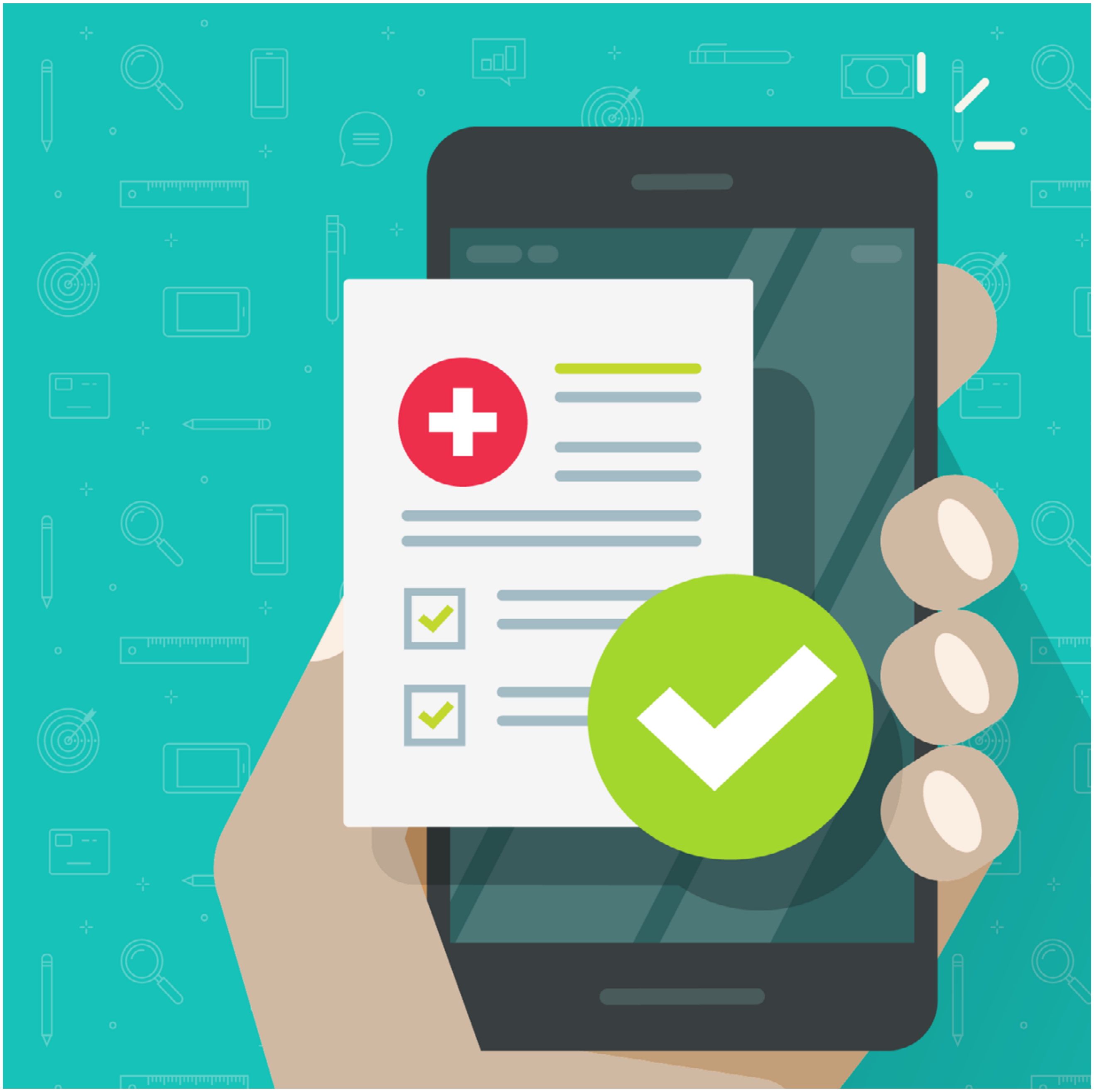
Modernizing Consent to Advance Health and Equity

A NATIONAL SURVEY OF KEY TECHNOLOGIES, LEGAL ISSUES AND PROMISING PRACTICES



Stewards of Change
INSTITUTE

Modernizing Consent to Advance Health and Equity

A NATIONAL SURVEY OF KEY TECHNOLOGIES, LEGAL ISSUES AND PROMISING PRACTICES

November 2021

This report was researched and written primarily by the following authors, with significant additional input from many others. Adam Pertman, a senior consultant to Stewards of Change Institute, also contributed writing and served as editor of the document.

Daniel Stein, President, Stewards of Change Institute
Brian Handspicker, Managing Partner, PracticalMarkets, Inc.
Matt Bishop, President and CEO, Open City Labs
Christine Alibrandi, Esq., Public Health Senior Attorney, Network for Public Health Law
Jennifer Bernstein, Deputy Director, Network for Public Health Law
Dan Chavez, Senior Consultant, Health Tech Solutions
Pooja Babbrah, Practice Lead, PBM Services, Point-of-Care Partners
Michael Solomon, Practice Lead, eCare Management, Point-of-Care Partners
Eric Jahn, CTO/Data Architect, Alexandria Consulting
Jim St. Clair, Executive Director, Linux Foundation Public Health
Mary Kratz, Executive Vice President, Interoperability Institute
Amanda Taylor, Consultant, Stewards of Change Institute

SOCI expresses sincere thanks to the Robert Wood Johnson Foundation, which funded this project.
The views expressed here do not necessarily reflect the views of the Foundation.

Robert Wood Johnson Foundation

We're especially grateful to the dozens of subject matter experts, technologists, government officials and other professionals nationwide who volunteered their time to conduct the work involved. A list of participants in this project is in Appendix C on Page 69, and the organizational logos of key contributors appear on Page 6.

Stewards of Change
INSTITUTE

TABLE OF CONTENTS (Page numbers are hyperlinked)

Executive Summary

In early 2021, the Stewards of Change Institute (SOCI) held an online symposium, in partnership with the Stanford University Center for Population Health Sciences, that culminated a yearlong, highly collaborative initiative titled "The National Action Agenda to Advance Upstream Social Determinants and Health Equity" (NAA).

Several recommendations grew out of that event. The primary one was to accelerate health-related progress by modernizing the archaic processes by which individuals (patients, clients, etc.) provide informed consent for their personal data to be shared across programs, systems and domains.

SOCI launched several projects to further that objective, including a scan of key efforts in the U.S. that aim to improve consent, as well as to explore the legal and technical challenges of enabling consent-driven data sharing across healthcare and human services. The results of that scan make up the bulk of this report. We also interviewed about two dozen subject-matter experts, reviewed relevant resources, and received ongoing information and insights from the dozens of additional experts who worked with us. This national scan offers the first examination/aggregation of consent-related activities in a decade. We undertook the project because we believe there's an urgency to obtaining and utilizing this accumulated learning for reasons including:

- The pandemic's spotlight on the need to improve information sharing and on the racial and socioeconomic disparities impeding better healthcare for too many people.
- A growing focus on the importance of the Social Determinants of Health and Well-Being (SDOH), without a clear roadmap or systems-level processes for addressing them.
- The immediate opportunity to apply, test and scale what we learn – with the goal of instigating and implementing structural change – beginning with the federally funded Integrated Care for Kids (InCK) sites in New York and New Jersey, which have agreed to be SOCI's implementation partners on this work.

The content in this report comes primarily from healthcare-related domains, because those are where issues related to consent currently receive the most attention and where, generally speaking, the most progress on modernizing consent processes is being made. That said, our "target audience" is not solely healthcare institutions and systems.

'As we're moving into this next generation of adding more complexity to the data sources . . . it is incumbent on us to really step up the game and make sure that we have true informed consent and that we have an appreciation for how people can be educated about who is seeing their data and when. . . . We're going to have to sort out a way to create an interoperability between public health and social care systems in particular.'

– Karen DeSalvo, MD, MPH, Chief Health Officer, and former ONC National Coordinator speaking at the HL7 35th Annual Plenary, September 20, 2021

Rather, our intent is to 1) provide information and insights for non-healthcare professionals to advance their consent processes; 2) spotlight the essential need to include and build trust with People with Lived Expertise in all phases of this work; 3) advance the creation and adoption of an open-source, replicable and customizable solution for consent-related efforts; and 4) accelerate understanding of the importance of cross-sector data sharing among all of those contributing to people's health and well-being (e.g., healthcare, human/social services, behavioral health, education and other SDOH factors) to increase development and implementation of processes to further that aim.

In conducting its scan, SOCI and its partners identified numerous governmental and business-sector organizations engaging in promising practices. For the purposes of this report, that means they have created, are creating or are now using digitized/computable consent systems (as opposed to paper-based ones) that hold the promise of significantly enhancing operational efficiency and effectiveness; giving individuals more-granular control over their data; demonstrably contributing to progress toward greater health equity and better outcomes; furthering cross-domain partnerships and/or better care coordination that addresses SDOH; and containing approaches, technologies and/or additional elements from which others can learn to improve their own efforts.

