Interoperability MATTERS
an initiative of The Sequoia Project

Moving Toward Computable Consent: A Landscape Review

April 24, 2025

the sequoia project

Table of Contents

Abstract

This landscape review explains the importance of managing privacy and consent when sharing personal health information, scans the current landscape of challenges facing those entrusted with personal health information, enumerates existing solutions, and explores the strengths and deficiencies of these approaches.

---

1. Introduction

As the sharing of health information becomes more widespread and commonplace, the ability to manage privacy expectations and consent requirements becomes even more important. This is particularly true as state-level policies on sensitive healthcare data diverge and create increased sensitivity about what data are accessed or shared. However, the healthcare field currently lacks tools and local policies to: (1) efficiently support the collection and sharing of computable consent (or a mechanism to record, share, and receive individuals' consent preferences through automated means); (2) routinely act on individual data elements in accordance with individuals' privacy preferences; and (3) effectively comply with complex and variable state, local, territorial, and tribal privacy rules. Increasingly, it is policy requirements that are driving technical, operational, and business responses. In January 2024, The Sequoia Project established a Privacy and Consent Workgroup as a part of its Interoperability Matters cooperative to tackle these challenges.

The Workgroup draws on the expertise of dozens of subject matter experts (SMEs) from across the health community, including healthcare providers, health information exchange leaders, technology and standards specialists, consumer and patient advocates, and privacy and other SMEs. It also includes liaisons from four federal agencies: the Office for Civil Rights (OCR) and the Assistant Secretary for Technology Policy's (ASTP) Office of the National Coordinator for Health IT (ONC) within the U.S. Department of Health and Human Services (HHS), the Social Security Administration (SSA), and the U.S. Department of Veterans Affairs (VA). (See Appendix 5 for a list of Workgroup members.)

The Workgroup is chartered to catalog key impediments to operationalizing privacy and consent policies and describe whether and how standards-based, automated technical solutions can support health information exchange at a national scale that appropriately protects privacy and respects individual preferences. In doing this work, the group

focuses on making progress at the implementation and operational level. While the Workgroup may also identify areas for federal and state policy attention, that is not its core focus.

This landscape review is a first step and reflects lessons learned from a series of presentations from those working to implement privacy and consent approaches at state, regional, and local levels (see section 6 below for a summary of the presentations). An initial draft of this paper was published in January 2025 for public feedback. The thoughtful and constructive feedback from stakeholders has been incorporated into this final paper. The Sequoia Project is thankful for the contributions of the Workgroup members, the organizations named in the paper, and those who contributed during the public feedback period.

Building from this baseline knowledge, the Workgroup intends to continue the work by identifying best practices and developing other practical guidance in collaboration with aligned organizations to further our collective ability to safely share health information to support better health and care, while also supporting the privacy and consent preferences of individuals.[1] The Sequoia Project also wants to hear from interested organizations to consider forming a new coalition that builds from and amplifies existing efforts.

2. Individual Perspectives on Privacy and Consent

Survey data over time demonstrates that individual consumers and patients want electronic access to their personal health information, for themselves, their caregivers, and their medical providers, to improve care. Surveys also consistently show that individuals have concerns about the privacy of their electronic medical records. Certain populations, including those with mental and behavioral health issues, are likely to have heightened concerns (See Text Box below for a sample of survey data over the years.)

[1] For readability, this document uses the term consent in a general sense. Certain laws, such as HIPAA, use alternative terms, such as authorization. While the legal differences are meaningful, it is beyond the scope of this paper to parse these terms.

Survey Findings Regarding Attitudes Toward Health Information Privacy

- 89 percent of people want their doctors to electronically exchange information with other doctors.[2]
- The adoption of electronic medical records led to consumer concerns about identity theft or fraud (80%), use of medical information for marketing purposes (77%), employers accessing health information (56%), and insurers seeing health information (55%).[3]
- 81 percent of patients favor increased access to health information for patients and providers.[4]
- 84 percent of individuals express confidence that their medical records are safeguarded from unauthorized viewing, but 66 percent express concerns about the privacy of their records when their data is electronically exchanged.[5]
- Nearly 75 percent of patients expressed concern about the privacy of their personal health data outside of clinical care settings.[6]

The role of consent in information sharing can be seen as both a way to bolster trust in data sharing and a mechanism that prevents the transmission of incomplete information. As discussed further below, identifying approaches such as consent management solutions and data segmentation tools that allow individuals to provide granular consent that can be shared through automated tools, could create a path forward. While some progress has been made in creating these types of tools, this approach faces technical and operational challenges.

---

[2] S. K. H. How, A. Shih, J. Lau, and C. Schoen, *Public Views on U.S. Health System Organization: A Call for New Directions*, The Commonwealth Fund, August 1, 2008, https://www.commonwealthfund.org/publications/other-publication/2008/aug/public-views-us-health-system-organization-call-new.

[3] *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*, Markle, November 1, 2006, https://www.markle.org/publications/1214-survey-finds-americans-want-electronic-personal-health-information-improve-own-hea/.

[4] *Most Americans Want to Share and Access More Digital Health Data*, Pew, July 27, 2021, https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2021/07/most-americans-want-to-share-and-access-more-digital-health-data.

[5] *Individuals' Perceptions of the Privacy and Security of Medical Records and Health Information Exchange*, Assistant Secretary for Technology Policy, June 2019, https://www.healthit.gov/data/quickstats/individuals-perceptions-privacy-and-security-medical-records-and-health-information.

[6] R. Mills, *Patient Survey Shows Unresolved Tension Over Health Data Privacy*, July 25, 2022, https://www.ama-assn.org/press-center/press-releases/patient-survey-shows-unresolved-tension-over-health-data-privacy#:~:text=About%20three%20out%20of%20five,they%20are%20%E2%80%9Cextremely%E2%80%9D%20concerned.

The Case for Granular Consent

Mistrust in data exchange has significant implications for quality of care. Individuals who have concerns over whether their health information will be kept confidential may practice "privacy protective" behaviors, such as not seeking care, or not disclosing truthful or complete information about medical history or health-related behaviors, due to concerns about the privacy of their health information. Many patients are afraid, with good reason, that sharing certain information, such as behavioral health, genetic testing services, women's health, gender identity or substance use history, may increase the likelihood of bias within the patient-provider relationship, or that such information may be used against them if released outside of the clinical environment.[7] To build trust, individuals need flexible privacy and consent tools that allow them to control what information is shared, with whom, and under what circumstances. This flexibility can facilitate important actions, such as receiving an unbiased second opinion or getting a fresh start with a new provider.

For their part, providers that routinely provide care for sensitive conditions, such as mental health or substance use disorders, often believe that they cannot share any information or that it would be against the provider's and/or patient's interest to share, for example by exposing the provider or patient to adverse proceedings. For certain providers, the use of paper records is considered the most privacy protected.

One tool policymakers have deployed to help address these concerns is giving patients some greater control over access to, and disclosure of, their health information, as explained in more detail below. Even in the absence of legal requirements, healthcare organizations may voluntarily provide patients with greater control over some or all of their health information as a matter of organizational policy and procedure. Some jurisdictions have also identified certain categories of "sensitive" information that are subject to different consent requirements. Despite these legal definitions, individuals may have their own views on what information they do and do not want shared, depending on their circumstances. Patients may also want to know who has accessed their records or revoke a consent they have previously provided.

In surveys, patients have expressed an interest in having more "granular" controls over access to their health data, rather than being required to opt-in or opt-out of all health

[7] C. FitzGerald, S. Hurst, *Implicit bias in healthcare professionals: a systematic review*, BMC Medical Ethics, March 1, 2017. WJ. Hall, MV. Chapman, KM. Lee, et al., *Implicit racial/ethnic bias among health care professionals and its influence on health care outcomes: a systematic review*, Am J Public Health 2015, October 15, 2015. P. Nong, M. Raj, M. Creary, et al., *Patient-reported Experiences of Discrimination in the US Health Care System*, JAMA Network Open, December 15, 2020.

data access or exchange.[8] More granular control is particularly important for vulnerable populations who have higher levels of medical mistrust. In the current landscape, individuals who have sensitive personal information may conclude that they have no choice other than to opt-out of data sharing. Unfortunately, this means they will experience limited interoperability compared with their peers, even when they and their providers are connected through existing interoperability networks and frameworks, which may result in care inequities. In some instances, this decision is made algorithmically by organizations or health information technology (IT) vendors seeking to ensure compliance with federal or state law. Anecdotal evidence suggests that more data is withheld from exchange than necessary to address individuals' privacy preferences. This situation results from to the lack of technological and operational solutions in place to segment and differentially manage data that should or should not be transmitted, as well as the need to comply with data privacy laws.

Allowing individuals to consent to sharing their healthcare data at a granular level promises to result in greater data sharing and deliver the following benefits:

- **Respect for Individual Autonomy:** Greater control over what is shared empowers individuals to confidently share sensitive data to inform their own care.
- **Increased Access:** Enabling granular privacy and consent management allows patients to share more data than possible under "all or nothing" conditions. Increased data sharing increases the likelihood of improved health and care decisions.
- **Affordability and Lower Costs:** Improved interoperability reduces the need to order duplicative tests, exams, and medical procedures from multiple providers.
- **Improved, More Equitable Outcomes:** Limitations in interoperability have been shown to have deleterious outcomes, such as increasing the time to decision-making in emergency treatment.[9]

The inability for patients to specify sharing preferences, leading them to opt-out of sharing altogether, also contributes to medical mistrust, particularly among historically marginalized populations, which has been widely demonstrated to contribute to poorer health outcomes.

---

[8] H. Soni, MA. Grando, AC. Murcko et al., *Perceptions and Preferences About Granular Data Sharing and Privacy of Behavioral Health Patients,* Research Gate, August 2019, (PDF) Perceptions and preferences about granular data sharing and privacy of behavioral health patients.

[9] J. Zhang, H Ashrafian, B. Delaney, A. Darzi, *Impact of Primary to Secondary Care Data Sharing on Care Quality in NHS England Hospitals,* npj digital medicine, August 14, 2023, Impact of primary to secondary care data sharing on care quality in NHS England hospitals | npj Digital Medicine.

As discussed below, the ability to provide granular approaches to data sharing requires both data segmentation capabilities and a consent management structure. It will also require significant educational efforts of individuals and healthcare providers on how to understand and effectively use granular consent. Individuals also may need help from providers to identify the data to be shared for a specific purpose, such as a specialty consultation.

The Risks of Incomplete Information to Support Care Decisions

Healthcare providers and institutions are unfortunately accustomed to making decisions in the absence of complete information about their patients or the populations they serve. Clinicians want to provide the safest most effective care possible. When they are denied access to some or all clinical information, they will make do with the data they have, but missing patient health information may alter a provider's decision making and the course of treatment for a patient. Missing, outdated, or otherwise inaccurate health information can contribute to lower quality care and clinical outcomes, leading to inappropriate care or avoidable errors of omission or commission on the part of providers.

With the advent of electronic health records and their exchange through local, regional, and now nationwide interoperability networks, most providers have gained the ability to access and utilize more complete and accurate information to inform their care decisions.

When information is withheld for a valid purpose, such as honoring a patient's request, responding to legal requirements, or an otherwise valid exception, treating clinicians have concerns that they may be held responsible for adverse patient outcomes that could have been avoided if they had more complete access. From the clinicians' point of view, it's important to know if there is additional but inaccessible information. Platforms that alert providers that information is being withheld could satisfy this need. Clinicians could then make further inquiries to either discern the withheld information directly from the patient or their representatives or to potentially obtain consent to access information that would otherwise be withheld.

