Interoperability MATTERS
an initiative of The Sequoia Project

DRAFT

Guidance to States: *Legislating Technical Standard Definitions for Existing State Sensitive Health Data Laws*

October 23, 2025

This draft is provided for public comment.
Please submit feedback to interopmatters@sequoiaproject.org by November 26

the sequoia project

Table of Contents

1. Introduction

Health data today is managed digitally. It is stored, maintained, processed, used, and exchanged across vast array of different information technology (IT) systems, platforms, and networks operated by an equally vast and diverse range of individuals and entities, from health care providers and health plans, public health departments and other governmental authorities, to third party applications and individuals (*e.g.*, patients, consumers, and their personal representatives and designated proxies) using a wide arrange of software and related services. As the nation moves toward greater interoperability—where health data should flow seamlessly and securely without special effort on the part of the user—there is an urgent need to ensure that privacy protections, particularly for sensitive health data, can keep pace and that the need for compliance with those privacy protections, doesn't bring interoperability to a grinding halt.

Federal law sets certain requirements for health information privacy but also allows states to set their own standards that are more privacy protective. Many states have long had laws on their books that provide heightened privacy protections for certain categories of sensitive health data generated by health care providers and health insurers, such as behavioral health, substance use disorder treatment, communicable disease treatment (including for sexually transmitted diseases/infections and HIV/AIDS), reproductive health, genetic testing, developmental and intellectual disabilities, and care provided to minors. And there has been an expansion of such laws, including provisions limiting the sharing of some data across state lines. However, these protections or restrictions cannot be meaningfully enforced in digital and networked environments without a technical infrastructure capable of recognizing and acting on those protections or restrictions. Inconsistent implementation within and across systems and jurisdictions creates confusion, increases risk of inadvertent sharing, and undermines trust that may ultimately lead to sharing less than is authorized, which may impact patient safety and health. Over-protection through blanket restrictions on an entire patient record can create a lose-lose scenario by increasing the risk of a privacy breach, since blocking access to harmless data may signal the presence of sensitive conditions elsewhere in the record, and reducing data sharing below the level the patient would ultimately prefer.

This paper offers guidance to states on how to bridge this gap by aligning their existing sensitive health data laws, applicable to health care providers and health insurers, with national technical standards for identifying sensitive health data. This alignment lays the foundation for enabling high-confidence, ***automated*** systems that apply each state's privacy rules and support an individual's privacy preferences with respect to how their

sensitive health data is shared. The goal of this guidance document is to create a common technical language for what constitutes sensitive health data, so we can better automate privacy rules and individuals' consent preferences at a granular level.[1] Building on the Sequoia Project's *Moving Toward Computable Consent: A Landscape Review* (April 2025), which outlined the policy and technical challenges of managing consent and privacy in electronic systems, this guidance gives states a practical path forward—one that supports privacy rules and computable consent by ensuring that sensitive health data can be consistently recognized and acted upon across technologies and jurisdictions.

2. The State Autonomy Principal

Federal privacy laws like the Health Insurance Portability and Accountability Act and its implementing regulations (collectively, "HIPAA") set a national baseline for the protection of health data but these laws expressly allow states to enact more stringent privacy protections.[2] This principle of state autonomy is foundational to the United States health privacy framework and reflects the important role states play in safeguarding the dignity, rights, and unique needs of their residents. As health data flows more easily across networks and jurisdictions, it is essential that this right of states to establish and enforce higher standards of privacy is not only preserved but technically supported.