It is important to emphasize that the systems, projects and other efforts described in our full report are not the only ones devising and implementing promising practices; rather, they are examples of such work, which we've sorted into four "categories:" Health Information Exchanges (HIE), Electronic Physical and Behavioral Health Record Systems (EHR), Community Referral Services (CRS), and Community Information Exchanges (CIE). One additional category, Industry and Governmental Initiatives, focuses on examples of federal or industry-supported efforts that have highly applicable learning related to consent.

Finally, we want to clearly state from the start that we recognize there are ethical and trust issues, privacy concerns, multi- jurisdictional laws and legal decisions, potential risks and even possible harms that must be factored into any work related to informed consent, and to the sharing of personal/ private information more broadly. The overarching goal of improving health, well-being and equity is undermined if those considerations aren't top of mind at every step, from planning to implementation.

Overview and Background

One of the most vexing impediments to maintaining privacy, while improving care delivery across health and social services through programs, is the lack of a coherent national framework or standardized digital means to enable and track approval by individuals to share their personal data within and across the multiple programs, systems and domains (e.g., education, housing, etc.) that contribute to everyone's health and well-being. Indeed, most processes for consenting to share information today are slow, onerous and hard to monitor or manage, largely because they're conducted in silos and are paper-based.

As a result, every organization must determine for itself how to manage the many factors involved, a reality that hampers efforts to achieve greater uniformity and otherwise drive innovation and progress. In addition, patients currently wishing not to share some of their records sometimes must either have their privacy compromised and share everything, or have to choose to share nothing and potentially receive worse services because the care team doesn't have the individual's full clinical and social context.

The bottom line is that, even when consent is documented, significant issues complicate the sharing process. The complexities involved include but aren't limited to:

Lack of consent "granularity." Consent is usually applied generally to an entire record, without empowering individuals to specify which data can be provided to whom or for what purposes. Lack of uniformity. There is no uniform definition of "consent," nor is there broad acceptance of what data, organizations and users are impacted by a specific consent.

Lack of communication. The many domains that can/ should share data have different systems and procedures in place that cannot "talk" to each other.

Lack of discoverability. With personal information distributed so widely, it is difficult for an individual to know what systems have their sensitive data or how to manage it.

Lack of trust and understanding. Perhaps most importantly, there is often a lack of trust -- especially among PwLE -- relating to service providers, as well as a lack of understanding of their consent- and privacy-related rights.

Enabling and accelerating the secure, digitized/computable exchange of personal health and social data could help healthcare and social services providers improve their assessments of patient/client risk and develop more- comprehensive, coordinated care plans.

Primary Findings and Learnings

The following are some of the key things we discovered, learned and discerned during the course of our scan, notably including from the interviews we conducted. The full report elaborates on all these points and others.

Identity management is a prerequisite for informed consent. If an individual's correct, verified identity is not determined and managed, then core issues such as privacy, data-sharing and informed provider services cannot be adequately, ethically addressed.

The development and implementation of effective consent procedures and architectures are hindered by: regulations (or the interpretation of them); a lack of understanding in some organizations of privacy rights and a tendency to interpret underlying regulations too restrictively; and "all or nothing" practices.

The participation of "People with Lived Expertise" needs to be meaningfully incorporated into current and future efforts relating to consent (as well as other efforts affecting them) to assure that their input, insights and influence are integral to the planning, decision-making, implementation and other aspects of this work.

The US suffers from a patchwork of uncoordinated federal and state laws that address privacy and consent issues in either healthcare or non-healthcare domains. Indeed, they often do not align with each other or lack clarity about how they interact, thereby leaving gaps and causing confusion even on fundamental questions.

There are no established structures for addressing and resolving multi-domain privacy and consent issues/problems/ challenges. Instead, they are currently dealt with in a piecemeal fashion, usually within the affected domain and with resolutions that primarily or exclusively impact only that domain.

There is no system, process or repository that enables a patient/client, provider, care-giver or any other professional/organization to find an informed-consent directive given by an individual, irrespective of where that person lives (or lived) or in what domain/context the consent was provided. That reality undermines even the most ambitious current efforts to improve services, processes and outcomes.

Outside of Health Information Exchanges (HIEs) and Community Information Exchanges (CIEs), consent standards have not been widely adopted to share and enforce consent declarations across IT systems. Instead, proprietary consent functionality enables collection, revocation and enforcement in siloed systems.

A lack of maturity of human service data standards could impede granular data sharing. Nevertheless, existing open-source technology could serve as the foundation for a Consent Service Utility, such as one being developed by SOCI, which would offer significant promise for enabling people to have greater control over their data.

Education and investments are needed for ongoing learning about the laws, regulations, policies, data and technologies that have an impact on informed consent. We stress "ongoing" because many of those things differ from institution to institution and state to state, and they are changing rapidly.

Voices from the Community

Because we steadfastly believe community engagement and the remediation of systemic bias and inequity are always vital, we interviewed members of the Bronx Community Research Review Board about this report and some of the issues it addresses. The BxCRRB's mission is to "eradicate health inequities" in marginalized communities in the Bronx. We chose the Bronx because it is the site of one of SOCI's partners in its consent work, the federally funded Integrated Care for Kids project.

These interviews constitute a first step toward far greater involvement by "people with lived expertise" in any planning or action steps we take as a result of what we've learned in conducting this project.

> 'There's no such thing as a single-issue struggle because we do not live single-issue lives,' said one interviewee.

The interviewees agreed that three keys to making progress on consent – and many other issues – are having a broad context, building trust and understanding the value of relationships. The full report elaborates on the following key points BxCRRB members made relating to consent:

Consent isn't just about the individual asked to provide it. Though it is often treated as a process affecting just a person filling out a form, that individual may have family with whom they want to discuss whatever they are being asked to consent to – and who could also be significantly impacted. That means the individual needs time to go home, think and talk, rather than having to immediately sign on the dotted line. In addition, the process should take into account the need to build relationships with doctors and other service providers, so it's about trust and not just information to complete a transaction.

It's a big problem if consent moves primarily to apps, especially for people in disadvantaged communities who might not own smartphones, don't have adequate wireless services and/or lack technical knowledge. Paper may be preferable for them, perhaps most significantly so they can take the forms home, where they can talk to others and think about the benefits and risks of sharing their data. And, whether the consent forms are on paper or on a device, it's critical that they be written in language that is easily understandable and as devoid as possible of specialized (ex., legal or technical) wording or jargon.

> Added another: 'It should be about relationality, relationality, relationality. . . . Data is not going to matter in the absence of remediating harm and shaping relationships.'

Professionals don't always understand the implications and consequences of their requests for consent. Rather, they view the process as purely transactional – you sign here now and then we'll provide a treatment or a service. The patient/client, however, may reasonably wonder how and with whom their information will be shared (perhaps a service provider who harbors a racial bias?) as well as what the consequences may be (ex., if a years-old court record is shared with a child welfare worker). So the process needs to include thoughtful conversations to ensure the individual is genuinely informed.

There's an inherent power imbalance between the people giving or denying consent – especially in marginalized communities – and the professionals providing social services or medical care. That means patients/clients can feel intimidated into approving the sharing of their personal information or believe (often rightly) that they have to do so to receive the treatment or service they require. Consent-related processes need to recognize this reality and mitigate its potentially negative impact, including by providing information to ensure that recipients clearly understand the risks as well as the benefits.

> And this third comment: `If I can't have an interactive relationship, I don't want it.'

A history of racism and socioeconomic disparities means the perspective of individuals being asked to provide their approval isn't shaped only by the questions relating to consent and information sharing per se. Rather, it's also based on personal and historical experience. So, for example, will they believe that all the people they're dealing with – or the ones receiving their data – have their best interests at heart? Will that information be properly used? Who will the real beneficiary be, the patient/client or the institutions requesting the consent and participating in the sharing?

Recommendations and Next Steps

A more-complete list, with elaboration on each item, is in the Recommendations section of the full report:

1. The dozens of participants in this project should collaboratively plan and carry out a series of activities in 2021 and 2022 (and beyond) to advance the information, insights and learnings reflected in this report.

2. Remediating socioeconomic and racial disparities, as well as building trust and furthering health equity, should be built into the framework of all the activities outlined in these recommendations.

3. People with lived expertise should be incorporated into all aspects of consent-related efforts to increasingly give them genuine agency over the decisions and actions that impact them most.

4. The ONC and other federal agencies, pointedly including ones that focus on SDOH and not just healthcare, should launch regular meetings on consent and data sharing.

5. SOCI and its collaborators should continue development of an open-source, standards-compliant Consent Service Utility (CSU) as a key part of implementing the guidance in this report.

6. A symposium should be planned, organized and staged in mid-2022 to share the ideas and insights reflected in this report, as well as additional ones generated by the activities above.