Ultimately, however, the balance between patient autonomy, privacy, and clinical decision-making is complex and context dependent. When faced with an urgent, critical need, some technical solutions exist to support "break the glass" functionality, whereby data requesters can access otherwise inaccessible data using specific methods that may involve documentation of a need to know and/or local collection of individual consent. However, traditional "break the glass" solutions are typically confined to a single system or organization, and address the need to bypass broad, often algorithmic, restrictions in certain clinical scenarios. The question of whether "break the glass" is appropriate if a

patient has proactively asked to limit sharing of specific data with certain actors is actively being considered by expert stakeholders in this space. Additionally, to enable broader access across systems, interoperability standards, including consent and privacy frameworks, are essential. However, the adoption of interoperable multi-tiered consent models remains limited, restricting their utility across healthcare settings.

3. Policy Challenges

This section summarizes the principal policy challenges to electronically sharing personally identifiable data used for health purposes from a regulatory compliance perspective—both those that provide privacy protections, such as the Health Insurance Portability and Accountability Act and its implementing regulations (collectively, HIPAA), and 42 USC 290dd-2 and its implementing regulations at 42 CFR Part 2 (collectively, "Part 2"); and those that promote the sharing of information, such as the Information Blocking Rule (see 42 USC 300jj-52 and its implementing regulations at 45 CFR Part 171). It does not address other complicating factors, such as state-based prescription drug monitoring programs or variable approaches to law enforcement access to information.

Laws and Policies Regarding Privacy and Consent

Today, there is no single, uniform data privacy protection and consent law that governs how personally identifiable data, including health data, can be used and disclosed. This lack of a common approach also extends to whether, when, and under what circumstances an individual's express, written authorization or consent is required for the use or disclosure of their information. Nor are there technical solutions available today that comprehensively identify regulated data and map that data to all the potentially applicable federal, state, tribal, or local requirements on the use or disclosure of such data—let alone consumer consent preferences—to ease the complexity of compliance for stakeholders. Rather, those who hold and want to share this data must contend with a patchwork of complex, non-computable, overlapping, and, at times, contradictory laws. Furthermore, these laws apply differently to different stakeholders depending on facts and circumstances that differ from case to case, and which may not align with an individual's actual privacy expectations or preferences. This complex web of rules leads to a reality where compliance concerns, rather than clinical considerations or patient preferences, drive business imperatives while still leaving data holders at risk for penalties for non-compliance.

It is a common misconception that HIPAA is the sole and final word on how health data may be used and disclosed. HIPAA merely provides a federal "floor" of requirements. It establishes minimum privacy protections (*e.g.*, use, disclosure and authorization requirements) for when protected health information (PHI)—a defined subset of health data—***may*** be used and disclosed by HIPAA-regulated entities (*i.e.*, HIPAA covered entities and business associates).[10] HIPAA does ***not*** preempt other federal, state, tribal or local laws that are ***more stringent*** than HIPAA,[11] and HIPAA has no application when the individuals and entities at issue are not HIPAA-regulated entities.[12] Thus, while it may be true that HIPAA permits the disclosure of PHI by HIPAA-regulated providers and health plans without an individual's HIPAA authorization for treatment, payment, and healthcare operations purposes (commonly referred to collectively as "TPO") under certain circumstances, that basic premise does not address the policy challenges posed by other federal, state, tribal, and local laws that are more stringent than HIPAA.[13] HIPAA requires a patient's authorization in any circumstance where the Privacy Rule does not otherwise require or permit a use or disclosure (for example, authorization is required for disclosures for marketing), and it can be challenging to identify and operationalize an applicable permission to use or disclose PHI in digital, networked environments.

To fully appreciate these policy challenges, it is necessary to first understand that the laws that govern the access, exchange and use of such data vary widely depending on four key factors: (1) who created, collected or otherwise gathered the data; (2) who will receive or access the data (taking into account the federal Information Blocking Rules, as described below); (3) for what purpose will the data be used or disclosed; and (4) whether the information constitutes a specially protected type of data. The following scenarios illustrate the variable impact of these factors.

1. ***Who created, collected or otherwise gathered the data***. For example, if a primary care provider (PCP) in California, who works for an outpatient clinic and electronically bills health plans, diagnoses a patient who resides in California with a substance use disorder (SUD), that SUD diagnosis is subject to HIPAA and the California Confidentiality of Medical Information Act (CMIA) with respect to how the PCP may use and disclose that patient's SUD diagnosis. (Notably, in this hypothetical, the PCP's SUD diagnosis is not subject to Part 2 because a PCP that works in a general medical facility and is not part of an identifiable SUD unit and whose primary function is not SUD diagnosis, treatment or referral for treatment,

[10] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996) and its implementing regulations found at 45 C.F.R. §§ Parts 160, 162 and 164, as amended from time to time.
[11] 45 C.F.R. § 160.203(b).
[12] 45 C.F.R. § 160.102.
[13]6 45 C.F.R. § 164.506.

is not considered a Part 2 program.) The PCP may generally use and disclose that SUD diagnosis without the patient's HIPAA or CMIA-compliant authorization for certain TPO purposes. However, that same SUD diagnosis maintained by the patient's Medication Assisted Treatment (MAT) provider who is cash pay only and doesn't engage in any HIPAA standard transactions, is not subject to HIPAA, but is most likely subject to Part 2 and may be subject to California's SUD law (Cal. Health & Safety Code § 11845.5). The MAT provider generally cannot disclose the patient's SUD diagnosis or MAT records for non-emergency TPO purposes without the patient's Part 2 and state-compliant consent. Moreover, the California-based, non-profit housing assistance program to whom the patient has voluntarily disclosed a SUD diagnosis, might be completely unregulated with respect to use and disclosure of that SUD data because non-profit entities are generally not regulated by the California Consumer Privacy Act (*see* Cal. Civ. Code § 1798.100 *et seq.*). Thus, ***who*** created or collected the SUD diagnosis may result in quite different outcomes for how that piece of information may be shared with others in a networked environment.

2. ***Who will receive or access the data***. If the PCP in the example above will be disclosing the PCP's SUD diagnosis to the MAT provider for treatment of the patient, HIPAA and the CMIA would permit the disclosure from the PCP to the MAT provider without the patient's authorization because HIPAA permits a HIPAA-regulated entity (like the PCP) to disclose PHI (like a SUD diagnosis) to another provider (like the MAT provider) for treatment purposes, even if that provider is not a HIPAA covered entity. (In this scenario, please keep in mind that the PCP is not a Part 2 program and the PCP's SUD diagnosis is not protected by Part 2.) But if the entity that will receive the PCP's SUD diagnosis from the PCP is not a healthcare provider, such as the housing assistance program, the PCP could only disclose the SUD diagnosis to the housing assistance program without the patient's authorization if the PCP determines that disclosure is necessary for the PCP's treatment of that patient. As it is not self-evident that disclosing a SUD diagnosis to a housing assistance program would be necessary for the patient's treatment, this is a case-by-case determination.

3. ***For what purposes will the data be used or disclosed***. As illustrated above, the purpose of the disclosure is equally as important as to whom the data will be disclosed. For example, no HIPAA or CMIA-compliant authorization would be required for the PCP (which is not a Part 2 program and not subject to Part 2) to disclose the SUD diagnosis to the housing assistance program if the PCP determines that the disclosure is necessary for the PCP's own treatment of the patient (*e.g.*, to coordinate or manage care between the provider and the

assistance program). However, if it is not necessary for this purpose, the patient's HIPAA and CMIA-compliant authorization would be required. Likewise, Part 2 might permit the MAT provider, which is a Part 2 program subject to Part 2, to disclose the SUD diagnosis to an emergency medical technician that arrives on the scene during a medical emergency in which the patient is unconscious, but not in non-emergency circumstances.

4. ***Whether the information constitutes a specially protected type of data***. Lastly, certain types of data (depending on who maintains it) are considered sensitive when subject to heightened privacy protections under certain federal, state, tribal, and local laws. For example, SUD information may be regulated more stringently under the federal Part 2 law and state health data laws. Many states also have sensitive health data laws that require specific authorization or consent for the disclosure of data regarding mental and behavioral health, reproductive health, HIV/AIDS, sexually transmitted diseases/infections, other communicable diseases, developmental or intellectual disability, neurological disease, genetic testing, and so on. Even HIPAA and Part 2 provide heightened restrictions on a subset of PHI defined as "Psychotherapy Notes" or "SUD Counseling Notes."[14]

When such laws apply and require an individual's authorization or consent to the use or disclosure of personally identifiable information, various procedural requirements may apply:

1. ***Type, form, and other requirements for the authorization or consent***. For example, when applicable, HIPAA and Part 2 both require ***written, signed*** authorization / consent from the individual and each have detailed, complex and ***different*** form requirements.[15] If the authorization / consent does not meet these requirements, the authorization / consent is invalid and any disclosure pursuant to the invalid form may constitute a violation of the law and a reportable breach. Some state and local laws may permit oral, implied, or constructive consents, whereas

[14] *See* 45 C.F.R. § 164.508(a)(2) and 42 C.F.R. § 2.11. HIPAA defines "Psychotherapy Notes" as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." 45 C.F.R. § 164.501. Part 2 defines "SUD Counseling Notes" as "notes recorded (in any medium) by a part 2 program provider who is a SUD or mental health professional documenting or analyzing the contents of conversation during a private SUD counseling session or a group, joint, or family SUD counseling session and that are separated from the rest of the patient's SUD and medical record. *SUD counseling notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." 45 C.F.R. § 2.11.

[15] *See* 45 C.F.R. § 164.508; 42 C.F.R. § 2.31.

others may require that the consent be in writing, signed, and specifically authorize the disclosure of the health data at issue. Many states also impose specific consent form requirements that can get as nuanced as requiring that a certain size font be used. For example, the CMIA requires that the authorization be handwritten or in typeface no smaller than 14-point type.[16] At a national level, this could mean that to share all a patient's health information in a networked environment, the technology and platforms must support authorizations and consents that meet ***hundreds*** of different requirements.

2. ***Who must sign the authorization or consent***. Who has the authority (control) over a patient's health data varies greatly when the patient is a minor or an adult who lacks capacity to make their own healthcare decisions. For example, under laws like HIPAA, Part 2, and state minor consent to treatment laws,[17] a minor may control the use and disclosure of a subset of their health data, such as the use or disclosure of the minor's SUD data, behavioral health data, or contraceptive data. In such instances, it may be necessary to get authorization from both the minor and the minor's personal representative to use and disclose the minor's full health data given that each party controls some (but not all) of the minor's health data.

3. ***Whether additional notices and downstream use and redisclosure restrictions apply***. Finally, whether an authorization or consent is required is not the only consideration for compliance with federal, state, tribal, and local laws. For example, traditionally 42 CFR Part 2 has required that when a MAT provider discloses the SUD diagnosis pursuant to the patient's Part 2-compliant consent, the MAT provider must also provide a notice about constraints on redisclosure of the Part 2 data by the recipient (depending on the status of the recipient and the type of consent given by the patient) and a copy of the consent (or clear explanation of the consent).[18] There are many state laws with similar requirements. For example, the CMIA requires that the disclosure of medical information pursuant to a CMIA-compliant authorization be accompanied by a communication about any limitations in the authorization.[19] Such laws also may impose downstream redisclosure restrictions on the recipients of such information.

