John Ohanian
Chief Data Officer
California Health & Human Services Agency
1205 O St.
Sacramento, CA 95814

June 1, 2022

The Electronic Frontier Foundation (EFF) appreciates the chance to offer feedback on the health data exchange framework and data sharing agreement being developed pursuant to AB 133, signed into law by Gov. Newsom on July 27, 2021 (enacting Health and Safety Code § 130290).

AB 133 is intended to improve Californians' access to usable electronic information and enable the effective and equitable delivery of services to improve their lives, in compliance with all applicable federal, state, and local laws, regulations, and policies. We are concerned, however, that the timeline laid out by AB 133 is too ambitious given the complexity of this task in today's political environment.

The law requires that the California Health & Human Services Agency (CHHS) establish a Data Exchange Framework that includes a single data sharing agreement (DSA) and a common set of policies and procedures (P&Ps) to govern and require the exchange of health information by July 1, 2022. Equally important, AB 133 requires that certain covered entities (including hospitals, physician organizations and medical groups, skilled nursing facilities, health plans and disability insurers, clinical laboratories, and acute psychiatric hospitals) execute the DSA by January 31, 2023; these signatories are expected to exchange or provide access to health information with other mandated organizations by January 31, 2024.

EFF has attended several stakeholder meetings and it appears that, despite the staff's excellent and hard work, AB 133's breakneck pace is not sustainable. As the January 2023 deadline approaches, stakeholder discussion of the DSA and P&Ps has revealed many obstacles and unresolved ambiguities or disagreements. For instance, the providers who must sign the DSA first are not confident that it will apply to later signatories – who will include many non-traditional entities who are not HIPAA covered entities and thus not subject to HIPAA privacy/security standards and may not even have the technical or organizational capacity to safeguard received patient data. They therefore worry that the forced data-sharing could harm their patients' privacy or subject them to liability for such privacy harms. Legislation may be needed to relax the timeline as well as to provide additional enforcement authority.

Structural framework deficiencies

The data exchange framework contemplated by AB 133 is a massive undertaking. Health data has long been deemed sensitive, and any DSA for health data should meet demanding privacy, security, and integrity criteria. Privacy concerns have only grown as the pandemic exposes many weaknesses in our health care system, including as it relates to public health.

Moreover, AB 133 is intended to include not merely electronic health information (EHI) but also SDOH (social determinants of health) data, data related to underserved or underrepresented populations, behavioral health and substance use data.

Not only is signing the DSA mandatory under AB 133, but the law covers entities that are subject to disparate legal and regulatory requirements in terms of privacy and security. Hospitals and other medical providers must comply with federal HIPAA as well as the state CMIA. State and local government agencies usually are not "covered entities" under HIPAA and have less stringent privacy rules. Indeed, under current California law, state agencies are governed by the Information Practices Act, while local government entities are not. Meanwhile, county behavioral health services (not yet required to sign) have been historically underfunded and may lack the IT infrastructure needed to participate, yet also deal with data subject to different standards than HIPAA itself.

In terms of legal compliance, this creates a complex situation. EFF has heard from providers and other stakeholders that they are concerned that signing the DSA will expose them and their patients to significant privacy risks. They also worry they may face liability from sharing patient data under a vague contract in which it is not clear what their sharing partners can or cannot legally do. Currently, however, the DSA speaks generally in terms of "applicable law" even though many are unsure of their legal obligations. If Entity "A" is expected to share data with Entity "B", how can they be sure that they each have the right authorizations or proper patient consent?

This is not merely a legal compliance problem, however. It is also not clear what data needs to be shared, and in what standards-based formats, for providers and plans to comply with AB 133 – which should include clarity on which data must be shared proactively in real-time and which data can be shared in response to queries.

This question of "what data" is exacerbated by the fact that AB 133 contemplates the inclusion of mental health and substance use disorder health information, including information that is protected under 42 CFR Part 2. Historically, it has been a significant challenge to determine how records covered under 42 CFR Part 2 regulations can be shared within integrated care settings, with interpretation and implementation of these regulations varying across the state.