State autonomy in health privacy is not an abstract principle; it manifests through the practical realities of lawmaking. State-level sensitive health data legislation—like most legislation—is incident and constituent driven. Patient experience narratives matter and can drive lawmakers to act on narrow yet meaningful gaps in data privacy. Indeed, many states have taken action to restrict sensitive health data more robustly than HIPAA by requiring patient consent for the use and disclosure of certain sensitive health data for treatment, payment, and ordinary health care operations. Still others impose additional procedural requirements on the use or disclosure of certain sensitive health data, such as giving the patient notice and opt-out rights or requiring that the recipient be given notice of prohibitions on redisclosures of the sensitive health data. For example, some states mandate a patient's explicit consent before disclosing genetic test results, even to other treating providers, and impose blanket prohibitions on the disclosure of such results to

[1] This guidance document does not expressly address the identification and tagging of sensitive data under consumer data laws that don't apply to individuals and entities (or data) regulated under federal and state laws generally applicable to health care providers and health insurers. Nor does it address the federal or state laws applicable to the use and disclosure of public health or other governmental data held by public health authorities or other governmental bodies. However, the same principles may apply.

[2] 45 C.F.R. § 160.203.

health insurers.[3] Other state laws give adolescents the right to control access to their behavioral health data,[4] reproductive health data,[5] or other health data generated from certain sensitive health care services for which the adolescent has the right to consent without parental/guardian consent.[6] In the wake of shifting federal protections for abortion care, some states have adopted laws that prevent abortion-related health data from being shared with, or accessed by, entities in other states or for purposes where such data might be used to investigate or prosecute patients and/or providers. These laws reflect each state's policy choices about the amount of privacy and autonomy they desire to give their residents. Any effort to achieve interoperability must account for and enable the implementation of those choices.

Appendix A includes a listing of common sensitive health data categories that may be more stringently protected under certain state laws.

3. The Need for Technical Standards: One Language for Technical Interoperability

In order for digital health data to flow consistently and reliably across systems, there must be a shared technical language - a single, standardized way for systems to interpret health data. Specifically, we're referring to assigning a category to the sensitive health data (*e.g.*, a security label) that can stay with the data when it is shared. This allows those sending and receiving data to appropriately protect the data in the context of the confidentiality policy (*e.g.*, jurisdictional privacy rule or patient consent) that applies to that sensitive health data. Without this, technologies may exchange health data, but they cannot truly interpret if and whether that health data contains particularly sensitive health data subject to applicable privacy and consent rules. Sensitive data may be mislabeled, privacy protections lost, or critical information overlooked entirely when technologies cannot appropriately communicate this information with each other using a single, standard language.

The current state of data segmentation for privacy and consent rules in digital health environments creates an unsustainable patchwork: many systems, each defining their

[3] *See, e.g.*, N.Y. Civ. Rights Law § 79-l (McKinney).
[4] *See, e.g.*, Tenn. Code Ann. §§ 33-3-104 and 33-8-202.
[5] *See, e.g.*, West's Ann. Cal. Fam. Code § 6925. In such circumstances, the minor (not the parent/guardian) is the individual who controls the release of those records. *See* 45 C.F.R. § 164.502(g)(3)(i)(A).
[6] *See* 45 C.F.R. § 164.502(g)(3)(i)(A); *see, e.g.*, A.R.S. § 44-132.01 (minor may legally consent to treatment for venereal disease); C.R.S. § 25-4-409 (minor may legally consent to examination for a sexually transmitted infection); Fla. Stat. § 384.30 (minor may legally consent to sexually transmissible disease treatment). Each state has many different instances in which minors of any age or certain ages may consent to certain type of health care services without parental/guardian consent.

own terms, working toward a common goal but ultimately unable to coordinate because they do not share the same language. Because of this variability that lacks a common vocabulary, today's electronic health IT systems cannot implement meaningful privacy and consent rules across systems, platforms, networks and diverse technologies, unless they are aligned on a shared technical standard and vocabulary of what constitutes different categories of sensitive health data, across each state's privacy and consent rules.