Beyond the variability of data privacy protections and consent requirements, law also enables other types of individual choice. For example, HIPAA permits individuals to request restrictions on the use and disclosure of their PHI for treatment, payment, and

[16] Cal. Civ. Code § 56.11.
[17] *See, e.g.*, 45 C.F.R. § 164.502(g) and 42 C.F.R. § 2.14.
[18] 42 C.F.R. §2.32.
[19] Cal. Civ. Code § 56.14

healthcare operations. In some instances, HIPAA requires covered entities to grant those restrictions, such as when patients ask to restrict the disclosure to their health plan of PHI about health services for which they paid in full.[20] Federal and state laws may further permit such consumer choices by mandating that individuals have notice of, and the right to opt out of (or in to) ***how*** their health data is shared. For example, regulations may specify the right to opt out of having information transmitted through health information exchanges/networks (HIN/HIEs),[21] or a policy that individuals must opt in to such exchange, such as the recent CMS mandated Payer-to-Payer application programming interface (API) requirement for CMS-regulated payers.[22] As noted above, complying with individuals' preferences to keep certain information private is currently challenging both from a technical and operational perspective without the ability to segment data and share computable consent.

Additionally, some (but not all) data holders are also tasked with ensuring that health data is interoperable; that is, made available for access, exchange or use without special effort on behalf of persons who are legally authorized to have this access, as described in greater detail in the section below.[23] Often, this must be done in digital, networked environments where the data is not created, collected, or tagged to align with all of the complex privacy and interoperability requirements in mind. It can also be quite challenging in remote, networked environments to implement the necessary security measures and processes for making sure that a person who engages with a device and has the patient's identifiers is both who they say they are (*e.g.*, John Smith is John Smith or Dr. Evelyn Jones is Dr. Jones) ***and*** has the appropriate legal authority—whether as a provider, payer, public health authority, or the consumer/patient or their personal representative—to access and control the disclosure of the consumer/patient's health data.

As a result of these varying laws, health data that may be created and/or used and maintained by healthcare providers in one state may be regulated quite differently when compared to health data that is created and/or used and maintained by a provider in another state, or by a health plan, a public health authority, a direct-to-consumer health application, a social service agency, or a community-based organization, even if the health data at issue (such as a person's SUD diagnosis) is exactly the same. Moreover, in networked environments, entities may be maintaining the same piece of health data on behalf of multiple different stakeholders across multiple different jurisdictions. As a practical matter, they may then have to follow the most restrictive legal preconditions that

[20] 45 C.F.R. § 164.522.

[21] *See, e.g.*, A.R.S. § 36-3803.

[22] *See, e.g.*, 42 C.F.R. § 422.121(b)(2).

[23] *See, e.g.*, 42 U.S.C. § 300jj-52 and 45 C.F.R. § Part 171; CMS Interoperability and Patient Access Final Rule, 85 FR 25510 (May 1, 2020).

apply to either them or their participants—such as imposing specific authorization and consent requirements for all data they hold, even if only a small component or segment of the data is subject to the more restrictive law.

For more information on federal and state consent laws, see Appendix 1.

Laws and Policies Encouraging or Requiring Data Sharing

Providers and other entities holding valuable health data frequently face two seemingly contradictory policy imperatives: (1) they may be statutorily required or feel ethically compelled to provide patients with consent rights prior to using or sharing their health information; but (2) many are also required to actively share data for any purpose for which such sharing is permitted. For example, the 21st Century Cures Act's Information Blocking Rule creates an expectation that healthcare providers, health information exchanges/networks, and certified health IT vendors will share electronic health records for any legally permitted purpose. Similarly, CMS has established expectations regarding data sharing by CMS-regulated health plans. However, these laws do not override legal consent requirements. Navigating between consent laws and legal expectations to share data poses significant challenges to healthcare entities. Further, individuals surveyed also respond favorably to a desire to have their health information shared for purposes beneficial to them, adding a further thumb on the scale in favor of sharing or, at a minimum, not creating burdensome consent infrastructure that creates obstacles to sharing in circumstances where individuals reasonably expect that their information would be shared, such as for treatment.[24] The legal and/or ethical imperative to share in beneficial circumstances also may create challenges for deployment of technologies that automate consent expectations.

For a brief summary of federal and state laws and initiatives promoting or requiring information sharing, see Appendix 2.

4. Operational Challenges to Consent Management

This section identifies challenges to capturing and sharing individual consent to share information in a way that is compliant with the wide range of policies outlined above, illustrating how policy drives business requirements and imperatives. Tools to automate and reduce the burden of consent management will need to take these operational challenges into account. It does not address the very real and important challenges that

[24] L. Rainie and M. Duggan, *3. Scenario: Health Information, Convenience and Security,* Pew Research Center, January 14, 2016, https://www.pewresearch.org/internet/2016/01/14/scenario-health-information-convenience-and-security/.

come from applying patient preferences to the sharing of information, or other challenges to interoperability, such as patient matching.

When health records were largely kept, stored, and shared in paper form, and the entity with the record controlled the access, it was easier to try to share only those records that the patient was comfortable sharing (or that were legally authorized to be shared). It was also easier to withhold (omit, mask, or white-out) sensitive information, even when that sensitive information was commingled with information not deemed by the patient to be sensitive or covered by particular consent laws. Now that records are mostly electronic and data sharing increasingly occurs through queries of networks, complying with sensitive data privacy laws and accommodating granular patient preferences has become a greater challenge.

Information exchange also raises challenges from having patients' health information maintained at multiple levels (such as the original record holder, intermediary networks, and other locations where the record has been shared). Consequently, individual privacy preferences—whether granted by law or by organizational policy or discretion—may need to be communicated to, honored, and operationalized by both entities that originate a record and downstream recipients.

Sharing health information in a respectful and compliant manner can require gathering and sharing consent. However, given the complexity of the policy environment, those who provide care or facilitate sharing of health information face many operational considerations and challenges to consent management. Issues to consider include:

- Individuals' willingness to consent to sharing of their information;
- Providers' and payers' ability and willingness to share sensitive information with other care providers and health plans in a privacy-protecting manner;
- The need for flexibility to manage changes in regulatory requirements and individual privacy preferences;
- The ability to simplify and standardize explanations of consent to share information to accommodate varying levels of health literacy; and
- The availability of a technical infrastructure that supports consent management, which includes obtaining, sharing, consuming, storing, managing, and acting on the consent information.[25]

[25] https://stewardsofchange.org/wp-content/uploads/sites/2/2023/10/SOCI-HIMSS-Consent-Learning-Lab-Report-Executive-Summary-8.1.23.pdf

Consent management must also occur across many stakeholders involved in accessing or transmitting health information, including, among others: healthcare providers, payers, local health jurisdictions, patients, community-based organizations, researchers, and law enforcement. Each stakeholder group may face unique requirements regarding consent. Each may also have their own forms, tools, processes, and workflows, complicating the ability to share and act on consent. Within all of these groups, user training and adoption must be a key consideration, with particular attention being given to ensuring that individuals understand what they are consenting to, and the potential consequences of withholding data. Working collaboratively across sectors could address some of these issues.

Obtaining consent

Operational challenges to obtaining an individual's consent to share their health information, or for a patient to establish their consent preferences, are multifaceted, spanning literacy, regulatory, technological, and implementation issues. Provider organizations must craft consent materials that not only meet stringent regulatory requirements and mitigate organizational risks but are also easily understandable to individuals, ensuring full transparency. Ideally, individuals should also be able to review their consent to share preferences with a clinician to understand potential clinical impacts of not sharing or sharing. A prerequisite to consenting to sharing or not sharing data is an understanding of the way data is exchanged across the healthcare ecosystem, the complexities of which can pose further educational challenges. As noted above, divergent consent requirements across jurisdictions and organization types add burden and variations in format and signature requirements necessitate ongoing forms management.

Workflow

Integrating data-sharing consent into existing workflows presents significant operational challenges, particularly in terms of timing and process integration. One major issue is embedding consent procedures into stakeholder workflows without disrupting ongoing processes or adding to provider administrative burden. Organizations must also ensure that procedures to capture and act on the revocation of consent are robust, as they must guarantee that information is shared appropriately if consent is revoked or modified. In some cases, obtaining consent to share information is part of the initial process for receiving services, raising concerns that this process may not be given the attention that it deserves in the rush to timely deliver needed care. For instance, patients may not have sufficient time to fully understand the implications of their consent decisions during the

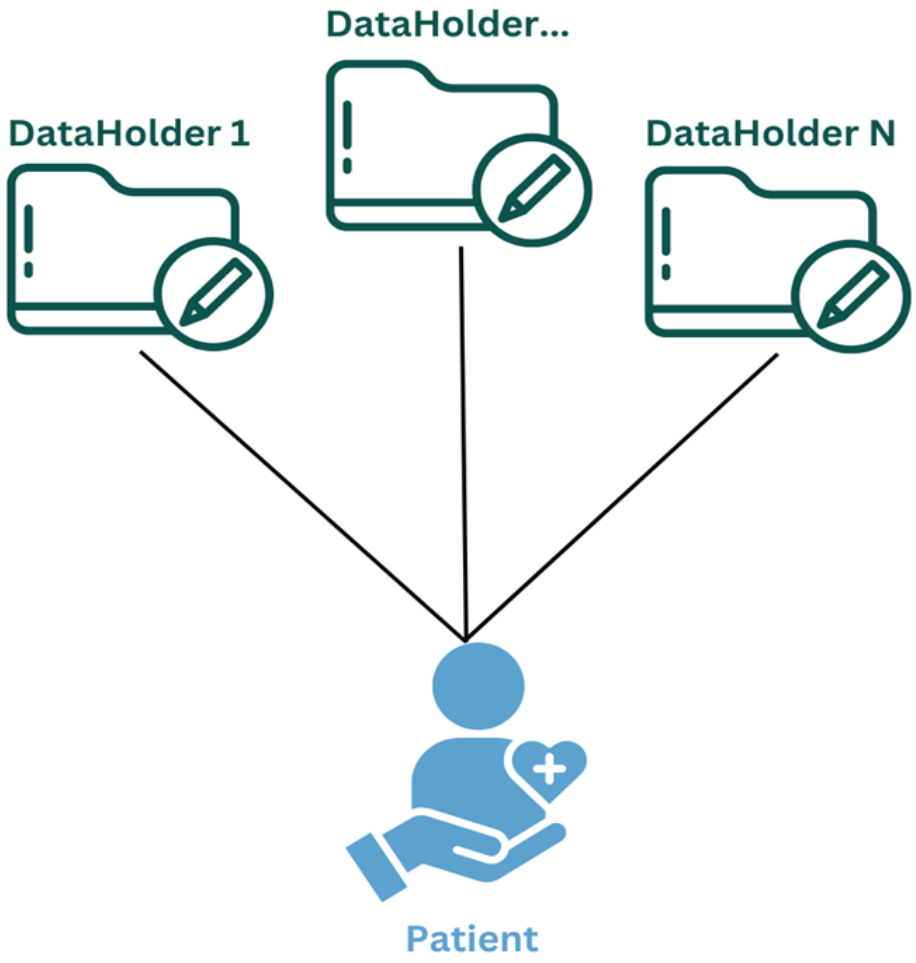
check-in process or be presented with tools that require additional steps (such as clicking on a link) to access a privacy policy. Distinguishing between different types of agreements and consents—such as consent to treat, consent for financial responsibility, and sometimes consent for participation in research or medical education, as well as consent to share information—adds another layer of complexity, requiring clear communications and efficient processes to ensure both compliance and patient understanding.

