaho, the Washington provider, the HIE, and the Idaho entities may be subject to differing requirements with respect to that information. If Washington caregivers are subjected to Idaho requirements and vice versa, the resulting conflicts of law may create a much broader standstill in personal health data interoperability and availability, which could negatively affect healthcare for everyone and aggravate preexisting clinician burnout.



2. **Focus on law enforcement agencies' access to sensitive personal information and access to such information via civil investigative process.** Many states seeking to bolster protections for sensitive personal information—including health information—outside the scope of HIPAA primarily endeavor to avoid the inappropriate investigation or enforcement of reproductive health service restrictions in their jurisdictions. Any disclosure of an individual's health information to law enforcement agencies should be permitted only within narrow and well-defined parameters. In particular, lawmakers should focus on eliminating the risk that an individual's reproductive health information may be used against an individual in a civil, criminal, or administrative proceeding, when the underlying action is permitted in the jurisdiction where it occurs.

To effectuate this requirement, any entity that engages in the commercial collection, processing, transfer, and sale of individuals' health information, should be required to comply only with legitimate requests for such information when accompanied by a written attestation that the recipient will not use or disclose the information for a prohibited purpose such as the use of an individual's health information for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking obtaining, providing, or facilitating reproductive health care that was legal under the circumstances in which it was provided.

a. **More granular warrant requirements.** States should also consider modernizing general requirements for warrant requests, consistent with consumers' evolving privacy expectations regarding their digital lives. For example, warrant applications and other requests for digital information may be overinclusive and may seek to enable a search of someone's entire device, when the information sought is limited to communications with a specific person or persons within a specific app. State statutes should keep up with modern expectations to require increased particularity in search requests.



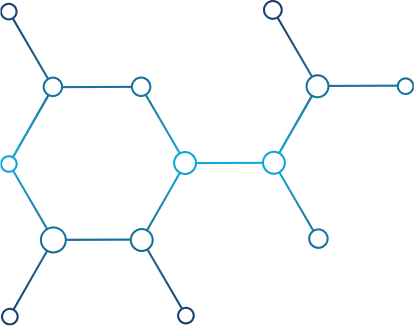
3. **Address limitations in technology.** Medical information must continue to be shared when and where it's needed. Patients, providers, and the entire care team rely on timely medical record interoperability. To continue advancing our progress in information sharing, unless a patient's record is withheld in its entirety due to the requester's failure to attest that it will not be used for a prohibited purpose (see above), reproductive health records and information related to abortion care often need to be segmented, segregated, or redacted before a record can be shared. Yet, technical capability to protect information at this level is not universally available and should be accounted for when addressing how to protect consumers' sensitive personal information against misuse or unauthorized access. Protection of privacy, promoting interoperability, and technical feasibility should be joint priorities.

4. **Focus on data minimization and purpose limitations while respecting consumer choice.** To further bolster interoperability and the sharing of medical information, patients and their care team must also trust that reproductive health records and information will not be misused by individuals or other entities. Policymakers should prioritize data minimization practices as well as limitations on the use of sensitive personal data consistent with comprehensive privacy laws and proposals that prioritize an individual's interest in governing the use and disclosure of their data. These proposals also include consumer rights requiring covered companies to respond to verified requests from individuals to delete, correct, or review information about themselves (among other things). Comprehensive privacy reforms could better balance the twin goals of ensuring better privacy and security protections for sensitive personal information as well as access to digital health tools.

    a. **Avoid commercial restrictions based on an overly broad definition of "sexual health" information.** If privacy restrictions seek to limit collection or processing activities involving data associated with accessing abortion services, they should be limited to information that indicates a consumer's attempt to acquire or receive "abortion services." Broader definitions may inadvertently sweep in over-the-counter product purchases for sexual health and browsing data unrelated to accessing abortion services.

5. **Avoid prohibiting improvement of digital health products and services.** Digital health tools are here to stay. We can expect worse outcomes and higher costs if the law effectively prohibits consumers from accessing them. Provisions that would prohibit transfer of certain user data points under a broad definition of "sale" that includes exchange of "valuable consideration" would drastically raise costs of simple product improvements, including those that would better protect privacy.

6. **Avoid dual regulation that could overcomplicate compliance and harm consumers**. State proposals should clearly exempt entities subject to HIPAA and health data privacy laws. If every state with a privacy law adopted differing requirements for protected health information (PHI) and non-PHI held by the same entity, the result would be unnecessary complexity across the country. Such a regime would inadvertently harm consumers by tying up digital health companies in compliance costs that fail to yield a commensurate consumer protection benefit and potentially diverting resources from product iteration and even privacy and security improvements.



7. **Avoid inappropriate restraints on collection and sharing of sensitive personal information for treatment, payment, and health care operations activities, consistent with HIPAA and subject to comparable privacy protections.** For entities that provide services directly related to treatment, but do not fall under HIPAA (i.e., because they do not engage in "covered transactions"), the ability to exchange data to enable the provision of treatment and the healthcare operations that undergird patient care is critical.

8. **Avoid imposing consent or other documentation requirements that are unaligned with consumer expectations or otherwise require the use of outdated mechanisms.** Some state proposals would require HIPAA-style authorization, which necessitates a great deal of friction and sometimes only authorizes collection and use for a short period of time. Where consumers expect to interface with an app or service within the app or on their devices, a requirement to provide a signed document to effectuate consent for collection or transfer of consumer information would render the service much costlier to provide and more unwieldy to use. Mandating high friction means of effectuating consent would fail to enable meaningful communication with consumers while imposing undue obstacles on their access to digital health tools.

9. **Enforcement.** The effective enforcement of any health privacy law begins with clarity about what the law requires of regulated entities. Definitional certainty is the bedrock upon which firms can construct frameworks of privacy by design. To the extent that enforcement is then necessary, it should stem from either concrete consumer harms or a pattern of infractions. Finally, private rights of action should be limited in scope to the relatively small universe of harms that are not otherwise redressable via agency enforcement.

Annotations

1. *Fed. Trade Comm'n, Flo Health Inc.*, FTC Matter No. 192 3113, settlement (Jun. 22, 2021), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc; Fed. Trade Comm'n, BetterHelp, proposed settlement (Mar. 2, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook; Office of the Atty. Gen., State of Calif., "Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information," (May 26, 2022), available at https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect.

2. States with comprehensive privacy statutes include: California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Utah, Virginia, and Oregon.

3. Emily May, Deloitte UK Centre for Health Solutions, "How digital health apps are empowering patients," HEALTH FORWARD BLOG (Oct. 19, 2021), available at https://www2.deloitte.com/us/en/blog/health-care-blog/2021/how-digital-health-apps-are-empowering-patients.html.

4. DELOITTE, MASTERING THE NEW DIGITAL LIFE: 2022 CONNECTIVITY AND MOBILE TRENDS, 3rd Ed., (Aug. 2022), available at https://www2.deloitte.com/content/dam/insights/articles/us175371_tmt_connectivity-and-mobile-trends-interactive-landing-page/DI_Connectivity-mobile-trends-2022.pdf.