7. A widely marketed webinar “learning series” should be organized to begin as soon as possible after publication of this report, and to continue at least until the 2022 symposium.

8. The InCK sites should be used as a national model for developing, testing and implementing the modernization of consent practices across programs, systems and domains.

Thanks to Our Participants

LF PUBLIC HEALTH

NIC NATIONAL INTEROPERABILITY COLLABORATIVE

SAN DIEGO HEALTH CONNECT Better Information • Better Care™

The Network for Public Health Law 10 YEARS STRONG

INTEROPERABILITY INSTITUTE

InCK NJ Integrated Care for Kids

FEI Systems

HIMSS℠

HSLynk

Point•of•Care PARTNERS HEALTH IT MANAGEMENT CONSULTANTS

MiHIN MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

CRISP

PatientCentricSolutions

ZANE NETWORKS

Midato Health™

OPEN CITY LABS

ALEXANDRIA CONSULTING

EHRA HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

Interoperability Connections that empower Coloradans

PracticalMarkets

kantara INITIATIVE™

aws

PP2PI

SAN DIEGO HEALTH CONNECT Better Information • Better Care™

HealthTech SOLUTIONS

gainwell

BE-InCKNY

Introduction

In early 2021, the Stewards of Change Institute (SOCI) held an online symposium, in partnership with the Stanford University Center for Population Health Sciences, that culminated a yearlong, highly collaborative initiative titled "The National Action Agenda to Advance Upstream Social Determinants and Health Equity" (NAA).

Several recommendations grew out of that event, the primary one of which was to accelerate health-related progress in our country by modernizing the archaic processes by which individuals (patients, clients, customers, etc.) provide informed consent for their personal data to be shared across programs, systems and domains.

SOCI subsequently launched several projects to further that objective, including a scan to identify key efforts throughout the U.S. that aim to improve consent, as well as to explore the legal and technical challenges associated with enabling consent-driven data sharing across healthcare and human service providers. The results of that scan, conducted with numerous collaborators during the past few months and funded by the Robert Wood Johnson Foundation, make up the bulk of the content of this report.

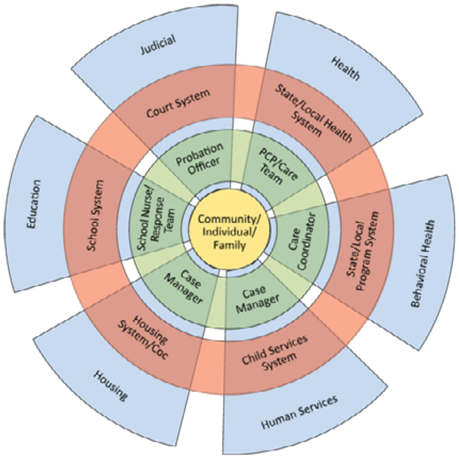
We also interviewed about two dozen subject-matter experts, reviewed research and other relevant resources, and received ongoing, substantive information and insights from the dozens of additional experts who worked with us. (Appendix C contains a list of all participants in this project.)

This national scan offers the first examination/aggregation of consent-related activities in a decade. We undertook the project because we believe there's an urgency to obtaining and utilizing this accumulated learning for an array of reasons. They include but are not limited to:

- The pandemic's spotlight on the need to improve information sharing and on the racial and socioeconomic disparities impeding better healthcare for too many people.
- A growing focus on the importance of the Social Determinants of Health and Well-Being (SDOH), without a clear roadmap or systems-level processes for addressing them.
- The immediate opportunity to apply, test and scale what we learn – with the goal of instigating and implementing structural change – beginning with the federally funded Integrated Care for Kids (InCK) sites in New York and New Jersey, which have agreed to be SOCI's implementation partners on this work.

This work also adds to the body of knowledge SOCI and its collaborators are using to define and design an innovative Consent Service Utility (CSU) as part of our Project Unify, which seeks to accelerate interoperability and information-sharing more broadly. The CSU and Project Unify, along with the scan, are among the consent-related projects we are currently conducting. They build on initiatives developed by governmental and private organizations for over a decade, largely instigated and supported by the Office of the National Coordinator for Health Information Technology (ONC) within the US Department of Health and Human Services.

Project Unify Conceptual Model



Person-centered care requires coordination of many intersecting service domains

It's important to underscore that one of our primary objectives for this report was to review consent-related initiatives not just in the world of healthcare, but also in other domains that significantly impact health and well-being. Those include but are not limited to education, justice and human/social services (abbreviated in this report to just "social services"). Our intent in widening the lens was to gain insights into what other domains can learn from healthcare, where most of the current work on consent is taking place.

Finally, we want to clearly state from the start that we recognize there are ethical issues, privacy concerns, multi-jurisdictional laws and legal decisions, potential risks and even possible harms that must be factored into any work related to informed consent, and to the sharing of personal/ private information more broadly. The overarching goal of improving health, well-being and equity is undermined if those considerations aren't top of mind at every step of planning and implementation.

Overview and Background

The advent of electronic health information standards in the late 1980s and early 1990s enabled more-efficient collection of personal health information, while also creating the potential for inappropriate sharing of that information. This concern led to the Health Information Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations, which codified the right of patients to protect their private information; HIPAA's regulations, in turn, set standards for the sharing of protected health information (PHI).

Subsequently, as organizations have explored their ability to electronically exchange data – and as the desire to share PHI has grown to improve care coordination, integrate medical services and for other purposes – an unintended consequence of HIPAA has been to unnecessarily hinder progress in those regards. It's also important to point out that, while HIPAA is a federal statute, electronic healthcare data exchange has also taken place within local healthcare systems.

More recently, the 21st Century Cures Act, ONC Cures Act Final Rule and the Centers for Medicare and Medicaid Services' (CMS) Interoperability and Patient Access rule have made it easier to share health-related data and easier for patients to access their personal health information in a desktop or mobile application (app) of their choice.

For instance, the Blue Button 2.0 project (a collaboration of the Department of Veterans Affairs, CMS and the Department of Defense) has enabled Medicare recipients to access their data through an app[1], and they can revoke access that they have previously authorized through Medicare.gov. These initiatives represent a major step in the right direction, but leave several issues unaddressed that are discussed in this report.

In the past few years, cross-sector data sharing has become critically important to a growing number of programs and initiatives throughout the country, including those mentioned above. At the same time, recognition of the role in health of SDOH (e.g., social/human services, behavioral health, education, courts, etc.) has become increasingly recognized. Indeed, research indicates that up to 80 percent of an individual's health and well-being are determined by these non-healthcare factors. Integrating social care into the healthcare of individuals, families and communities requires the ability to readily share personal social information with healthcare providers and health information with social care providers.

One example of the application of SDOH data to family health is the Integrated Care for Kids (InCK) program, an innovative model funded by the federal Centers for Medicare and Medicaid Innovation (CMMI). The InCK awardee sites in New Jersey and New York, which participated in this scan project and are SOCI implementation partners, are seeking to improve outcomes for the populations they serve by augmenting medical/clinical assessments with a more-comprehensive child view through data that can be contributed by school districts (e.g., student attendance) and government agencies (e.g., foster care).

In addition to the explosive growth in the collection and use of personal data related to healthcare, human services and other fields, increasingly sophisticated and ubiquitous technologies for the collection of people's information more generally have kept the public debate over privacy at center stage. This phenomenon is occurring at an ever-accelerating pace and with an increasingly greater focus on privacy and security; a few examples include the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Pan-Canadian Trust Framework (PCTF), electronic Identification, and Authentication and Trust Services (eIDAS), among others.

Enabling and accelerating the secure, digitized/computable exchange of personal health and social data could help healthcare and social services providers improve their assessments of patient/client risk and develop more-comprehensive, coordinated care plans. Most pointedly, since the information sharing is meant to help individuals and families, it would enable them to tell their stories more accurately and comprehensively to a wide variety of service providers.

It's important to point out that accessing or sharing this information requires not only adhering to HIPAA and additional relevant healthcare privacy statutes, but also to other non-healthcare privacy laws such as the Family Educational Rights and Privacy Act (FERPA).

[1] Blue Button® 2.0, "Improving Medicare Beneficiary Access to Their Health Information, Center for Medicare and Medicaid Services," 2019, https://w ww.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/Blue-Button

One of the most vexing impediments to maintaining privacy, while improving care delivery across health and social services through programs such as InCK, is the lack of a coherent national framework or standardized digital means to enable and track approval by individuals to share their personal data within and across the multiple programs, systems and domains (e.g., education, housing, etc.) that contribute to everyone's health and well-being. Indeed, most processes for consenting to share information today are slow, onerous and hard to monitor or manage, largely because they're conducted in silos and are paper-based.

'Those issues include, but are not limited to, identity verification and management; privacy protection; and a progression from absolute "opt-in/opt-out" choices toward more granularity in selecting what data can be shared, with whom and under what circumstances.'