These workflow concerns can be exacerbated by resource differences. For example, a health system might contract with a release of information vendor for patients to electronically consent to or authorize the sharing of their information. However, if an individual has little-to-no internet service, or lacks a printer or a phone with a camera that can capture a photo ID, it is hard to provide a meaningful authorization. In addition, different communities may have populations with specific needs based on culture, language, varying education levels, internet availability, technical aptitude, and age-related challenges. This presents issues with creating consents and workflows that are accessible to all and understandable to the population.

Maintaining accuracy of the person's identity throughout the process of obtaining consent and responding to requests to share data poses another challenge. In particular, enabling any level of patient centric consent management requires patient identity/matching across data holders. Patient matching is critical to privacy and consent management to ensure entities can manage the complete, distributed patient record as efficiently and effectively as possible.

For example, a patient may have data sharing consent forms and rules with multiple data holders (Figure 1). Consistent management of these rules requires simple tools for the patient to manage these holistically, while enabling a data holder to have access to all applicable consents and rules that they must honor. This requires matching patient identities across data holders, awareness of the existence of the patient's consent forms and rules repositories whether in one central place or distributed, and access to consent information in a computable format. The necessary technical components and infrastructure are in design and early development stages but are not yet widely available.

Figure 1.



Resources

Ideally, organizations will have sufficient resources to implement processes to capture and manage consents through an ongoing program with staff training, oversight, accountability, and quality management. However, keeping up with consent requirements can be especially challenging for small organizations, those with limited resources, and those operating in multiple jurisdictions. Employing or contracting adequate health information, legal, technical, and other expertise may not be possible for all organizations. Even when experts are consulted to provide implementation guidance or support, the daily maintenance of forms, version control, tracking, access, delivery, and customer service impose burdens. Furthermore, even when a satisfactory program exists for request of the most common data sets, the handling of exceptions (*e.g.*, data sharing

consent related to minors/adolescents, Part 2 data, genetic data, etc.) creates additional difficulties. Implementing processes to manage these situations poses challenges such as providing alternative consent methods, implementing emergency overrides, and maintaining audit trails to ensure compliance and accountability.

The challenge of compliance with changing regulations and guidance over time can lead to inaccurate actions being taken or the wrong information being relayed to the requestor. This confusion may also lead to withholding information entirely. Two common examples include:

- Staff incorrectly interpreting Part 2 requirements as applying to all behavioral health or SUD-related data, rather than a specific SUD treatment subset, and therefore concluding they can't share anything without consent. However, it bears noting here that due to data segmentation infeasibility (*e.g.*, where it is impracticable to distinguish the Part 2 data from non-Part 2 data), staff may have to apply Part 2's protections over all their data to ensure compliance with Part 2 for the protected SUDs data.
- Staff incorrectly interpreting HIPAA as requiring authorization for ALL disclosures, even those for which HIPAA does not require authorization, such as to the patient or to another healthcare provider or health plan for continuity of care.

Consent management tools that support data holders in navigating these operational issues could both improve the ability to honor individual privacy preferences and reduce burden. Technologies that provide electronic consent enforcement could further streamline processes by eliminating the need for staff to interpret complex regulations.

5. Technology Challenges to Consent Management

Policy requirements have driven the implementation of consent management and the respective technical specifications for decades. This section reviews the standards and technology approaches that have emerged to support electronic consent management, as well as additional issues that arise in bringing these tools into widespread use.

Consent and the Degree of Choice

While the technical requirements of consent are as nuanced and detailed as the laws and policies that govern them, such requirements can broadly be considered as existing along a spectrum depending on the degree of patient choice and specificity of the consent. At

the most basic or simplified end, consent is binary; at the most specified or detailed end, consent is granular.

Binary consent, where patient choice is minimized, is considered a relatively simpler solution for implementation in data exchange and is generally implemented in one of two ways. In opt-out models, a patient's data is accessed, released, or exchanged by default unless a patient takes action to withdraw. Conversely, in opt-in models, a patient's data is accessed, released, or exchanged only with affirmative consent. Under either approach, binary consent is all or nothing, meaning that the full record is either withheld or shared in its entirety.

However, there is an additional nuance of this binary technical implementation worth noting. In states such as New York, regulations require that patient data be released to the statewide health information network regardless of patient consent. However, a patient must "opt-in" for their data to be accessed by their provider at the point of care.

In other cases, health information may be shared with, and maintained and used by, an intermediary, like an HIE/HIN that functions as a HIPAA business associate or Part 2 qualified service organization, but that intermediary may not re-disclose/release that information to third parties through its health information exchange services without the patient's further opt in (or may not share a patient's information with third parties through such HIE/HIN services if the patient has opted out).

Granular consent, where patients have a relatively higher degree of involvement and associated control of their data, requires a more complex solution for implementation in data exchange. While the individual choice(s) can still be considered binary as to whether their health information may be exchanged through an HIE/HIN in the first instance (opt-in or opt-out), what increases is the number of choices and complexity of exchange, such as opting in or out of who gets their information (*e.g.*, "yes" to Dr. Jones, but "no" to Dr. Smith), what information is shared (*e.g.*, "no" to behavioral health information), or for what purposes (*e.g.*, "yes" for treatment but no for research). Depending on the particular requirements or technical maturity, granular consent exists when patients have the ability to provide or deny consent for specific exchange purposes, to the release of particular data types, or for access by individual providers.

Implementation of Binary Consent

Automation of binary consent, or individuals' decisions to globally opt in or opt out of data sharing, has had some success. Historically, consents were collected using paper forms

that were then manually entered into electronic systems maintained by the data holder (such as healthcare providers, insurers, or clearing houses). These systems could then enable automated actions consistent with the binary consent (share or withhold the entire record) but typically could not share the consent document itself.

One of the early efforts to create an automated tool that could share a consent document across systems was the Integrating the Healthcare Enterprise (IHE®) Basic Patient Privacy Consents (BPPC). This specification paved the way for exchanging a digital representation of the consent between partners in a network, using the IHE Technical Framework (Profiles). This approach treats consents as opaque documents (similar to a pdf), often with binary semantics ("opt in" or "opt out") but with standard metadata that makes it possible to search for, retrieve, and share the consent. This means that a data requester can digitally confirm that it has an individual's consent to ask for a record in a machine-readable form, without having to send a copy of the consent itself via mail or fax.

The use of IHE standards for consent management effectively allows for sharing of consent, but also comes with some limitations. The IHE defined technical transactions ITI-55, ITI-38, and ITI-39 (i.e., patient discovery, document query, and document retrieval) do not allow for granular consent requirements and customization of response to a query. In this model, healthcare organizations and other data holders sharing a consent must first agree upon the content needed, collection method, and data use agreements covered by the consent documents made available by these transactions. With each new consent requirement, the parties to exchange must establish new agreements to align the consent form's content, collection, and scope of disclosure covered. The multiplicity of requirements present scalability issues for adopting this as a nationwide standard. They have, however, been used successfully for some use cases, including by the Social Security Administration (see case example on page 29).

While a breakthrough in electronically sharing consent documents, these initial IHE standards are not well equipped to handle granular consent requirements that differ based on patient preferences, exchange purposes, state and local regulations, and criteria specific to certain types of patient populations or clinical data. However, IHE has also created the Advanced Patient Privacy Consents (APPC) specification, that supports a more granular view of the rules expressed in the consent. Although IHE APPC has not been widely adopted, the ideas from this specification became one of the inputs to the emerging IHE Privacy Consent on FHIR (PCF) specifications discussed below.

Implementation of Granular Consent

The Health Level Seven® (HL7®) Fast Healthcare Interoperability Resource (FHIR®) standard allows data holders to share specific information through granular "resources" rather than an entire record. It also encodes the data using vocabulary standards that allow different data systems to "speak the same language." This flexibility, combined with the use of application programming interfaces (APIs) that support access to and exchange of granular data, allow for the development of automated approaches to granular consent.

In contrast, another HL7 standard, the Clinical Document Architecture (CDA®), organizes health data into full clinical documents, such as discharge summaries or encounter reports, making it less suited to granular data sharing or consent management than FHIR resource-based model.

Specifically, the HL7 FHIR Consent Resource was a major step forward in enabling granular consents that include policy rules about what information to share, and under what circumstances in machine-readable form, bringing forth the concept of a "computable consent" that can be adjudicated and enforced automatically. There have been various proof-of-concept implementations and demonstrations for computable consents, including the ASTP/ONC LEAP Consent project. The emerging IHE Privacy Consent on FHIR (PCF) specifications further this effort by specifying profiles of the FHIR Consent resource and defining a maturity model ranging from *basic* to *advanced* consents with more sophisticated rules that depend on data tagging/labeling. An advanced consent may encode an individual's preferences based on the type of sensitive data and deny access to any data labeled as being related to that category. Challenges to this approach include the need to label each record in the system, including historical data and decide how to handle unlabeled data.

As part of the FHIR core specification, the FHIR Consent resource also comes with a standard API for creating, retrieving, searching, and updating consents that are maintained in a given system. This basic API provides the essential ingredients of consent management operations to simplify and automate some of the operational challenges noted above.

However, the higher-level business operations of consent management need further implementation guidance to successfully automate the process of collecting, acting on, and sharing individuals' privacy preferences. This includes processes such as: (1) inviting an individual to provide consent; (2) consent form review and navigation; (3) signing and

enacting a consent; (4) reviewing existing consents; (5) consent revocation; (6) consent provenance; and (7) delegation of the consent. Some of these functions have been covered by the IHE PCF standard, but a new implementation guide that is being developed by the FHIR at Scale Taskforce (FAST) specifically targets these consent management capabilities.

FAST also intends to provide technical guidance on implementing the infrastructure for disseminating the lifecycle events of consents, including creation of a new consent and revocation, to an ecosystem of partners where consent enforcement may take place. This ensures that participants can outsource consent management operations to a third-party entity and rely on the API and notification for integrating consent enforcement into their workflows.

While significant progress has been made, the consent standards will need to be further developed, broadly adopted, and supported by changes in policies and operational processes by individual healthcare organizations before granular consent can be widely implemented and available.

Data Segmentation for Privacy

Another complementary approach to granular control of data is Data Segmentation for Privacy (DS4P). DS4P is defined as the process of breaking data into elements (or segments) to identify those elements that need additional restriction, often via tagging and the inclusion of metadata. There are four components of a DS4P solution:

- Policies, rules, specifications, and the technology to determine tags through a Security Labeling Service (SLS);
- Specifications for how to represent different types of sensitive information using standardized tags;
- Specifications for how to record these tags on different types of data structures and formats including granular tagging of sections/portions of the data; and
- Policies, rules, and technology for how to receive, interpret, and process tagged data.

Currently, there are standard specifications and implementation guidance on how to record tags (or Security Labels) through a range of information sharing standards, including HL7 v2 messages, HL7 CDA® documents and specified entries within documents, and HL7 FHIR resources. The HL7 FHIR DS4P Implementation Guide (IG) provides an additional mechanism for tagging more granular FHIR elements, as well as recording labeling metadata. This IG also provides implementation guidance for building

an SLS, although standardization of interfaces for interacting with such a service remains a work in progress. The HL7 Security Workgroup is currently preparing to update this specification to provide additional guidance on implementation and update the value sets.