This is why the use of national technical standards, implementation specifications and guidelines—such as the standards being developed by organizations like Health Level Seven International® (HL7®)[7] with the HL7 security labels, confidentiality codes, and sensitivity value sets and the profiles and implementation guides developed by Integrating the Healthcare Enterprise (IHE)[8]—are so critical. They aim to provide the common rules, codes, and definitions that create a unified technical language for understanding how to identify information that falls under each sensitive category, and how to record and communicate this identification in the form of security labels in different data structures and protocols, such as identifying what structured elements in health data make that data categorically behavioral health data, substance use disorder data, communicable disease data, reproductive health data, gender affirming care data, and so on. States can continue to define what information is sensitive under their own laws, but without a shared technical language, those protections risk being enforced inconsistently or lost the moment data leaves one system or state and enters another. Appendix B covers in more detail the importance of standardized data segmentation (*e.g.*, tagging) and how that segmentation is foundational to supporting granular consent options for patients whose information is shared in electronic and networked environments.

To be clear, this standardization of the categories of sensitive health data is only one component of the types of technical solutions necessary to identify and segment sensitive health data to then apply privacy rules to the sensitive data based on various applicable policies, including state and other jurisdictional laws, patient preferences, and provider policies. Because many state and federal laws also apply privacy protections based on the type of *data source*—as opposed to the category of sensitive health data—it remains necessary to allow regulated individuals and entities to apply security labels associated with certain sensitive health data categories to all the data from certain data sources even if the attributes of the underlying data set may not seem to fall within the sensitive health data category. For example, under the federal law governing substance use disorder records (42 USC 290dd-2 and 42 CFR Part 2 (collectively, "Part 2")), all personally

[7] HL7 is a global standards-developing organization that creates frameworks and standards for the exchange, integration, sharing, and retrieval of electronic health information.
[8] IHE is an international initiative launched by health care professionals and industry to improve the way computer systems in health care share information. IHE defines the rules of the road for how to use existing standards to support specific use cases.

identifying information created by or received from a federally assisted substance use disorder treatment program (*e.g.*, medication-assisted treatment (MAT) clinics) is subject to Part 2 protections. This includes information that may not appear, on its face, to relate to substance use, such as information about the patient's migraines or bipolar disorder.[9] In these situations, the regulated individual or entity may need flexibility to apply the "substance use disorder information" security label to the entire data set—including physical and mental health data—so the disclosing system can send it with the required Part 2 notice and consent, and the receiving system can accept the label and apply the appropriate Part 2 confidentiality rules.

4. Model Language for Sensitive Health Data Definition

States have long played a central role in shaping health data policy by defining what information is legally protected and by requiring the technical means to enforce those protections. Just as states have previously mandated standardized formats for electronic claims processing and eligibility checks to ensure efficient communication between providers and health plans, they now have an opportunity to do the same for sensitive health data. By adopting legislation that relies on standardized technical definitions for categories of sensitive health data, states can bridge the gap between legal rules and technical implementation, ensuring that their privacy protections are not only meaningful in principle but actionable in practice.

The model language in this document provides states with a legislative framework for defining sensitive health data categories in a way that aligns with national technical, clinical, administrative, and financial terminology standards. This approach empowers states to preserve their policy autonomy while contributing to a unified technical language for privacy—so that sensitive health data protections travel with the information across systems, technologies, and jurisdictions.

Please note: The blue bracketed language indicates that the state will need to modify the language to integrate with the terms and terminology used by that state's health data privacy and security laws.

[9] *See, e.g.*, ONC/SAMSHA, Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me?, *available at* https://coephi.org/app/uploads/2021/05/SAMHSA-guidance-Part-2-applicability.pdf.

4.1. Model Language on Electronic Sensitive Health Data Segmentation Standards

1. Purpose.

The purpose of this section is to support the adoption of national standards for identifying and segmenting sensitive health data, enabling [state] to implement meaningful, consistent privacy protections that can be communicated across technologies and across state lines. Without standardized technical definitions of sensitive health data, [state's] heightened protections cannot be effectively applied or enforced in networked environments. This section advances both privacy and interoperability by establishing computable safeguards aligned with national standards.