As a result, every organization must determine for itself how to manage the many factors involved, a reality that hampers efforts to achieve greater uniformity and otherwise drive innovation and progress. In addition, patients currently wishing not to share some of their records sometimes must either have their privacy compromised and share everything, or have to choose to share nothing and potentially receive worse services because the care team doesn't have the individual's full clinical and social context.

The bottom line is that, even when consent is documented, significant issues complicate the sharing process. The complexities involved include but aren't limited to:

Lack of consent "granularity." Consent is usually applied generally to an entire record, without giving individuals (clients, patients, consumers, etc.) the ability to specify which information in the record can be provided to which providers or for what purposes.

Lack of uniformity. There is no uniform definition of "consent" (or "informed consent") across programs, systems and domains, nor is there a broad acceptance of what data, organizations and users are impacted by a specific consent.

Lack of communication. The many domains that can/should share data (health, social services, etc.) have different systems and procedures in place that cannot "talk" to each other and don't use the same vocabulary for the information being communicated.

Lack of discoverability. With personal information distributed so widely across online systems, including health and social services systems, it has become very difficult for an individual to know what systems might have sensitive information about them and how to then manage their privacy preferences and the consent to access that information across all these systems.

Lack of understanding. Perhaps most importantly, most people lack a fundamental understanding of their rights relating to privacy and to granting – or denying – consent. In addition, as discussed elsewhere in this report, even professionals whose responsibility is to monitor or enforce HIPAA (as well as other restrictive statutes) too often don't understand its usage and err on the side of not releasing information that could be legally shared.

Even as the provision and tracking of consent become more electronic and granular, expectations are increasingly being placed on patients/clients to understand the processes, issues and implications involved. The people who live in underserved and marginalized communities are the least likely to succeed in navigating the consent process and ensuring they can provide the consents they genuinely want.

There are many reasons this is the case, most notably the significant gaps between higher and lower socioeconomic strata relating to access to technology, education, employment, transportation and other SDOH factors. These hurdles are raised even higher by the fact that most forms used to obtain informed consent are replete with legal, medical and/or other complex terms rather than being written in plain language that's readily understood by most people irrespective of their literacy level.

In addition, people with more opportunities and resources are less dependent on others to ensure that they receive the care they need and that their care is coordinated; that is, they have the wherewithal to promote better communication and services for themselves regardless of whether the professionals/programs involved are operating optimally. So, by broadly improving healthcare and care coordination through better consent processes, the most-significant impact will be on populations that have benefited the least from the systems available to serve them.

These inequities require greater ongoing attention as electronic forms of consent continue to grow. It seems clear that the goal should be to level the consent playing field, so that everyone has the same opportunities to provide an informed "yes" or "no" to the sharing of their personal information, thereby diminishing the impact of socioeconomic disparities and advancing health equity.

There are many contributors to the current reality, from trust, governance, legal and technological issues; to political, ideological and cultural differences; to the racial and economic biases that have systemically undermined some members of society throughout U.S. history.

Updating or replacing antiquated approaches/systems will obviously take time, but we also believe the activities at the heart of this report – i.e., conducting a scan of national, state, county, private-sector and other major consent-related efforts, and then widely disseminating its findings – will in itself make meaningful contributions.

The heartening news is that many efforts are indeed now being made to address these concerns in a variety of ways. This report highlights a number of promising consent efforts. In particular, it focuses on how they are working to modernize the consent process in order to expedite the secure sharing of key data, streamline processes and improve outcomes. Many of these efforts, like the work being conducted by SOCI, build on the longtime efforts of the ONC.

In 2014, for example, the ONC published "Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure,"[2] and then funded projects to further its goals.

Pointedly, that vision included "the ability to manage patient consent decisions regarding the use and disclosure of health information electronically," according to a paper produced by the Mitre Corporation for the ONC that year. The Mitre publication, "Electronic Consent Management: Landscape Assessment, Challenges and Technology,"[3] was among the resources that informed our own project.

[2] The Office of the National Coordinator, "Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure," 2014, https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

[3] MITRE Corporation, "Electronic Consent Management: Landscape Assessment, Challenges, and Technology," 2014, https://www.healthit.gov/sites/default/files/privacy-security/ecm_finalreport_forrelease62415.pdf

More recently, annually since 2018, the ONC has supported a host of initiatives under its Leading Edge Acceleration Projects in Health Information Technologies (LEAP), all aimed at advancing the development and testing of data-sharing functionalities to support clinical care, research and improved healthcare outcomes. These ongoing efforts include the HL7 Da Vinci Project, the Chesapeake Regional Information System for Our Patients (CRISP) and the Fast Healthcare Interoperability Resources (FHIR) at Scale Task Force (FAST), among many others.

A common denominator among these important, innovative undertakings is that they typically focus mostly or entirely on healthcare, though that has begun to change in the last few years as the ONC has increasingly incorporated SDOH into its vision and funding. Indeed, last year the ONC published a "Health IT Framework for Advancing SDOH Data Use and Interoperability."[4]

One of SOCI's primary objectives throughout its 15-year history has been to expand cross-sector interoperability and information-sharing efforts beyond healthcare and into other domains that impact people's health and well-being; that is, ones that are now generally understood as components of SDOH.

We brought this perspective into our work on the scan for this report, which deliberately widened the lens through which we examined consent-related efforts nationwide to understand not only what is happening in healthcare, but also to see what comparable or applicable work is being conducted in other domains to enhance learning for every relevant system and organization.

One of the many lessons we have learned ourselves, or at least had reinforced, is that there needs to be greater recognition of the myriad, complex issues that must be addressed to truly modernize consent, pointedly including by making consent "computable," that is, minimally reliant on human actions. Those issues include, but are not limited to, identity verification and management; privacy protection; and a progression from absolute "opt-in/opt-out" choices toward more granularity in selecting what data can be shared, with whom and under what circumstances. Finally, it's relevant to point out that the many participants who joined SOCI to conduct our scan and produce this report uniformly agree this unprecedented work promises to help drive substantial progress in furthering the secure, cross-sector sharing of sensitive/legally protected information.

Toward that end, over time, we believe modernizing consent processes will contribute to:

Greater efficiency and lower costs, including by:

- Helping individuals and their families, particularly in underserved communities, navigate the many programs and services available to improve their health and well-being.
- Enabling professionals to provide more-integrated, better-coordinated health-related services and social programs such as a real-time, updated care plan for every individual.
- Streamlining operational and legal processes, while reducing duplication.

A diminution and remediation of socioeconomic and racial disparities by empowering people in less-advantaged populations with more information and easier-to-access tools for receiving services that, today, they often don't know they can receive or have difficulty obtaining. In addition, once care coordination and provision are indeed broadly improved, health-related outcomes presumably will become more uniform (whereas we know such outcomes are currently better for people with greater resources).

Improvements in health and well-being for all the reasons already cited, such as better care coordination and more informed, holistic and person-centered care.

[4] Jawanna Henry and Samantha Meklir, Office of the National Coordinator, "ONC Health IT Framework for Advancing SDOH Data Use and Interoperability," 2021, https://www.healthit.gov/buzz-blog/interoperability/onc-health-it-framework-for-advancing-sdoh-data-use-and-interoperability

Goals and Objectives

The immediate-term goal of SOCI's scan project was to identify, assess and aggregate key information about the processes with which individuals (patients, clients, customers, etc.) provide consent to share their private/personal data and how that data is or could be accurately and responsibly updated, shared, used and tracked, primarily by healthcare and human/social services providers. We have focused primarily on major efforts in the United States at the national, state, county and organizational levels that appear to be making demonstrable progress on improving consent-based information sharing.

This report focuses mainly on examples of informed consent and related efforts in the healthcare domain, where the most activity relating to consent is taking place. Potentially more importantly, it also includes relevant laws, technologies and approaches to data-sharing consent within and across other programs, systems and domains that significantly impact people's health and well-being (e.g., education, child welfare, etc.).

We're calling out these "social determinant" factors because they have not received sufficient attention to date; that's the case even though some, when better integrated with medical services, clearly have a huge positive influence on overall health and well-being, while also contributing to the mitigation and amelioration of socioeconomic disparities to advance health equity for everyone.

This project is one of several that SOCI is conducting relating to consent. We have made this environmental scan a priority because, at the highest level, our goal is not just to help improve the status quo.

Rather, our vision is to modernize and digitize the consent process so that it can be truly computable and ***granular*** (i.e., provide individuals with the ability to say "yes" or "no" regarding very specific data, in very specific circumstances and to very specific recipients, rather than just broadly opting in or out); readily adaptable or replicable; coherent and consistent in critical regards such as their standards, vocabularies, identity matching and management; and highly customizable. We strongly believe doing so will contribute to substantial progress by:

- Broadly improving health, health equity and well-being, including by remediating racial and socioeconomic inequities for disadvantaged and under-resourced populations.
- Enhancing privacy relating to data-sharing, as well as building trust in the process, by both service providers and those who receive their services.
- Advancing care coordination and person-centered services by enabling, streamlining and accelerating the exchange of information that can be used to accomplish those aims.
- More quickly, routinely and comprehensively integrating SDOH data (from education, behavioral health, justice, etc.) into the understanding and provision of care.
- Promoting greater uniformity in applying consent across sectors and helping individuals understand what consent means in the specific circumstances where they provide it.