ASTP/ONC certification regulations support, but do not require, adoption of more granular use of standards-based data tagging by healthcare providers. Specifically, the agency has voluntary certification criteria that demonstrate the ability and use of health IT to support security tagging at the document, section, and data element levels of a C-CDA®, using the relevant HL7 standards.[26] As of January 2025, close to 40 products listed on the agency's Certified Health IT Products List had been certified to these criteria.[27]

HL7 terminology provides initial value sets for recording the tags for different sensitivity classes (such as behavioral health, substance use treatment, and sexual health) as well as confidentiality levels (such as restricted, very restricted, and normal confidentiality). The HL7 FHIR DS4P Implementation Guide also provides a placeholder and value sets for these codes. However, further guidance is needed on the clinical value sets that would inform the labeling of common classes of sensitive data such as behavioral health that are covered by consent or restriction mandates, or that some providers would find valuable to have the ability to withhold from sharing in some circumstances due to patient preferences. Computable consent will require broad agreement on standard value sets and sensitivity flags.

Implementation Experience and Challenges

Pilots of the DS4P standards and consent management platforms suggest they are useful tools. However, widespread adoption of tools to enable granular data segmentation and consent management in support of individual privacy preferences remains elusive.

Pilots have generally been narrowly focused on consent to share substance abuse disorder treatment data restricted by Part 2 and other narrow use cases. Given current policy developments, consent to share sensitive reproductive healthcare data and behavioral health data has recently been prioritized as well. Collaborative efforts, led by the Shift Task Force in conjunction with industry stakeholders such as the Gravity Project and OpenNotes, have developed additional high-value clinical use cases.

In addition, previous pilots have not always fully deployed available technology. For instance, in one pilot, the organization chose to adopt an "all or nothing" approach to

[26] C.F.R. § 170.315(b)(7) and § 170.315(b)(8).
[27] Certified Health IT Product List, https://chpl.healthit.gov/.

sharing records, even though the technology allowed for redaction of data in a particular category based on a patient-specified privacy policy.[28] The DS4P FHIR IG and the Privacy Consent on FHIR (PCF) IHE profile now allow for more granular data tagging, but need to be further tested through reference implementations.

Key Factors for Success

To accomplish widespread adoption of DS4P and related consent management standards, four key factors need to be addressed:

1. ***Standardized terminology value sets to define categories of sensitive data.*** Although the Substance Abuse and Mental Health Service (SAMHSA) developed a Consent2Share (C2S) Value Set Authority Center (VSAC) sensitive condition value set to support data segmentation, it has not been maintained over time. Further, this value set focuses mostly on substance use disorder and behavioral health and is not comprehensive for other potentially sensitive conditions. Organizations such as the Shift Task Force and the National Association of Community Health Centers (NACHC) are working together to develop, disseminate, and maintain such publicly available value sets.

2. ***Implementation guidance and support.*** Stakeholders involved in one pilot noted organizational push-back due to the complexity of implementation. The following questions underscore where stakeholder consensus and policy guidance may be needed.
    a. How should competent patients be informed that withholding data from treating clinicians and other caregivers brings risks or that data may not be withheld in all circumstances given the complexity of IT systems?
    b. What approaches to automation (such as artificial intelligence/machine learning or natural language processing) might be deployed to minimize implementation burden?
    c. How can the privacy tags (or security labels) deployed in one system be recognized and acted on in a consistent manner across vendor platforms?
    d. Should a receiving system notify end-users, such as a primary care physician, that a record has been redacted, and if so, how? Are there ways to enable the end-user (such as a primary care physician or an emergency

[28] *Protecting high stakes PHI: DS4P healthcare standards enhance the privacy of sensitive data*, *in* Journal of AHIMA 85, no. 4 (April 2014): 30-34. J. Coleman, *Segmenting Data Privacy: Cross-industry Initiative Aims to Piece Out Privacy Within the Health Record*, *in* Journal of AHIMA 84, no.2 (February 2013): 34-38. G. Linden, *Minnesota OCP-C2S Project*, ONC Annual Meeting 01/2020. J. Stefano, *C2S Real World Implementation*, ONC Annual Meeting, 01/2020.

department clinician) to access the redacted information with appropriate consent or in an emergency?

e. How can systems enable the withholding of data related to sensitive data that an individual has requested be withheld? For example, if an individual does not want to share a sexually transmitted disease diagnosis, should related lab results, medications and allergies also be withheld? Sensitive diagnoses may also be referenced in other parts of a medical record, such as the medical, surgical, or sexual health history, as well as in free text documentation, making it challenging, if not impossible, to completely mask the existence of the information.

3. ***Standardized rules that can be computable.*** Even as value sets are being developed, computable privacy and consent rules are not yet widely available. Without well-defined, computable rules that align with the complex web of policies described above, a nationally scalable infrastructure that can enable data holders to manage privacy consistently is not feasible. Furthermore, these rules will need to be incorporated into both HL7 standards-based data exchange (whether traditional messages, documents, or emerging resource-based exchange) and any other data exchange involving sensitive data.

4. ***Incentives for adoption.*** Under current policies, DS4P is an optional standard with limited uptake due to the cost of development and the challenges to implementation noted above. Even if the standard matures and the related terminologies and implementation guidance are developed, adoption may not happen without a policy or financial incentive.

Recent state-level policies underscore the need to address these issues. For example, the State of Maryland enacted a law requiring HIEs to block the interstate exchange of procedure codes associated with certain types of sensitive information.[29] In addition, California enacted a law (AB 352) requiring EHR developers, certain digital health companies, and certain other businesses that electronically store or maintain Californian's sensitive medical information to enable:

- Limitations on user access privileges to information systems that contain medical information related to gender affirming care, abortion, abortion-related services and contraception only to those persons who are authorized to access the medical information;

[29] Maryland House Bill 812, *Health – Reproductive Health Services – Protected Information and Insurance Requirements,* https://legiscan.com/MD/text/HB812/2023.

- Prevention of the disclosure, access, transfer, transmission or processing of such information to any person or entity outside of California;
- Segregation of medical information related to gender affirming care, abortion, abortion-related services and contraception from the rest of a patient's medical record; and ability to automatically disable access to segregated medical information by individuals and entities in another state.[30]

It will be critical to monitor the implementation experience of these states for EHR developers and healthcare providers, and any others that pass similar laws, to inform future efforts.

Automation with Human Review of Consent

Most interoperability today is performed in a synchronous, automated manner that does not allow human review of the patient's consent to release electronic health information. This means that, in some cases, systems have moved directly from manual release of information processes, in which a person would examine the consent to ensure that it is complete and correct before sharing information, to automated query and response methods of exchange. Such processes could result in inappropriate sharing in cases where consent is required.

The "Deferred Patient Discovery" specification, however, operates asynchronously by building upon the IHE Cross Gateway Patient Discovery (XCPD) transaction (ITI-55) to introduce an advanced mechanism for handling patient discovery requests. This deferred processing mechanism allows for decoupling a data request from immediate processing, offering flexibility in scenarios where the responding system may not be able to process the request instantaneously due to load balancing, system maintenance, or other operational constraints. This allows organizations the opportunity to not only pause and review the consent, but also properly confirm the patient matching results.

Deferred Processing Mechanism

The deferred mode enables systems to queue patient discovery requests and process them at a later time, which is particularly useful for environments with fluctuating workloads and for workflows which require human review of the consent based on policy requirements. The actual timing of when the request is processed is not dictated by this

[30] DF. Gottlieb and R. Bank, *California's New Reproductive Privacy Laws AB 352 and AB 254 Create Complexities for Health Information Sharing,* November 17, 2023, https://www.mwe.com/insights/californias-new-reproductive-privacy-laws-ab-352-and-ab-254-create-complexities-for-health-information-sharing/.

specification, allowing participants in the transaction to define timing and priorities through business-level agreements (such as service level agreements or policies). Support for this feature is currently limited, and its implementation may require careful coordination.

Message Exchange Pattern

In the immediate processing mode, a standard single two-way message exchange is used (request-response). The deferred mode introduces a more complex interaction, requiring a two-step, two-way message exchange:

1. The initiating system sends a patient discovery request, and the responding system acknowledges receipt but does not provide an immediate response to the request.
2. Once the request is processed, the responding system sends the final result back to the initiating system in a separate message. This two-step process allows for asynchronous communication, separating the request initiation from the actual delivery of the response.

This deferred processing mechanism is ideal for large-scale health information exchange where patient discovery requests across systems may face delays due to differences in system availability or performance and provides the capability for human review of the consent when needed. Deferred processing may be a barrier to immediate data access when this is needed to support acute clinical care. In addition, healthcare organizations that implement these types of mechanisms will need to ensure that they consider all of the regulations that apply to them, including the Information Blocking Rule.

Case Example: Social Security Administration Use of IHE Transactions for Supporting Consent Management

Organizations in the healthcare community use the IHE standards ITI-55, ITI-38, and ITI-39 to exchange clinical documents. Similarly, industry standards are available for managing and exchanging patient consent forms (*e.g.*, IHE BPPC). In this model, the Querying Organization and Responding Organization use the standards to identify the presence of a consent form as part of establishing a shared patient and are able to exchange those consent forms. The Social Security Administration (SSA) uses these standards for exchanging consent forms to support their Disability Determination Program.

For patients seeking Disability Benefits, the SSA initiates an ITI-55 Cross Gateway Patient Discovery Query to a healthcare organization where a patient received care. In addition to the patient demographic elements used to identify a shared patient, the SSA includes an Access Policy Identifier in the SAML token. The healthcare organization may initiate an ITI-38 Cross

Gateway Query to the SSA using this Access Policy Identifier to retrieve consent forms signed by the patient. The SSA responds to this query with the available consent documents signed by the patient. The healthcare organization may then initiate an ITI-39 Cross Gateway Retrieve transaction to download the signed patient consent form.

The workflow described above is widely used today to electronically verify the presence of a consent form for patients seeking Social Security Disability Benefits. Previously, healthcare systems exchanged these consent forms with the SSA by mail and fax. Today, the SSA has implemented electronic industry standards with over 250 healthcare organizations representing over 41,000 providers.

Vendor Specific Approaches

Given the challenges to standardized approaches to data segmentation and consent management laid out above, health systems commonly rely on a vendor-specific approach to consent management provided by their existing EHR vendor or other technology partners.

Vendor-specific solutions can offer additional features. Organizations have established business relationships and familiarity with their EHR vendors. Similarly, organizations with a specific vendor's technology in place typically turn to these vendors to implement new features or change system configurations. These reduce the burden on the local health system but do not promote alignment with other organizations that use a different blend of health IT vendors and systems, or may have configured the same vendor's system differently. Below is one example of a vendor-specific approach.[31]

Approaches to consent management through Epic

Health systems and other providers that use Epic agree to the Care Everywhere Rules of the Road prior to participating in community-wide exchange for Treatment. These rules establish principles of trust for Treatment-based exchange, including:

- Universal reciprocity between participants: all organizations must share with one another.
- Consent requirements are determined by the disclosing organization.
- Consent requirements must be fulfilled prior to disclosures by an organization.
- Disclosing organizations may request a copy of any consent form authorizing a disclosure.

[31] The Workgroup requested, but did not receive, any additional descriptions from any other vendor systems.

- An elected community-led Governing Council meets to enforce and update these rules, as well as resolve disagreements within the community.