2. Definitions.

For purposes of this section, the following definitions apply:

"Business" means any legal entity, including a corporation, partnership, limited liability company, association, trust, joint venture, nonprofit organization, governmental entity, quasi-governmental entity, or any other organization, whether for-profit or not-for-profit, that is formed, organized, or authorized to operate under the laws of this state, any other state, or under the laws of the United States, and that conducts operations, engages in commerce, or offers goods or services within this state. It does include a natural person acting in their individual or personal capacity.

"Sensitive Health Data Law" means those state laws for which the state provides privacy protections that are more stringent than those provided by the Health Information Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act, and their implementing regulations.

"Standard Sensitive Data Codes" means those value sets developed by HL7® International and adopted and approved by the [appropriate state regulator] in accordance with [the statute that gives that state regulator the authority to promulgate rules and regulations].

3. Sensitive Health Data Segmentation Standards.

(1) A Business that electronically stores or maintains [health information] on the provision of [health care services] on behalf of a [health care provider], [health care insurer], [patient/caregiver], or contractor or subcontractor of the foregoing, shall use Standard Sensitive Data Codes to support compliance with the State's Sensitive Health Data Laws. A Business that complies with this Section shall be deemed to have appropriately identified the data subject to the applicable Sensitive Health Data Law.

(2) (A) The Standard Sensitive Data Codes required in subsection (1) shall be adopted and approved by the [designated regulatory authority] in accordance with [the statute that gives that state regulator the authority to promulgate rules and regulations].

(B) When adopting rules under this Section, the [designated regulatory authority] shall:

(i) consult with national and state organizations involved with the standardized exchange of health data, and the electronic exchange of health data, to develop and implement Standard Sensitive Data Codes;
(ii) if applicable, meet federal mandatory minimum standards following the adoption of any national requirements for the transaction of sensitive health data; and
(iii) may not require a [health care provider], [health care insurer], [patient/caregiver], or contractor or subcontractor of the foregoing to use a specific software product or vendor.

(3) Nothing in this Section shall prohibit a Business from implementing additional standards, implementation specifications, or technologies for the purpose of segmenting data, provided that all of the following conditions are met: (A) its use is not prohibited under other applicable law; and (B) such implementation does not impede or compromise the ability to transmit or receive Standard Sensitive Data Codes in accordance with regulations promulgated under this Act.

4. Compliance Deadlines and Enforcement Discretion.

(1) A Business shall not be required to implement Standard Sensitive Data Codes as required under this Act until the [designated regulatory authority] promulgates final regulations specifying the applicable standards, formats, implementation specifications, and technical guidance for such codes.

(2) Following the effective date of the final regulations promulgated under subsection (1), a Business shall have not less than two (2) years to comply with the requirements related to Standard Sensitive Data Codes. The [designated regulatory authority] may extend this compliance period for one or more classes of Businesses or for particular use cases, upon a showing that such extension is necessary to ensure feasibility, interoperability, or continuity of operations.

(3) Notwithstanding any other provision of this Act, the [designated regulatory authority] may exercise enforcement discretion and shall not impose penalties or sanctions against a Business for noncompliance with the requirements related to

Standard Sensitive Data Codes if the Business demonstrates that it has made, and is continuing to make, good faith and commercially reasonable efforts to come into compliance. In determining whether to exercise enforcement discretion under subsection (3), the [designated regulatory authority] may consider factors including, but not limited to: (i) the size and resources of the Business; (ii) the nature and scope of the Business's data segmentation practices; (iii) any documented efforts to assess, plan for, and implement compliance measures; (iv) the extent to which the Business has engaged with industry guidance, vendors, or relevant implementation resources; and (v) any unforeseen technological or interoperability barriers beyond the Business's control.

5. Call to Action

Policy language and technical standards are essential, but they do not create adoption on their own. To ensure patient privacy is meaningfully protected while enabling appropriate data sharing, we call on states and interested stakeholders to take the following steps:

(1) **Evaluate the model for uniform sensitive health data segmentation in state contexts.** First and foremost, we recommend that states evaluate whether and how they could adopt the guidance above to ensure alignment with developing national technical standards and each states' existing sensitive health data laws. Both lawmakers and relevant state agencies should be engaged and special consideration should be given to implementation deadlines and enforcement discretion given that national standards for data segmentation are still developing.