Specific to this project, our objectives include:

- Aggregating and summarizing major consent-related efforts nationwide in healthcare, behavioral health, human services and other SDOH domains. Our aim is to create greater awareness and understanding of the role of privacy and consent in the sharing and use of personal data within and across programs, systems and domains.
- Informing Project Unify's consent-related efforts, especially defining governance and technology blueprints for a CSU, a replicable, open-API architecture for use within and across healthcare, behavioral health, social services, education and justice systems. SOCI is conducting proof-of-concept demonstrations to develop the technical requirements and blueprints for CSU implementations within our Project Unify and in collaboration with the InCK sites in New York and New Jersey.

Providing current and future consent-related efforts nationwide with knowledge and insights to enhance and accelerate their work by identifying key promising practices based on other data regulatory models; federal and state laws, policies and regulations; technologies, frameworks and approaches; research and other resources. We believe this content will be useful because many of the efforts examined in our scan were simply unaware of what others are doing or what elements of each other's work might help to advance their own.

Primary Findings and Learnings

The content in this report comes primarily from healthcare-related domains, because those are where issues related to consent currently receive the greatest attention and where, generally speaking, the most progress on modernizing consent processes is being made. That said, the "target audience" of this report is not solely healthcare institutions and systems.

Rather, our intent is to 1) provide information and insights for non-healthcare professionals to advance their consent processes; 2) advance the creation and adoption of an open-source, replicable and customizable solution for consent-related efforts; and 3) accelerate understanding of the importance of cross-sector data sharing among all of those contributing to people's health and well-being (e.g., healthcare, human/social services, behavioral health, education and other SDOH factors) to increase development and implementation of processes to further that aim.

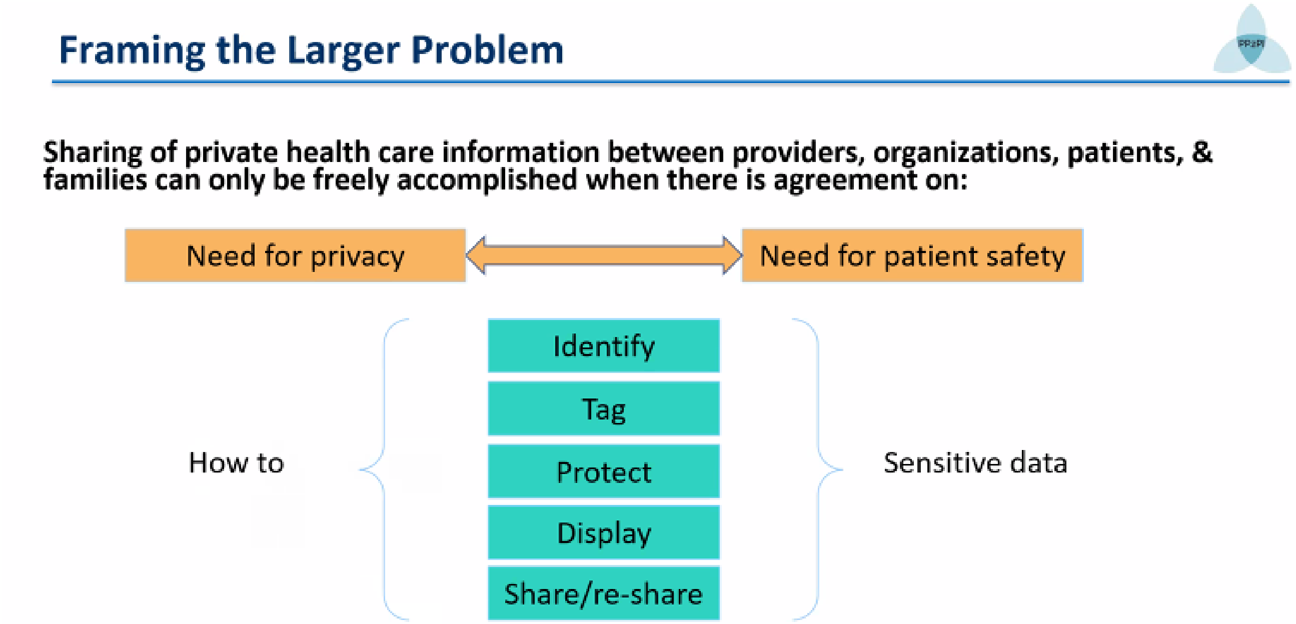
Against that backdrop, here are some of the key things we discovered, learned and discerned during the course of our scan, notably including from the interviews we conducted:

- **Identity management is a prerequisite for informed consent**. If an individual's correct, verified identity is not determined and managed, then core issues such as privacy, data-sharing and informed provider services cannot be adequately, ethically addressed. While digital identity is out of the scope of this report, it's critical to underscore this interdependency. We look to models such as Creating Access to Real-time Information Now through Consumer Directed Exchange (CARIN Alliance), the European Union's electronic IDentification, Authentication and trust Services (EU eIDas) and Pan-Canadian Trust Framework (PCTF) as references.

- **The development and implementation of effective consent procedures and architectures are hindered by:** regulations (or the interpretation of them); a lack of understanding in some organizational cultures of privacy rights and a tendency to interpret the underlying regulations too restrictively; and a continuation of "all or nothing" practices. This is the case even though Informed consent is recognized as a serious concern across all healthcare-related domains, as well as many others.

- **The participation of "People with Lived Expertise" needs to be increasingly, meaningfully incorporated** into current and future efforts relating to consent (as well as other efforts affecting them) to assure that their insights and influence are integral to programmatic planning, decision-making and implementation of this work. While progress is being made, it is clear that cultural, economic and social disparities have impeded the integration of PwLEs into projects and programs that impact them most.

- **The US suffers from a patchwork of uncoordinated federal and state laws that address**



Framing the Larger Problem

Sharing of private health care information between providers, organizations, patients, & families can only be freely accomplished when there is agreement on:

Need for privacy ⟷ Need for patient safety

How to { Identify, Tag, Protect, Display, Share/re-share } Sensitive data

Credit:PP2PI

privacy and consent issues in either healthcare or non-healthcare domains. Indeed, they often do not align with each other or lack clarity about how they interact, thereby leaving gaps and causing confusion even on such fundamental questions as who may or must obtain a consent in specific circumstances, what information is covered by that consent and with whom sharing can occur.

- **HIPAA allows for more sharing of PHI than many healthcare providers, social service organizations and patients/clients recognize.** Sometimes due to fear of liability for unauthorized disclosure (among other reasons), many providers default to not sharing PHI without express, written patient authorization, which can delay or hinder the provision of care. For example, HIPAA allows a provider to share PHI with an individual's case manager at a domestic violence shelter – without needing to obtain written patient authorization first – if the case manager is part of the care team.

- **There are no established structures for addressing and resolving multi-domain privacy and consent issues/problems/challenges**. Instead, they are currently dealt with in a piecemeal fashion, usually within the affected domain and with resolutions that primarily or exclusively impact only that domain. This is particularly the case when domains have both public- and private-sector dimensions. The result is that improvements and/or solutions tend to be idiosyncratic and circumstantial, rather than replicable or generalizable for others.

- **There is no system, process or repository that enables a patient/client, provider, care-giver or any other professional/organization** to find an informed-consent directive given by an individual, irrespective of where that person lives (or lived) or in what domain/context the consent was provided. That reality undermines even the most ambitious current efforts to improve services, processes and outcomes.

- **Outside of Health Information Exchanges (HIEs) and Community Information Exchanges (CIEs), consent standards have not been widely adopted to share and enforce consent declarations across IT systems.** Instead, proprietary consent functionality enables the collection, revocation and enforcement of consent within siloed systems. That said, Electronic Health Records (EHRs) are increasingly participating in National Trust Framework organizations, which focus on legal and policy agreements and common standards that operate under HIPAA exceptions that allow the exchange of medical data without consent for the purposes of payment, treatment and operations.

- **A lack of maturity of human service data standards could impede granular data sharing.** Existing open-source technology could serve as the foundation for a Consent Service Utility, offering significant promise for enabling people to have greater, more granular control of which of their education or human services data is shared with organizations of their choice. But the amount of granularity enabled will depend on the maturity and adoption of the data standards of the systems that are sharing the data – and, as of now, those systems are still in the early stages of their lives.

- **Partly due to the huge disparities in care exposed by the pandemic, there appears to be a greater focus on and more urgency across domains** on practices that modernize consent processes and, more broadly, that advance the sharing of personal/sensitive data. That's evidenced by a growing number of efforts at all levels to confront the challenge of protecting privacy while also furthering the exchange of important information, rather than continuing to travel the "all or nothing" route.