Adopted in 2008,[32] Epic customers have seen exchange increase significantly under the Rules of the Road. As of December 2024, the Epic community exchanges over 20 million patient charts[33] each day, with half of those exchanges occurring with organizations using other EHR vendors through Epic community's participation in the Carequality, eHealth Exchange, regional HIEs, and federal agencies such as the VA, SSA, and US Department of Defense (DoD).

Providers that use Epic determine their own policies on when consent is needed and what information a consent must contain, based on the privacy laws that apply to them and other considerations. This allows them to flexibly manage consent requirements to account for differences in patient population, local policy, state laws, and business agreements, as necessary. These consent requirements are often determined by characteristics of the care the patient received from a given organization. Examples include substance use disorder treatment services protected by Part 2, mental/behavioral health treatment, genetic testing services, gender affirming care, and pediatric care to the extent such care is subject to additional state privacy requirements.

For example, for patients with characteristics that would require the patient's written consent before disclosing the record to another provider for Treatment, providers that use Epic can create consent forms specific to their own organization, tailoring the content to meet relevant regulatory requirements for the specific exchange. Epic-using organizations distribute their consent form templates to all other Epic organizations that have agreed to the Care Everywhere Rules of the Road. Additionally, each organization specifies the methods by which their patients may sign consent, including prospectively at the organization, electronically via the organization's patient portal, or embedded at the point of care at another provider organization that uses Epic. Importantly, the patient's consent is obtained using the forms and policies required by the organization releasing the patient's record.

Epic's approach relies on three technical elements that allow organizations to operationalize consent management. First, consent requirements are checked and communicated to the data requestor as part of each transaction. Second, each organization's consent forms are shared and distributed with all other organizations in the

[32] *Care Everywhere,* HIMSS, https://www.himss.org/resource-environmental-scan/care-everywhere.
[33] Epic, https://www.epic.com/software/interoperability/.

Epic community. Finally, patients can be presented with the disclosing organization's consent form when they receive care at other organizations.

However, this model has certain limitations. For example, Epic does not provide a centralized consent management platform that is designed to automate the consent forms used by its provider organizations, or to support consent revocation or expiration. Additionally, this model does not support healthcare organizations that do not use Epic health IT systems. For instance, when patients seek care from organizations using non-Epic health IT systems, when those health systems connect with Epic customers via FHIR APIs or IHE transactions today, they may see "Patient not Found" if a consent requirement applies, instead of a more accurate code denoting the need for a consent computable with Epic's model. This increased consent burden may be a barrier to providing care.

6. Exploring Existing Consent Models and Frameworks

In 2024, Sequoia's Privacy & Consent Workgroup engaged with a diverse range of states, organizations, and leading SMEs to advance the implementation of consent management solutions. By fostering dialogue among stakeholders, the workgroup is working to identify best practices and seek solutions that prioritize patient preference and data privacy.

Several initiatives are tackling consent management in innovative ways. The Shift Task Force is engaging industry stakeholders to develop granular data segmentation standards and implementation guidance that support patient-driven sharing of health information through informed consent. This includes identifying informed consent use cases across various platforms and demonstrating effective data redaction and partial record sharing. While challenges remain in defining sensitive information and establishing standardized value sets for categories like behavioral and reproductive health, the Shift Task Force is underscoring the need for extensive testing and implementation. Stewards of Change Institute (SOCI) has recently led Consent Workshops, co-sponsored with HIMSS Government Affairs, resulting in the concept of a Consent Service Utility (CSU) which addresses many of the legal and regulatory issues through the idea of National and Community-level Consent Catalogs where both existing as well as new linguistically and legally vetted and computable consent-to-share documents can be found. The CSU's technical architecture builds off the LEAP Consent Decision Service (LEAP-CDS) work for the further implementation of Management (consent execution and storage), Discovery (consent and record retrieval), and Decision Services (application of consent rules to applicable documents prior to transmission) across systems. The FAST Initiative has produced a FHIR Consent Resource Implementation Guide to support various consent models, despite facing challenges related to technology and state privacy

regulations. The HL7 Data Segmentation for Privacy (DS4P) standard seeks to improve data segmentation for consent, requiring industry consensus on its application while incorporating security labeling into authorization and consent management processes, as discussed above.

At the state level, the New York eHealth Collaborative (NYeC), in partnership with the New York State Department of Health, is shifting from an opt-in consent model to a statewide community consent framework. Meanwhile, the New Jersey Innovation Institute (NJII) is implementing an electronic consent management solution to allow for the transmission of Part 2 data to providers, consented to by patients. In Maryland, the Chesapeake Regional Information System for Our Patients (CRISP) is developing code-based systems for parsing and filtering data in response to new legislation, allowing affirmative patient consent for disclosure. The San Diego Community Information Exchange (CIE) is exploring universal consent for social determinants of health data and collaborated with California Advancing and Innovating Medi-Cal (CalAIM) on the Authorization To Share Confidential Medi-Cal Information (ASCMI) Pilot, aimed to facilitate exchange of data needed to implement programs that require obtaining members' sensitive data, as mandated by state and federal law. In Washington state, the Washington State Health Care Authority (HCA) has launched an Electronic Consent Management (ECM) solution to enhance the exchange of sensitive data to improve care coordination and reduce the administrative burden associated with managing consent.

Together, these initiatives highlight a complex landscape of consent management efforts across states, each addressing distinct regulatory and operational challenges. Appendix 3 contains a table of the organizations and states that presented to the workgroup, further highlighting their current initiatives and the challenges faced with their respective approaches. For a complete list of links and additional resources, please refer to Appendix 4.

7. Conclusion

While health information exchange is growing and individuals increasingly seek electronic access to their health information to enhance care, persistent privacy concerns must be thoughtfully addressed to build trust in these systems, particularly for those with highly sensitive health information.

While healthcare organizations want to honor individual privacy practices, they are challenged by the wide and increasing array of varying federal, state, and local laws that create uncertainty about when patient authorization or consent should be collected and

how to act on it. In addition, information gaps may occur when highly sensitive health information is withheld, raising concerns about whether and how providers are made aware that information is missing and how it may be possible to access such information in an emergency.

The absence of a uniform national data privacy law and the complexity of overlapping regulations create significant challenges for stakeholders, resulting in defensive compliance-driven decisions that often overshadow clinical considerations and patient preferences. Today, organizations are implementing local consent management solutions based on the policies of the states in which they operate and the relationships they maintain with state entities, including state health departments and health information exchanges (HIEs). While these policies influence business practices for consent management, they frequently fail to address the broader challenges of aligning with individual preferences and achieving effective interoperability.

Healthcare organizations currently lack adequate technical solutions and implementation guidance to support gathering and acting on consent documents and patient privacy preferences. While IHE standards for consent management offer a foundational framework, their limitations in flexibility and granularity create significant challenges for widespread adoption in diverse healthcare environments. This complexity is compounded by data management issues, including inconsistencies in data formats that affect accessibility.

More collaborative work is needed to improve, test, and build operational tools for consent management. That work should be multi-modal, including further understanding of the feasibility and impact of data segmentation that enables healthcare organizations to honor individual's privacy preferences at a more granular level. Additionally, policy work should be directed towards addressing the growing complexity of regulations that could significantly hamper the sharing of information, as healthcare organizations feel compelled for compliance reasons to share "none" because they cannot share "all" of the data in a record.

Call to Action

Privacy and consent is a complex issue, particularly in healthcare, with many organizations working piecemeal on technical, operational, and policy approaches. The Privacy and Consent Workgroup will continue its critical mission. The Sequoia Project also wants to hear from interested organizations to consider forming a broad coalition to collaboratively move forward with the implementation of real-world computable consent

approaches. As seen in this landscape review, there are many stakeholders with many approaches. To be successful, everyone will need to collaborate and coordinate efforts to tackle specific implementation issues and advance the use of standards-based consent management and data segmentation for privacy. The goal is for information exchange to occur in ways that are both compliant with privacy rules and respect individuals' privacy preferences.

Topics to be addressed include:

- Guidance on organizational-level policies and workflows to improve consent management, including consideration of break the glass functionality.
- Community engagement for standardizing consent approaches (opt-in/out, granular consent, etc.).
- Community engagement on technical standards for data segmentation and consent.
- Accessing and exchanging and using standardized consent across organizations
- Consideration of how best to deploy and utilize data segmentation capability in health IT.
- Other outstanding issues to be noted.

Working together, stakeholders can identify concrete ways to improve and standardize consent management and address privacy concerns on the frontlines of healthcare. Providers, patients, and their caregivers, are depending on us to progress granular and computable consent capabilities.

For further information or to join with The Sequoia Project in future efforts, please contact InteropMatters@SequoiaProject.org.

Appendix 1: Federal and State Privacy and Consent Policy Landscape

This Appendix presents a non-exhaustive list of federal and state laws (as well as recent changes or proposed changes to those laws) that stakeholders should consider when embarking on efforts to exchange health data in digital and networked environments across multiple jurisdictions and involving a variety of differently regulated and unregulated stakeholders.[34]

Federal Privacy & Consent Policies

- **HIPAA**. HIPAA regulates protected health information (PHI) maintained by or on behalf of HIPAA covered entities or business associates. Collectively, this refers to healthcare providers that engage in HIPAA standard transactions (such as electronically billing health plans), health plans, clearinghouses, and those individuals and entities that assist them in performing their HIPAA-covered functions and who need to have access to PHI in order to perform those functions.[35] HIPAA provides heightened protections for psychotherapy notes[36] and requires that HIPAA-regulated entities honor a patient's request to not share PHI that pertains solely to self-paid healthcare items or services with a patient's health plan.[37] It also generally requires a HIPAA authorization for the use and disclosure of PHI, unless an exception applies (such as the exception for sharing information related to treatment, payment, or healthcare operations, or TPO).[38] Under the HHS Reproductive Health Final Rule,[39] HIPAA further prohibits the use and disclosure of PHI to conduct investigations or impose liability on persons for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive healthcare,[40] and requires that HIPAA-regulated entities receive attestations before disclosing PHI that is potentially related to reproductive healthcare in response to requests for health oversight activities, judicial and administrative proceedings, law enforcement purposes, or to coroners and medical examiners.[41]

[34] Special thanks to Velatura HIE Corporation for contributing this content.
[35] *See, e.g.*, 45 C.F.R. § 164.500.
[36] 45 C.F.R. § 164.508(a)(2).
[37] 45 C.F.R. § 164.522(a)(1)(vi)(B).
[38] 45 C.F.R. § 164.506.
[39] 89 FR 32976 (Apr. 26, 2024).
[40] 45 C.F.R. § 164.502(a)(5)(iii)
[41] 45 C.F.R. § 164.509.