(2) **Strategic planning and program management.** Comprehensive planning will be needed at the state and industry level prior to implementation efforts in order to: (A) clarify goals, objectives, and scope; and (B) identify ownership and authority. Designating a clear project owner for the state's efforts and securing stakeholder leadership across affected agencies and organizations is critical to shepherd new processes through development, implementation, and ongoing operation.

(3) **Infrastructure and technology funding.** To advance compliant sharing of sensitive health information that honors individuals' privacy preferences will require investments in infrastructure, data management, and implementation. States may want to consider funding sources such as:

a. State budget appropriations;
b. Medicaid Enterprise Systems (MES) funding;
c. Federal, or other, grants such as from the National Science Foundation, National Institutes of Health, or a state department of human services. National Science Foundation (NSF), National Institute of Health (NIH), a state Department of Human Services (DHS); or

d. CMS Innovation Models such as Transforming Maternal Health.

(4) **Multi-agency collaboration and stakeholder engagement for implementation.** Use cases involving sensitive data often require coordinated action across multiple agencies and organizations, which may be best facilitated using a state-sponsored technical working group with workgroup members from each agency and appropriate subject matter experts. For example, behavioral health initiatives may involve mental health, public health, Medicaid, child services, aging, technology, corrections, and privacy/security agencies. Coordinated planning across all relevant entities creates more efficient and comprehensive implementation. Beyond government agencies, states should engage statewide associations, health information networks/exchanges, health IT vendors, health care organizations, social services, behavioral health providers, education systems, municipalities, and other key partners. Involving end users in the implementation process improves adoption and usability.

(5) **Education and guidance.** As states adopt standardized approaches to sensitive health data, they will need to also issue clear, accessible guidance to regulated entities and the public on how sensitive health data protections will be implemented, enforced, and integrated into existing privacy frameworks. Such communications are essential to successful implementation and building and maintaining trust.

6. APPENDIX A

This Appendix A includes the following:

- A non-exhaustive listing of the categories (and subcategories) of health data generated by health care providers or health insurers that may be subject to heightened privacy protections under state laws; and
- A discussion of how the use of non-medical and non-technical terminology to describe these categories[10] can lead to inconsistent interpretation and application to the detriment of individual privacy as well as interoperability, as wary health care institutions opt to simply not share health data rather than risk non-compliance. As discussed in the guidance document, we believe that each state's preferences and descriptions of these categories can remain unchanged while passing legislation that enables technology systems to consistently implement a language for identifying and functionally marking [11] these categories so that appropriate confidentiality policies and individual preferences can be applied and shared across different technical systems, platforms, and networks.

6.1. Sensitive Health Data Categories and Subcategories

The following is an illustrative (but not exhaustive) list of the types of sensitive health data categories that need to be supported through standardized technical standards:

- Communicable diseases, including without limitation HIV/AIDS and sexually transmitted diseases/infections (STDs/STIs)
- Mental or behavioral health
- Reproductive health care, including without limitation abortion, contraceptive care, *in vitro* fertilization, and family planning
- Gender affirming care
- Substance use disorder (SUD) (*e.g.*, drugs and alcohol)
- Genetic test results and/or genetic information
- Developmental or intellectual disorders
- Immunization records
- Other diagnosis or injury specific information (*e.g.*, COVID diagnosis, malignancy, brain tumors/injuries, etc.)

[10] This Appendix does not cover those state laws that more stringently protect records held or created by public health authorities or other governmental bodies.
[11] How sensitive data is functionally identified can vary depending on the technology. Functional identification can be done via tagging and/or other technical functionality that can distinguish the sensitive data.