- **A common thread among promising practices, especially to make consent work on a large scale, is that they include some degree of governance.** While projects like InCK provide a geographic and programmatic focus (e.g., on Medicaid or child protection), a well-designed governance structure clears a path for bringing in all the necessary players, expanding the impacted area, increasing the programs involved and managing the consent process to optimize results.

- **Education and investments are needed for ongoing learning** about the laws, regulations, policies, data and technologies that have an impact on informed consent. We stress "ongoing" because many of those things differ from institution to institution and state to state, and they are changing rapidly. That is the case not only for healthcare, but also for all the SDOH domains that contribute to health and well-being.

Consent in Healthcare: Critical Factors for Success

As previously noted, healthcare is the world in which informed consent has received the most attention to date and in which the most progress has been made on modernizing these vital processes so they are increasingly digitized/computable. It's therefore critically important to examine the role of consent in healthcare both to drive continued improvements in that domain and to learn key lessons that can be applied in other SDOH-related domains.

A review of scholarly literature and primary research involving practitioners in the field has identified five approaches that are vital to the success of electronic support for a patient's informed consent (eConsent). Success was defined through the achievement of three broad outcomes: greater acceptance of the eConsent technology by patients and providers, increased perception of eConsent as a vehicle for more-informed consents compared to paper-based forms, and higher levels of comprehension by patients of authorized or declined consents.

The five critical success factors (CSFs) are: **Patient-Centered Model**, **Patient-to-Many Model**, **Shared Decision-Making Support**, **Strong and Trusted Version Control** and **Best Practices for Usability**. Together, they form a holistic, interrelated framework to guide development and evaluation of eConsent (see Figure 1: eConsent Framework). Although certain elements are more important in a specific type of eConsent than in others, all five are universally applicable.

This section of the scan report presents the findings from primary and secondary research conducted by Point-of-Care Partners during the 12-month period ending May 2021.[5] Results and analysis are organized by each of the five CSFs. Note that patients or their designated proxies (e.g., agent with medical power of attorney) have legal standing to grant consent for release of health information, evaluation and treatment, etc. (Proxy Consent, 1993).[6] For ease of discussion, subsequent references to the patient also include designated proxies.

Patient-Centered Model

In this model, patients control consent management and are the owners of eConsents on record (Brandner, et. al., 2016; Heinze & Bergh, 2014).[7] An emergency department physician asserted that "these documents need to be owned by the patient, not the physician. Healthcare is moving from physician-centric to patient-centric. ..." (POCP, 2020b)[8] The eConsents are managed through an organization-agnostic, standards-based (e.g., Integrating the Healthcare Enterprise [IHE] technical frameworks) application that is designed for use by a diverse adult population (e.g., race, ethnicity, various levels of education, health and computer literacy) across different devices such as smartphones, tablets and computers.

Using the eConsent application, augmented with online and in-person training and support, the patient creates a personal care team. Its members include healthcare professionals at a specific organization, relatives, individuals with medical power of attorney, etc. For each team and its members, the patient chooses which sections of their health record (e.g., behavioral health history) are restricted, if applicable, and timeframes for consent such as a specific episode of care or an expiration date (Heinze & Bergh, 2014).[9] The IHE Advanced Patient Privacy Consents profile (APPC) is a standards-based option that can be implemented to transport structured policies reflecting these patient choices (IHE, 2019).[10] Retrospectively, through the eConsent application, the patient is able to view who has accessed which records and when.

Patient-to-Many Model

Consent in today's U.S. healthcare system is no longer based solely on a single patient-provider relationship. A patient who receives care from multiple providers across an integrated health system, for example, should be

[5] Point-of-Care Partners [POCP]. (2020a). Interview with a hospital medical director who is also a professor of medicine. POCP. (2020b). Interview with an emergency department physician.

[6] Proxy Consent. (1993). Law and the Physician Homepage. LSU.edu

[7] Brandner, A. et al. (2016). The Patient Portal of the Personal Cross-Enterprise Electronic Health Record (PEHR) in the Rhine-Neckar-Region. Exploring Complexity in Health: An Interdisciplinary Systems Approach, A. Hoerbst et al. (Eds.)

[8] POCP. (2020b). Interview with an emergency department physician.

[9] Heinze, O. & Bergh, B. (2014). A model for consent-based privilege management in personal electronic health records. *Stud Health Technol Inform, 205*, 413-417.

[10] Integrating the Healthcare Enterprise [IHE] (2019) IHE wiki advanced patient privacy consents

able to grant privileges at the practitioner, department or organization level instead of having to identify each individual provider.[11] A patient-to-many model for eConsent is especially useful when urgent care or emergency admissions leading to intensive care are necessary. The U.S. healthcare industry's shift to value-based care delivered via Accountable Care Organizations and Patient-Centered Medical Homes makes the patient-to-many model an imperative.[12]

Shared Decision-Making Support

Education and interactive discussions leading up to the eConsent process for a particular type of disclosure (e.g., advance care planning, health information exchange) are essential to ensure the patient comprehends the extent and implications of the consent being considered. An evidence-based, transparent and collaborative informed-consent framework is composed of interpersonal coaching on disclosures and consent, as well as multiple conversations with members of the care team and interactive, online educational materials.

The education and coaching for informed consent are provided with a focus on the documents to be disclosed and, when applicable, in the context of the patient's healthcare evaluation and treatment, along with the benefits and risks associated with granting or denying consent. This new approach to eConsent leads to better comprehension of informed consent. Patients show a higher level of trust and engagement in shared decisions, which can result in better health outcomes.[13]

Strong and Trusted Version Control

A single incident in which an outdated eConsent or associated document (e.g., Advance Directive) is acted upon is all it may take for patients and their care teams to lose confidence and trust in the eConsent system. Accurate, up-to-date and reliable version control is therefore imperative, and a single, centralized directory – containing an audit trail of all eConsents for an individual – is critical to achieving such control. The transparency attributes of blockchain technology, specifically its ability to provide a secure and auditable ledger of transactions[14] may provide the infrastructure needed to support this objective.

A centralized directory containing the locations and versions of eConsent records, as well as related documents, is vital to a distributed model of storage. Gaining the acceptance of health systems to track eConsent and related documents stored elsewhere is a major challenge.[15] For example, a model based on a centralized directory and decentralized document storage would allow custodians of advance care plans to manage those documents to comply with organizational policies or government regulations, while the directory could enable community-wide access to the most-current version. For transparency and auditing purposes, a trail of updates and previous versions would be available.

Best Practices for Usability

Four best practices are essential for gaining acceptance of the eConsent system and supporting implementation of the CSFs summarized above.

First, the eConsent application must be platform-agnostic, i.e., able to operate on mobile devices and computers supporting various commercial operating systems. Ideally, versions of the eConsent user interface and content are available for use by people without access to broadband Internet and/or who have limited computer skills.

Second, the user interface should comply with the most-current version of the Web Content Accessibility Guidelines (WCAG) to provide access for people with disabilities. The WCAG principles are that access should be perceivable, meaning different alternatives are offered for seeing and hearing content; operable, so there are various ways to navigate; understandable; and robust, including by being compatible with current and future user-interface

[11] Brandner, A. et al. (2016). The Patient Portal of the Personal Cross-Enterprise Electronic Health Record (PEHR) in the Rhine-Neckar-Region. Exploring Complexity in Health: An Interdisciplinary Systems Approach, A. Hoerbst et al. (Eds.)

[12] Campbell, K. & Parsi, K. (2017). A New Age of Patient Transparency: An Organizational Framework for Informed Consent. ***The Journal of Law, Medicine & Ethics, 45***, 60-65.

[13] Campbell, K. & Parsi, K. (2017). A New Age of Patient Transparency: An Organizational Framework for Informed Consent. ***The Journal of Law, Medicine & Ethics, 45***, 60-65.

[14] Yaqoob, I. et al. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. ***Neural Computing and Applications***.

[15] Point-of-Care Partners [POCP]. (2020a). Interview with a hospital medical director who is also a professor of medicine.

technologies.[16] Falling short on any of these WCAG principles can unintentionally exclude significant numbers of patients from having access to the eConsent application.

In addition, to be understood by diverse populations, content should be developed to support different levels of computer and health information literacy. For example, an educational module explaining the purpose of the eConsent application should be shaped for an individual with a fifth- to eighth-grade education level[17] and users should be enabled to set their own pace for consumption of content.[18]

The review of each topic within the module should offer a series of branches to more in-depth material intended for anyone wanting to understand more-detailed or complex aspects of consent in the particular area of focus (e.g., sharing health records across a health information exchange). As a patient takes an online education module, direct and synchronous access to a professional qualified to answer questions is critical to comprehension. [19]

Finally, to further comprehension and recall, the end-user should be given the opportunity to complete a self-assessment of the educational content.[20] If completed, it should be logged for access by authorized persons such as eConsent program managers, quality-assurance personnel, etc. as a means of assessing the effectiveness of the content.