- **42 U.S.C. 290dd-2 and Part 2 (collectively "Part 2")**. Part 2 regulates the use and disclosure of certain substance use disorder (SUD) treatment records that originate from certain regulated SUD providers. Part 2 requires a Part 2-compliant consent (which is different from a HIPAA authorization) for the use and disclosure of protected Part 2 records unless an exception applies. Unlike HIPAA, there is not a general TPO exception. Under the CARES Act Final Rule changes,[42] a special type of TPO consent may be obtained that allows HIPAA-regulated ***recipients*** of the Part 2 records to ***redisclose*** the records as permitted by HIPAA;[43] however, even these HIPAA-regulated recipients cannot use or disclose the Part 2 records in proceedings against the patient and a patient may always revoke the TPO consent, which cuts off further uses and disclosures of the Part 2 records.[44]

- **Title X Confidentiality Regulation.** The Title X confidentiality regulation applies to organizations that receive Title X funding for family planning services and protects the personal facts and circumstances obtained by the Title X providers about individuals who receive such services.[45] It prohibits the release of such information without the patient's written authorization, except as necessary to provide the Title X services or as required by law.[46] It also has special rules about the disclosure of a minor patient's Title X data.[47]

- **Federal Privacy Act.** The Federal Privacy Act[48] governs the use and disclosure of personally identifiable information about individuals that is kept by federal agencies, such as the Veterans Administration (VA) or the U.S. Department of Defense (DoD). It is more restrictive than HIPAA and generally requires an individual's prior written consent for disclosure, unless an exception applies.[49]

- **CMS Medicaid Privacy Regulation.** The Medicaid privacy regulation requires State Medicaid agencies, as well as Medicaid managed care organizations and Children's Health Insurance Program (CHIP) managed care entities (as well as their subcontractors), to obtain consent from a family or individual, whenever possible, before responding to a request for information from an outside source, unless the information is being used to verify income, eligibility and the amount of

[42] 89 FR 12472 (Feb. 16, 2024).
[43] 42 C.F.R. § 2.33(b).
[44] 89 FR at 12553.
[45] *See* 42 C.F.R. § Part 59.
[46] 42 C.F.R. § 59.10(a).
[47] *See, e.g.*, 42 C.F.R. § 59.10(b).
[48] 5 U.S.C. § 552a.
[49] 5 U.S.C. § 552a(b).

a medical assistance payment.[50] CMS has recently interpreted this regulation as requiring specific patient consent to the disclosure of a patient's Medicaid data to an out-of-network provider or non-Medicaid/non-CHIP payers, even for treatment and healthcare operations purposes.[51]

State Privacy & Consent Policies

- **State Health Data Laws** (*e.g.*, health data maintained by state-regulated healthcare providers and payers). Each state in the United States has dozens of state-level health data laws that may more stringently regulate the use and disclosure of certain types of health data maintained by certain types of individually licensed health care providers and regulated healthcare entities. For example, in California, the California Confidentiality of Medical Information Act (CMIA) (with respect to abortion data released outside of the state)[52] and other laws like its HIV test results statute,[53] Lanterman-Petris-Short Act (LPS),[54] SUD statute,[55] and hereditary disorders statute[56] all generally require a patient's consent for the disclosure of the protected data even for treatment purposes.

- **State Public Health Data Laws** (*e.g.*, health data maintained by public health authorities and other state or local governmental entities). Separate and apart from the state laws that regulate the use and disclosure of data maintained by providers and payers, are those laws that apply to governmental bodies and public health authorities. Where a provider or health plan may be authorized to share health data for certain purposes (like TPO), a public health authority may not be granted similar permissions. For example, in Arizona, health data reported to the Arizona Department of Health Services (ADHS) for its chronic disease surveillance system strictly limits when that reported data may be used and disclosed to third parties.[57]

---

[50] 42 C.F.R. § 431.306(d).

[51] *See* 89 FR 8758, 8811 (Feb. 8, 2024) (interpreting the regulation as prohibiting "disclosing data to an outside source, such as providers that are not enrolled with the state Medicaid or CHIP agency, and that might be participating in an HIE, without prior permission from the individual") and *id.* at 8850-51 (interpreting the regulation as prohibiting "disclosing data to an outside source, such as non-Medicaid or non-CHIP payers, with whom the HIE might exchange data, without prior permission from the individual").

[52] Cal. Civ. Code § 56.110.

[53] Cal. Health & Safety Code §§ 120980, 120985 and 121010.

[54] Section 5328 of the Lanterman-Petris-Short Act, Cal. Welfare & Institutions Code §§ 5000 et seq. (the "LPS Act").

[55] Cal. Health & Safety Code § 11845.5,

[56] Cal. Health & Safety Code §§ 124975 – 124996.

[57] *See, e.g.*, A.R.S. § 36-133(D) (limiting disclosures to "studying the sources and causes of cancer, birth defects and other chronic diseases" or "[t]o evaluate the cost, quality, efficacy and appropriateness of diagnostic, therapeutic, rehabilitative and preventive services and programs related to cancer, birth defects and other chronic diseases").

- **State Data Segmentation Laws.** Some state laws, such as those in California and Maryland, require certain regulated entities to take additional steps to identify, segment and protect certain types of sensitive health information, such as medical information related to gender affirming care, abortion and abortion-related services, and contraception.[58]

- **State HIN/HIE Laws.** Many states have laws that specifically regulate the exchange of health data through HIN/HIEs and give patients the right to opt out of the exchange of their health information in this manner. For example, Arizona uses a notice and opt out approach to health information exchange whereas Nevada requires notice and opt in to such exchange.[59]

- **State Consumer Data Laws.** As of August 2024, there are at least 22 states that have state consumer data laws that govern how certain organizations use and disclose consumer data. While all of these state laws generally have exemptions or exceptions for data that is maintained as PHI by HIPAA regulated entities, many of these laws apply to non-HIPAA regulated entities, such as community-based organizations ("CBOs"). Indeed, several of these consumer data laws apply to non-profit CBOs that meet the jurisdictional thresholds for applicability.[60]

- **State Data Broker Laws.** There are also a growing number of states that have data broker laws that may apply to those technology companies that support the infrastructures and services necessary to deploy digital platforms and electronic health information.[61]

[58] *See, e.g.*, Cal. Civ. Code § 56.101; Md. Code § 4-302.5 and COMAR 10.11.08, 10.25.18.

[59] *See* A.R.S. §§ 36-3801 through -3809; N.R.S. §§ 439.581 through 439.597 and Nev. Admin. Code §§ 439.572 through 439.596.

[60] *See, e.g.*, Colo. Rev. Stat. Ann. § 6-1-1304(2)(o) and 4 Cal. Code Regs. § 904-3, Rule 2.02; 6 Del. C. § 12D-103(b)(1), (3); Md. Code Ann., Com. Law § 14-4603(a)(4); Minn. Stat. Ann. §§ 325O.03(Subd.2)(a)(20); Nev. Rev. Stat. Ann. § 603A-490; Or. Rev. Stat. Ann. § 646A.572(2)(r); Wash. Rev. Code Ann. § 19.373.010; N.J. Stat. Ann. § 56:8-166.13.

[61] *See, e.g.*, N.R.S. §§ 603A.300 to 603A.360, O.R.S. § 646A.539, Texas Business & Commerce Code 509.001, *et seq*, 9 V.S.A. §§ 2430, 2431, 2446 & 2447.

Appendix 2: Survey of the Federal and State Interoperability Landscape

This Appendix presents a set of federal and state policies on health information exchange that stakeholders should consider when embarking on efforts to exchange health data in digital and networked environments across multiple jurisdictions and involving a variety of differently regulated and unregulated stakeholders[62].

- **Federal and State Information Blocking Rules.** Certain regulated actors are also prohibited from engaging in practices that are reasonably likely to interfere with the access, exchange and use of electronic health information, unless the practice is explicitly required by law or a regulatory exception applies, such as an exception that permits information blocking to the extent reasonable and necessary to comply with underlying federal, state, tribal, and local privacy laws. These are intent-based statutes that exist at the federal level (see the federal Information Blocking Rule, 42 USC 300jj-52 and 45 CFR Part 171) and in some states, such as Tennessee[63] and Connecticut.[64] In 2024, ASTP-ONC also finalized the HTI-1 Final Rule[65] and HTI-3 Final Rule[66] changes to the federal Information Blocking Rule, which expanded and added new safe harbor protections, including a new exception for protecting access to reproductive healthcare.

- **CMS Interoperability Mandates for CMS-Regulated Payers and Providers and Similar State Laws.** Certain regulated payers are also required to participate in certain federal or state mandated health information exchanges or patient access policies, including Patient Access APIs and soon-to-be-coming Provider Access APIs and Payer-to-Payer APIs. The CMS interoperability mandates specifically apply to Medicare Advantage Organizations, State Medicaid and CHIP agencies, Medicaid Managed Care Plans and CHIP Managed Care Entities, and Qualified Health Plan Issues on the Federally-Facilitated Exchanges.[67] However, certain states—such as California and Tennessee—have expanded these mandates to commercial payers.[68]

---

[62] Special thanks to Velatura HIE Corporation for contributing this content.
[63] 2024 Tennessee Laws Pub. Ch. 931 (S.B. 2012).
[64] Conn. Gen. Stat. Ann. § 19a-904d.
[65] 89 FR 1192 (Jan. 9, 2024).
[66] 89 FR 102512 (Dec. 17, 2024).
[67] *See, e.g.*, 89 FR 8758 (Feb. 8, 2024).
[68] *See* 2024 Tennessee Laws Pub. Ch. 931 (S.B. 2012); 2022 California Laws Pub. Ch. 888 (S.B. 1419 (codified at Cal. Health & Safety Code § 1374.196 and Cal. Ins. Code § 10133.12).

- **Electronic Health Information Technology Certification Requirements and CMS Promoting Interoperability Programs.** ASTP-ONC has long sought to standardize and provide base (or minimum) functionality for certified health IT through its certification program, which CMS has incentivized by tying Medicare payments to the meaningful use of such certified health IT (called "Promoting Interoperability").[69] These include minimum technical and security standards for patient access APIs and export functionality. These standards have also formed the technical basis for the CMS interoperability mandates discussed above. However, compliance with certification requirements are only legally required to the extent a technology company is seeking to obtain or maintain certification status or to the extent required by another law, such as the CMS interoperability mandates.

- **The Trusted Exchange Framework and Common Agreement (TEFCA), the California Data Exchange Framework (DxF) and other State or Regional HIN/HIEs.** There are also a host of requirements applicable to those who are required to participate in the California Data Exchange Framework (DxF), which is the statewide framework for health information exchange in California,[70]or who choose to participate other state or regional HIN/HIEs or in nation-wide TEFCA exchange.[71] In each instance, these trust frameworks for health information exchange put the burden on those who are using the exchange services to disclose their data to ensure that they not only have the necessary patient authorizations or consents in place to disclose the data to third parties who participate in exchange under these frameworks, but that the technology systems, platforms and networks that they use to support this exchange can meet all other legal requirements that might apply.

[69] 45 C.F.R. § Part 170 and CMS, Promoting Interoperability Program, *available at* https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs (last visited Aug. 30, 2024).
[70] Cal. Health & Safety Code 130290; *see also* CDII, Data Exchange Framework, *available at* https://www.cdii.ca.gov/committees-and-advisory-groups/data-exchange-framework/ (last visited Aug. 30, 2024).
[71] 42 U.S.C. § 300jj-11(c)(9); *see also* RCE, RCE Resource Library, https://rce.sequoiaproject.org/tefca-and-rce-resources/.

Appendix 3: Exploring Existing Consent Models

The Sequoia Privacy & Consent Work Group heard directly from a diverse range of organizations, states, and regional entities pursuing computable consent and data segmentation solutions. This Appendix provides a high-level summary of the information shared by these organizations.