At least one large county behavioral health department in California recently undertook developing and implementing a universal consent form to be used across providers and delivery systems and discovered that providers were often unclear about when and how consent was obtained, and whether the consent on file was still valid.

Of course, to speak of consent is to bring patients and individuals to the fore. While the DEF is intended for the benefit of Californians, the DSA is a contract signed by entities, not patients. Will individuals be able to know what of their data has been shared from their medical providers? Will they know how often it has been shared, to whom, for what reasons? Will they be able to prevent data that they consider to be sensitive or confidential

from being shared? If individuals have no control of their own data, they will lose trust in their providers and in the system.

We can approach this question of patient trust from the opposite direction as well. What happens if a signatory to the DSA shares patient data or otherwise harms patient privacy or autonomy? Sadly, it is not at all clear in the current state of the DSA. As noted earlier, providers and payors (and their business associates) are generally regulated by the relatively familiar HIPAA rules. But many entities that will be signing the DSA are not subject to HIPAA, like social service organizations and community support providers.

Of course, it is well known that even HIPAA safeguards are no panacea. Just last week, it was reported that a GE Healthcare customer, a global drug research company named Quintiles, "had taken data GE considered confidential — millions of patient medical records stripped of identifying information — and linked it to a massive trove of insurance claims, vacuuming up financial details tied to the patients' medical problems, prescriptions, and doctor's visits."[1]

It makes sense to facilitate data-sharing among disparate entities that support patients, but unauthorized data-sharing will not only hurt patients but also make it harder to build trust. Unfortunately, AB 133 included neither language about enforcement or compliance, nor assigned any authority for enforcement or compliance. Stakeholders have repeatedly expressed concern that unauthorized or unlawful data-sharing is a serious risk that may be impossible to mitigate without significant enforcement or compliance authority. The question of anticipated actual compliance with all applicable laws cannot be continually kicked down the road. No responsible health provider would want to share data into a system that does not protect patient privacy.

Implications for individuals seeking reproductive care

As noted, Gov. Newsom signed AB 133 in July 2021. In September 2021, Texas adopted a law allowing residents to seek civil damages against anyone who aids an abortion after six weeks of pregnancy. Clinics in Texas shut down to avoid a deluge of lawsuits. "Thousands of patients are now seeking abortions elsewhere, overwhelming neighboring Oklahoma and New Mexico and pushing some women further afield to more friendly states including California."[2]

---

[1] Casey Ross. "How a complex web of businesses turned private health records from GE into a lucrative portrait of patients." *StatNews*. https://www.statnews.com/2022/05/23/hipaa-patient-ge-data-privacy-profit/

[2] Alexei Koseff. "'When you don't know where to go, you come here:' California preps to be a haven for abortion rights." *CalMatters*. https://www.kpbs.org/news/local/2022/05/04/when-you-dont-know-where-to-go-you-come-here-california-preps-to-be-a-haven-for-abortion-rights.

Indeed, after the Texas law took effect, Gov. Gavin Newsom convened a coalition of reproductive rights, health and justice groups, to explore how to make the state a "sanctuary" for abortion. (See, e.g., https://www.cafabcouncil.org/) In May 2022, the public is now increasingly aware that reproductive rights are in political jeopardy after the leaked Supreme Court decision in the case of *Dobbs v. Jackson Women's Health Organization*.

Will the data-sharing agreement and its policies and procedures allow out-of-state actors who do not respect reproductive rights—including out-of-state law enforcement—to obtain data about persons seeking or providing abortions in California? Will patients be able to prevent the sharing of information that they consider confidential? This is just one example of the ways this information can be used to harm individuals. Other vulnerable populations should also be concerned, given the inclusion of SDOH data: domestic violence and human trafficking survivors, for example, can be at risk from provider disclosures; some out-of-state public officials even regard gender-affirming care for transgender children to be child abuse.

If ever there were a time to be concerned that a nascent data-sharing framework might have unintended consequences, it is now. We respectfully urge you not to rush the development of a structure, so that the state may carefully consider and center data privacy concerns and avoid needless harm.

Sincerely,

Lee Tien
Legislative Director and Adams Chair for Internet Rights
Electronic Frontier Foundation