6.2. Unintended Consequences

Often, states use non-medical and non-technical terminology in their definitions of sensitive health data categories. Inconsistent interpretation and application of such definitions can lead to a host of unintended consequences, including but not limited to:

- Inadvertent disclosures of sensitive health data;
- Inadvertent withholdings of health data from lawful uses and disclosures;
- Wholesale withholding of all health data, including but not limited to the potentially sensitive health data, due to data segmentation infeasibility issues and the need to comply with the legal preconditions of the most restrictive laws; and
- Decreased access to care where patients cannot trust how their data is being shared across multiple different organizations and across state lines.

These unintended consequences can be significantly ameliorated if states follow the suggestions in this guidance document to adopt technical definitions for these categories that are based on nationally recognized standards that are tied to the appropriate medical and technical terminology.

7. APPENDIX B

This Appendix B discusses the importance of standardized data segmentation and how that segmentation is foundational to supporting granular consent options for patients whose information is being shared in electronic and networked environments.

Over the past decade, one of the central goals of patient privacy regulations and supporting technologies has been to move beyond binary, all-or-nothing control models, such as simple “opt-in” or “opt-out” mechanisms, toward more granular data control. This shift recognizes that individuals may have different comfort levels with different types of data, and should not be forced into a single, blanket choice about how much, what, and in what manner their data is shared with others. Granular control empowers patients to make nuanced decisions about who can access different parts of their health information and to what extent. This increased autonomy can enhance trust in the health care ecosystem and foster a stronger sense of agency. Importantly, when patients can restrict access to only their most sensitive information while allowing broader use of non-sensitive data, they may feel more comfortable participating in data sharing initiatives. This, in turn, supports more robust health research, public health efforts, and innovation, while still respecting individual privacy preferences.

Granular control can be expressed across multiple dimensions, including specific time frames, care settings, types of clinical encounters, or even individual data authors. However, at its core, the purpose of granular control is to give patients a meaningful and manageable way to express their privacy preferences around sensitive categories of data without manual selection of individual data items. For example, a patient who is uncomfortable sharing information related to reproductive health should not be expected to comb through their medical record and individually identify each note, lab result, or diagnosis code that falls into that category. This approach is not only burdensome and inefficient but also assumes a level of familiarity with clinical terminology and health record structures that most patients do not possess. Instead, a more effective model allows the patient to simply indicate that any data classified under a predefined category, such as “reproductive health,” should be withheld from sharing. This approach aligns privacy controls with patients’ intuitive understanding of their own privacy concerns.

Similarly, state policymakers, including legislators and agency leaders, can express policies based on common terms (such as “substance use disorder treatment” and “genetic data”), rather than delving into deep clinical definitions. By creating precise interpretations of these predefined legal categories, security labeling enables health IT systems to implement the intent of the law.

In sum, security labeling enables patients and policymakers to express preferences and policies in broad terms and simply by referencing sensitive categories rather than enumerating specific data elements. For example, a patient can prohibit sharing of certain data simply by naming the sensitive data category and then the security labeling service determines what data is subject to such a rule. At an abstract level, the security labeling service is a semantic mediator that closes the gap between the intuitive notion of a sensitive data category such as “substance use disorder treatment” or “behavioral health” and its precise instances, thereby giving the patient the ability to express their preferences with terms based on a common-sense expectation of privacy.

On the enforcement side, such rules can be adjudicated by a rules-based policy engine by relying on the security labels, as attributes of the data, to determine whether a rule about a sensitive category applies to a particular data element. By providing a mechanism to identify individual data elements subject to each sensitive category, security labeling makes the enforcement of such rules possible.

The Shift Collaborative, a nonpartisan, multi-stakeholder initiative that develops privacy-respecting tools and guidance, has developed a publicly available sandbox where interested parties can explore a variety of use cases leveraging synthetic data. This tool demonstrates the dynamic application of sensitivity labels based on a patient’s consent options and will allow stakeholders to test and validate the use of standards-based workflows in their own systems using comprehensive open-source sensitive data value sets. This sandbox is available at: https://shiftinterop-sandbox.technicise.eu/.