The above precepts lay out a very high standard that can best be met by a single or small number of utility vendors, as meeting these standards would impose a heavy burden on each individual information-sharing system.

Service Implementation Considerations

The consent service itself should be implemented in a way that allows it to operate in a variety of contexts, avoiding dependencies on particular technologies and product offerings as much as possible. This allows development and replication with fewer technical restrictions and vendor preferences. Consent service implementation non-functional requirements should include:

[16] W3C Web accessibility initiative (2019). Accessibility principles. Zahra, S.A. ed.

[17] Ramos, S.R. (2017). User-Centered Design, Experience, and Usability of an Electronic Consent User Interface to Facilitate Informed Decision-Making in an HIV Clinic, CIN

[18] Coughlin, C. (2015). ECONSENT: CAN INFORMED CONSENT BE JUST A CLICK AWAY? Wake Forest Law Review, 45, 381-397.

[19] Ramos, S.R. (2017). User-Centered Design, Experience, and Usability of an Electronic Consent User Interface to Facilitate Informed Decision-Making in an HIV Clinic, CIN

[20] Coughlin, C. (2015). eConsent: Can Informed Consent Be Just a Click Away? Wake Forest Law Review, 45, 381-397.

- Ability to run and easily scale within a variety of available cloud environments and upon underlying operating systems.
- Ability to run locally in a non-cloud environment, offline and on a limited scale, for development purposes and testing.
- Ability to quickly "stand up" a basic consent service in as few steps as possible; and
- Free, open-source software licensure to promote reuse and innovation.[21] This is not related to fees a Consent Service Utility implementer may charge a hosted customer.

Informed consent is becoming increasingly complex as the digital exchange of individuals' confidential information expands. Efforts to deliver healthcare and social care in integrated, coordinated models adds to this complexity.

The ongoing migration of paper-based informed consent to electronic consent is necessary in the era of digital health and value-based care. However, success is not guaranteed.

An eConsent system model that has as its pillars the five critical success factors described above has the potential to enhance appreciation for, and engagement in, truly informed consent for releasing information and authorizing treatment.

As we begin to seriously implement the coordination of care across disciplines and domains, to improve outcomes and eliminate repetitive processes, it is critical to create a systematic way to share consent across the various services involved. Whole patient care coordination will only be successful if the technology standards and infrastructure are in place to enable providers to abide by the applicable laws and regulations governing privacy protections, as well as to make it easy for clients to authorize or decline the sharing of their information.

[21] Open Source Initiative, "Open Source Licenses by Category," https://opensource.org/licenses/category

History of Consent in Healthcare

Informed consent in healthcare is defined as a record of a healthcare consumer's choices that permits or denies identified recipient(s) or recipient role(s) to perform one or more actions, within a given policy context, for specific purposes and periods of time. There are four types of informed consent in healthcare:

Privacy. Agreement to collect, access, use or disclose/share information.

Medical Treatment. Agree or refuse to undergo a specific treatment/procedure.

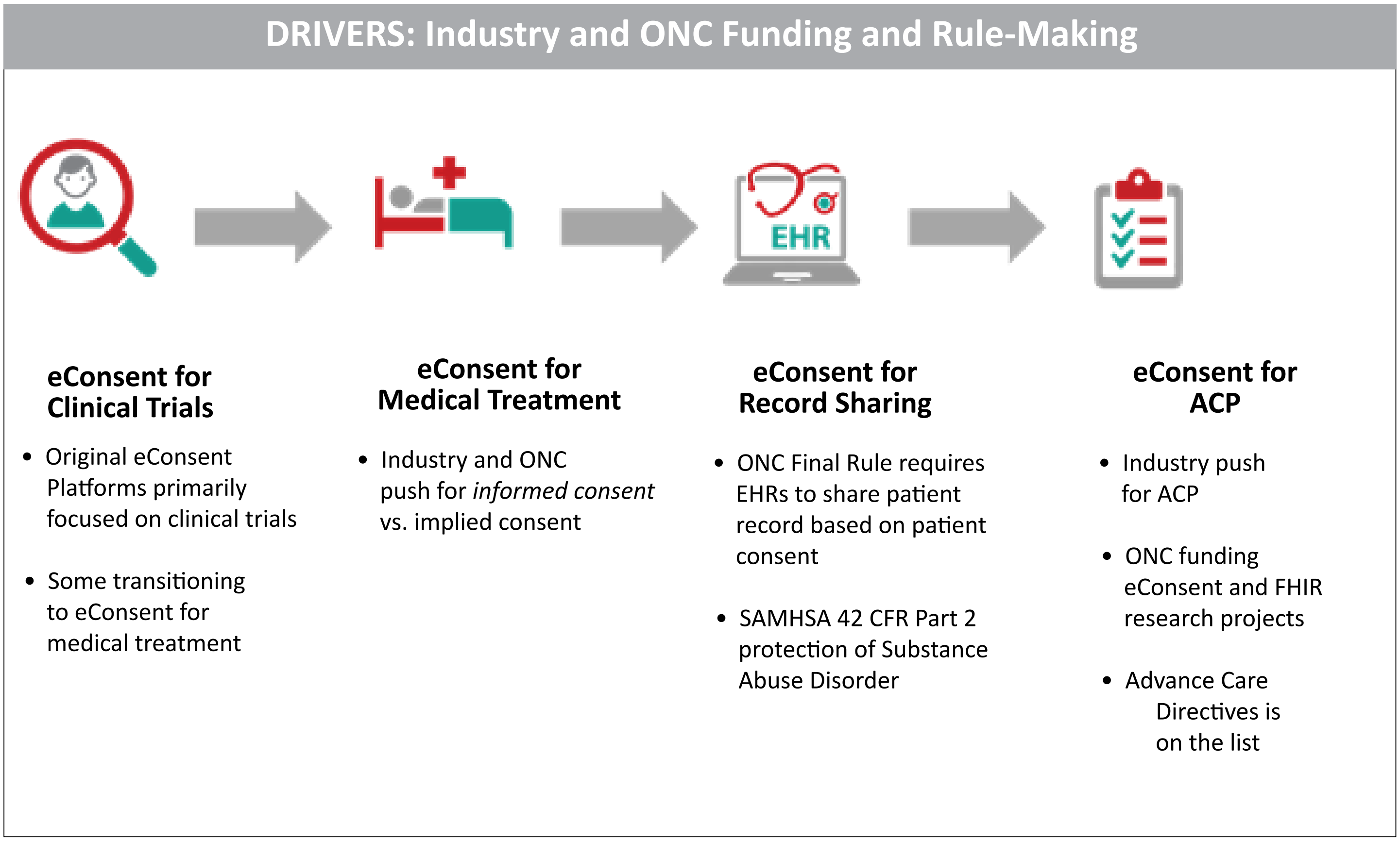
Research. Agree to participate in a study or clinical trial.

Advance Care Directive. Specifies future treatment if the patient is incapacitated.

Looking at a historical view of eConsent in healthcare, the original eConsent platforms focused primarily on consent for clinical trials. The informed-consent process for clinical trials had been paper-based.

But, given the increasing complexity of clinical studies – along with challenges faced by clinical trial companies with respect to quality, compliance, patient understanding and trial retention – the industry moved to a technology-supported eConsent process. The intent was to empower patients and their caregivers to make better, more-informed decisions and create process efficiencies for sites, Health Authorities, IECs/IRBs and sponsors.

Industry pressure, as well as ONC funding and regulatory rule-making, are leading to advancements in the healthcare eConsent industry. (See the graphic below.)



DRIVERS: Industry and ONC Funding and Rule-Making

eConsent for Clinical Trials

- Original eConsent Platforms primarily focused on clinical trials
- Some transitioning to eConsent for medical treatment

eConsent for Medical Treatment

- Industry and ONC push for *informed consent* vs. implied consent

eConsent for Record Sharing

- ONC Final Rule requires EHRs to share patient record based on patient consent
- SAMHSA 42 CFR Part 2 protection of Substance Abuse Disorder

eConsent for ACP

- Industry push for ACP
- ONC funding eConsent and FHIR research projects
- Advance Care Directives is on the list

CREDIT: ONC LEAP Consent Project

Ethical Concerns, Challenges, Benefits

Stewards of Change Institute and its partners embarked on this project, as well as related efforts to improve consent processes, because we strongly believe that doing so will contribute over time to systemic, significant progress on a variety of issues that are cited throughout this document.

They include better care coordination and outcomes; fewer socioeconomic disparities and greater health equity for disadvantaged communities; increased trust and understanding between those providing and recieving services; more-efficient and effective procedures; and lower costs, among others.

While we clearly see the benefits of this work, however, we also recognize that there are ethical concerns that need to be understood and addressed in any effort that involves people's sensitive personal information. Similarly, while there's broad consensus that securely sharing such data among the "right" professionals is the right ultimate objective – with consent playing a key role – there's equally broad recognition that the road to getting there is strewn with challenging legal, technical, organizational, cultural, policy and procedural hurdles.