State or Organization	About	Initiatives	Challenges
Shift Task Force	An industry-wide collaborative effort to advance data segmentation and consent	The Shift Task Force is gathering expert stakeholders from across the industry to "mature granular data segmentation standards and implement guidance in order to sponsor patient-driven sharing of health information with informed consent and advance interoperability in a more equitable manner". The Shift Modified Delphi Process / implementation workgroup is looking at use cases to advise Informed Consent use cases between EHRs & others (Patient Portals, HIEs, Apps, Payers, etc.) The Shift Technical Workstream is creating demonstrations of data redaction, patient consent, and partial record sharing.	Determining what constitutes "sensitive" data is subjective and can be inconsistent. A lack of standard value sets for sensitive information like behavioral health and reproductive health can lead to inconsistencies and confusion. More implementation and more extensive testing is needed.
HL7 Data Segmentation for Privacy (DS4P)	DS4P is a standard to achieve data segmentation for consent	DS4P and consent standards provide a framework to further define critical content that needs industry consensus building on how to use them and any needed refinements. The HL7 FHIR® Implementation Guide: Data Segmentation for Privacy (DS4P) provides FHIR guidance for applying security labels with coded tags for use in access control systems governing the collection, access, use, and disclosure of the target FHIR Resource(s) as required by applicable	Additional guidance is needed on HL7 standard codes for various sensitive data categories and clinical code value sets linked to each sensitivity category.

State or Organization	About	Initiatives	Challenges
		organizational or jurisdictional policies.	
The New York eHealth Collaborative (NYeC)	NYeC is an HIE/HIN partnering with the New York State Department of Health (DOH) to lead the Statewide Health Information Network for New York (SHIN-NY), a network connecting healthcare professionals and regional HIEs across the state. NYeC is working with New York State to implement a regulatory approach to statewide Information sharing.	NYeC, in partnership with the New York DOH, is working to move the state from an Opt-In "Consent to Access" model of consent to a SHIN-NY Statewide Community Consent model. This approach supports participation in National Networks and offers a more streamlined approach to consent, supportive of sharing data with community-based organizations. Current consent law in New York deploys an opt-in model, requiring regional HINs known as "Qualified Entities" (QEs) access to patient information only with written affirmative authorization from the patient or their authorized representative. Through SHIN-NY Policy, exceptions exist where data may be accessed without consent such as emergency "break the glass", public health reporting & access, and patient care alerts.	The current opt-in "consent to access" model of consent in New York makes it difficult to share data with organizations that do not collect consent, like community-based organizations and payers. Additionally the opt-in process is burdensome for both providers and patients. Providers must collect consent prior to accessing patient records (with limited exceptions such as emergency "break the glass"). Patients must opt-in at every facility / provider / point of care. Lastly, the opt-in model limits the ability for New York HINs to participate (e.g., reciprocate) in National Networks.
New Jersey Innovation Institute (NJII)	Health Information Exchange working with the state of New Jersey on consent for sensitive information sharing	The New Jersey Department of Health, together with the NJII, is implementing an electronic consent management solution (eCMS) to allow the transmission of Part 2 data to providers as consented to by patients. NJII is engaging in consent pilots beyond	There is difficulty integrating new "redisclosure notice" requirements into EHR systems until technology supports it. New Jersey's HIV law avoids redisclosure notice requirements, leading to inconsistencies with Part 2 changes.

State or Organization	About	Initiatives	Challenges
		Treatment, Population Health & Health Care Operations Uses & Disclosures in partnership with NJHIN, to include NJ licensed substance abuse providers, HIV/AIDS information, and Behavioral Health Providers.	Behavioral Health consents still require recipient names, complicating data sharing through HIEs.
Chesapeake Regional Information System for our Patients (CRISP)	Regional HIE in Maryland working to implement regulations related to consent to share	In Maryland, Senate Bill 786 was introduced in both the Maryland Senate and the House of Representatives (HB 812) as part of a suite of bills in response to Dobbs. In response to Senate Bill 786, CRISP is developing code-based systems for parsing and filtering data, and allowing affirmative patient consent for disclosure. Maryland is an opt-out state.	HIEs/HINs will need to integrate complex data parsing and consent mechanisms and accurately filter data according to prescribed code sets. They will also need to accommodate patient consent preferences, a task that some HIEs/HINs openly acknowledge they are unable or unwilling to undertake. Queries related to sensitive code sets, especially those concerning individuals with uteruses, may be blocked due to regulation.
Serving Communities Health Information Organization (SCHIO), San Diego's Community Information Exchange® (CIE) and 2-1-1 San Diego	Local collaboration to address universal consent for SDOH data, and a variety of information uses.	CIE employs role-based permissions and an audit trail for data privacy and security. Consent follows an opt-in model in CIE. The ASCMI pilot was a California DHCS pilot where three health/community information exchanges participated (Manifest MedEx, 2-1-1 San Diego, SCHIO). The ASCMI pilot gauged the willingness of individuals to share sensitive information for care coordination, with outcomes suggesting people are open to sharing data when informed about the benefits. Feedback from the pilot highlighted the need for a standardized universal consent form at the state level to streamline care coordination efforts across different programs and jurisdictions.	Provider buy-in has proved a challenge, as well as the variability in approaches to consent among different providers. Concerns about privacy and the accuracy of resource information

State or Organization	About	Initiatives	Challenges
Integrating the Healthcare Enterprise (IHE) Privacy Consent on FHIR	IHE is a standards organization working to advance consent.	IHE created a FHIR Consent Resource Implementation Guide that supports various consent models, including Basic, Intermediate, and Advanced Consents like DS4P. The Privacy Consent on FHIR (PCF) Profile provides support for patient privacy consents and access control where a FHIR API is used to access Document Sharing Health Information Exchanges.	Some organizations may not have the technology available to implement, even at the basic level. Varying state privacy requirements may be challenging to deploy in actual clinical environments.
Washington State Health Care Authority (HCA)	HCA is Washington's largest health care purchaser and its behavioral health authority.	The Washington State Health Care Authority has launched an Electronic Consent Management (ECM) solution, named "ConsentLink", to enhance the exchange of SUD data and other sensitive data types. This initiative aims to improve care coordination and reduce the administrative burden associated with managing consent. HCA is focusing first on storing consents to enable SUD data exchange. While in the very early stages of its pilot, ConsentLink is a platform that will support existing processes, including paper-based, with a baseline solution and build out incrementally to meet providers where they are. Washington State's ECM solution is not linked with the state HIE.	Some providers that have existing electronic consent management processes built into their systems have questioned the need to adopt another solution outside their method. The Part 2 rule released in February of 2024 has a two-year compliance window, which will require ConsentLink to be flexible to meet providers at their various stages of transition to the new practice.
Stewards of Change Institute (SOCI)	SOCI is a thought leadership and advocacy organization working to advance interoperability	SOCI has been focusing on the challenge of informed consent for sharing protected and private data. The organization established the National Interoperability Network (NIC) to serve as a	A few challenges include: Different levels of sensitivity of data (e.g., 42 CFR, Part2, general PHI, social care sensitive information, etc.).

State or Organization	About	Initiatives	Challenges
		community-driven platform that promotes information exchange and collaboration across various sectors.	Different levels of authorization, i.e., can you know a system has a record for an individual, and can you see an entire record/document (FHIR Consent) or specific sensitive fields (DS4P). Lack of a trusted sharing network, which inhibits building confidence by consumers/clients in their providers and care coordinators and safekeeping of their personal information.
Access Consent Policy Specification		Both eHealth Exchange and CareQuality provide a method that allows organizations to obtain a consent from the data requestor during the patient discovery transaction. This capability has been utilized by the Social Security Administration to request electronic health information for making disability determination for millions of patients over a decade.	Some organizations have concerns about automating this process without review of the consent.

Several studies and reports have been referenced throughout this section. For a complete list of resources and links, please refer to Appendix 4.

Appendix 4: Resource List

Additional readings and resources for further exploration.

- After Roe Fell: Abortion Laws by State
- SHARES: Substance Use HEalth REcord Sharing
- Carequality-Framework Policies (2023 PDF)
- FAST Consent at Scale Report (August 2023 PDF)
- FAST Consent Management Confluence page
- FAST Consent Management environmental scan and gap analysis
- Beckers Healthcare: Health data exchanges could prevent code blues, Epic finds
- HELP Senate Privacy Report (2024)
- ONC summary of Consent work (last updated 2019)
- ONC's Discovery Workshop on eConsent (Summer 2022)
- SHIFT: The Independent Health Care Task Force for Equitable Interoperability
- Statewide Health Information Network for New York (SHIN-NY) Governance
- State-Level Legal and Political Strategies Following the Repeal of Roe v. Wade, National Academies of Sciences, Engineering, and Medicine (2024).
- Stewards of Change Institute: Modernizing Consent to Advance Health and Equity (2021)
- Stewards of Change Institute: Institute Consent Learning Lab (2023)
- Stewards of Change Institute: Catalyzing Whole-Person Care: Consent-to-Share is the Key (2024)
- Part One: Privacy & Consent Management Landscape and Challenges to Scale | EHRA Blog
- Part Two: Privacy & Consent Management Landscape and Challenges to Scale | EHRA Blog

Appendix 5: Privacy and Consent Workgroup Members

The Sequoia Project is grateful to the members of the Privacy and Consent Workgroup for their contributions to this paper. While their expertise has been invaluable, this report is a collective effort and the views expressed are not those of any individual or organization.

- Lauren Riplinger, **American Health Information Association**
- Andrew Tomlinson, **American Health Information Association**
- Jeff Coughlin, **American Medical Association**
- Britt Bohannon, **Atlas Health Hub**
- Bart Carlson, **Azuba**
- Devi Mehta, **Blue Cross Blue Shield Association**
- Hannah Galvin, **Cambridge Health Alliance**
- Deven McGraw, **Citizen Health**
- Tatum Sihina, **Contra Costa Health**
- Mohammad Jafari, **Senior Privacy and Integration Specialist**
- Rosh Singh, **Cozeva**
- Caitlin Riccobono, **CRISP Shared Services**
- Elizabeth Delahoussaye, **Datavant**
- Susan Clark, **DirectTrust**
- Aaron Tait, **Epic**
- Matt Molisani, **Epic**
- Jaffer Traish, **findhelp**
- Hilary Greer, **HCA Healthcare**
- Steven Lane, **Health Gorilla (Co-Chair)**
- Julie Lowry, **Henry Ford Health**
- Alisa Kuehn, **Indiana Health Information Exchange**
- Matt Becker, **Kno2**
- Dennis Giokas, **Marble**
- Mo Weitnauer, **MRO Corp**
- Tucker Bair, **MRO Corp**
- AJ Peterson, **Netsmart**
- Helen Oscislawski, **New Jersey Innovation Institute**
- Jennifer D'Angelo, **New Jersey Innovation Institute**
- Samuel Roods, **New York eHealth Collaborative**
- Daniel Werlin, **NextGen**
- Lacey Millsap, **OCHIN**
- Tim Noonan, **Office for Civil Rights (liaison)**
- Kathryn Marchesini, **Assistant Secretary for Technology Policy (liaison)**

- Hans Buitendijk, **Oracle Health**
- Laurie Peters, **Orion Health**
- Daniel Chavez, **Serving Communities Health Information Organization**
- Lynne Nowak, **Surescripts**
- Martin Prahl, **Social Security Administration (liaison)**
- Peggy Pugh, **US Department of Veterans Affairs (liaison)**
- Lynne Harbin, **US Department of Veterans Affairs (liaison)**
- Elizabeth McElhiney, **Verisma**
- Barbara Carr, **Verisma**
- George Bessenyei, **YoCierge, Inc.**
- Melissa (Mel) Soliz, **Velatura HIE Corporation**

Sequoia Staff and SMEs

Chantal Worzala

Lindsey Elkind

Kathryn Lucia

Anna McColister, *Liaison to the Consumer Engagement Strategy Workgroup*