Ethical Concerns

Potentially Negative Consequences of Sharing Information. Beneficence is a guiding ethical concept in human-subject research; essentially, it suggests that participants in a study or clinical trial should benefit from it (a corollary of which is "do no harm"). That principle is not usually explicitly addressed in work relating to security, regulatory compliance and other aspects of privacy, consent, information sharing and data-use agreements.

The result is a significant risk of causing unanticipated or unintentional harms, including ones that might result from an action for which informed consent was given. Thoughtful, well-constructed governance and transparency are therefore key to mitigating the possibility of negative consequences; in addition, the individuals whose information will be shared should be able not only to provide consent at a point in time, but also to:

- Review the record of their data as it is exchanged through various phases and be permitted to revoke consent at any time.
- Review clear documentation of the ways their data have been coded and integrated with other data.
- Object to classifications, logged records and specific uses of their data.
- Request changes to and deletion of any inaccurate information.
- Be alerted to the possibility of false positives or negatives in identity matching, and be able to review and contest such matches. This should also apply to the other person(s) whose identity is being confused, conflated or mistakenly matched in the process.
- Monitor and comprehend the ways (for institutional users) in which aggregate data is used in algorithmic decision-making processes and predictive analytics.

Understanding Stigma and Other Sensitivities. To the extent that health and social services integration includes child welfare and substance use disorders (SUDs) – which, together, affect millions of children and families – consent issues should be understood in a context of stigma, disincentives for self-reporting clients' needs, treatment effectiveness, and the risks of data being used by external systems. The role of the family/dependency court systems is also significant as they affect ultimate child welfare outcomes such as reunification or termination of parental rights. These include:

- An ongoing discussion in which terms are used like "replace the child welfare system" rather than reform it, citing "over-surveillance" of racial groups as a diversity/equity issue that causes disproportionate removal of Black and other minority children.
- The deep stigma attached to drug-using parents, including laws in half the states that define prenatal substance use as formal child abuse reportable to child welfare, which creates a significant disincentive for parents to self-report or consent to reports about their need for treatment because of a fear of child removal and/or incarceration.
- Inconsistent judicial rulings regarding persons with SUDs who are complying with prescribed medication-assisted treatment, but who are assessed as non-abstinent and thus non-compliant.
- The publicity given to recent breaches in data system security, leading to hundreds of thousands of records becoming available to unauthorized users and ransom-seekers.

The practice experience of InCK sites with consent issues in their present form may inform the need to respond to these issues. Some sites, including New Jersey, have developed drop-off analyses that track screening, referrals, enrollment and successful participation in services, which can document clients' willingness and ability to access and use services once consent has been given across agency lines.

Challenges

Potential Coercion. At-risk, dependent and/or vulnerable populations can perceive that they must provide their consent for information sharing in order to receive critical services. It is therefore crucial to assess and analyze all consent language and models to build trust and guard against explicit or implicit coercion. At a minimum, this should include testing for meaning and intention in the various forms of communications that accompany consent services or apps.

Limits in Communicating Consent Data. While consent functionality enforced by proprietary code is common within health IT systems, open-source and open-standards consent technologies lack broad adoption within health IT systems, and consent data is rarely communicated across systems. A good deal of clinical data exchange across systems falls under HIPAA's treatment, payment and operations (TPO) provisions, which allow healthcare data to be shared for TPO purposes without express patient authorization (consent).

'Indeed, many patients/clients already don't read through the sweeping "all-or-nothing" permissions they're currently asked to sign in medical offices, social service agencies, schools and other settings.'

While some systems are piloting efforts using a FHIR resource to communicate consent data, relying on an external utility to enforce consent and enable or limit data sharing is not a norm for health IT systems or providers. Moreover, while FHIR use is part of the Gravity Project's Implementation Guide for referrals to human services, clinical to human services closed-loop referral is a subset of potential use cases to address an individual's health and well-being.

Ensuring Revocation Reaches Those Who Need to Know. When a HIPAA authorization to share PHI is revoked, each entity authorized to use or disclose that information has the legal obligation to communicate the revocation to all its downstream business associates. That means, if a patient uses a provider's portal to revoke HIPAA consent, it not only impacts consent within the EHR, but also any re-release of the data by any technology microservice that is part of the EHR, provider or health IT system acting under that authorization. Without embracing a common standard or a consent utility, each system must devise its own way of contacting subcontractors about not re-releasing the data of a patient who revokes consent.

Because software today is built by getting a piece from this vendor and a library from that vendor (a microservices approach), this problem is bigger than any one patient having to manage multiple logins for each Patient Health Record used by each provider. In other words, because so many systems access data as part of care delivery, it is incumbent on every involved entity to communicate revocation to its subcontractors (and their subcontractors) because it's not feasible for even the most tech-savvy patients to do so themselves.

Preventing Consent Overload or Fatigue. It's clear from nearly all aspects of our scan that a critical goal, in healthcare and other domains, should be to empower individuals to provide (or deny) consent with increasingly greater granularity. Enabling them to pick and choose which specific data they want to share, with whom and under what circumstances – while also giving them the ability to change their minds at any time – could feel onerous to some people.

Indeed, many patients/clients already don't read through the sweeping "all-or-nothing" permissions they're currently asked to sign in medical offices, social service agencies, schools and other settings. Researchers, practitioners and others developing and implementing more-granular consent processes need to be acutely aware of this risk and act at every stage to make consents as "user-friendly" as possible and to minimize potentially negative impacts.

Benefits

Establishing, standardizing and expanding computable/digitized consent-related processes, as well as improving the ability to track them across healthcare and social/human services, will help to remediate or resolve an array of long-standing problems; here are a few examples of areas in which substantial progress could be achieved:

Cut Down on Wasted Time and Duplicative Services. Across clinical and human services providers, there isn't an easy way to track and share consent and accompanying records, which means patients/clients may spend more time providing their information (multiple times) and/or retaking assessments. This can mean filling out new intake forms for a new provider or, for someone who experienced trauma, having to retell their story, potentially retraumatizing them. These processes could be minimized if there were more comprehensive adoption of common, open standards for electronic consent and the exchange of associated records.

Enable Better Care Coordination. Efficacious care coordination is currently impeded from coast to coast every day due to the challenges of securing informed consent, thereby complicating or stymying efforts to provide more-holistic, person-centered services. A lack of care coordination also undermines efforts to streamline processes, control costs, implement best practices and, most importantly, promote optimal outcomes for individuals whose data needs to be shared.

Accelerate Focus on and Integration of SDOH Data. For stakeholders seeking to address SDOH, a lack of data interoperability means that assessments remain the primary means of measuring patient social needs. Typically, providers today target a program to a limited patient demographic (e.g. Medicaid or dual-eligible recipients), leaving large swaths of the patient population with unmet social needs. Improving consent and data interoperability across healthcare and human services providers would enable cross-domain care teams to more-readily target programming to patients shared across their systems, while lessening the need for assessments when that data could be shared (with consent) from partner organizations.

Increase Cross-Sector Understanding, Cooperation and Collaboration. CMMI has funded programs like InCK to reduce out-of-home placements by improving care coordination across core relevant domains such as schools, child welfare systems and others. Child-level data is needed from each of those systems to identify individuals who are at risk, provide interventions and measure their impact. A Consent Service Utility could enable and expedite this type of data sharing across domains possible, a critical aspect of offering whole-person care.

Voices from the Community: Consent Should Be about Relationships and Trust as Well as Processes

During the summer of 2021, the nonprofit Center for Democracy and Technology (CDT) held an online series of convenings with subject matter experts nationwide to discuss the critical importance of community engagement when shaping best practices in the sharing of personal information across sectors. Their specific focus was the sharing of educational data, but most of the lessons learned during CDT's project are directly applicable to this report on consent-related efforts in the U.S., which are obviously intended to enable and expand the sharing of information across numerous sectors in addition to education (i.e., healthcare, social services, etc.).

A draft of the report CDT is preparing about its project includes the following sentence about the core reason for community involvement at every stage of developing and implementing policies and practices related to data sharing: "This population has the greatest stake in the success or failure of a given data sharing initiative; as such, public agencies have a practical incentive, and a moral obligation, to engage them regarding decisions being made about their data."

The draft report also emphasizes a significant caution relating to sharing information, one that is also front-and-center in the work we've conducted for this consent report; that is, the risk that some data is biased (or just of poor quality) and that some data sharing could have harmful effects as well as positive ones. Furthermore, the draft language adds: "Data sharing that takes place without the knowledge or consent of parents and students, or data that is used for a different purpose than originally planned and to which the subject did not consent, increases the likelihood . . . of misuse and damages the trust of the community with whom agencies are working."

[The CDT expects to complete its guidance document in late 2021; once it is published, we will add it to the Resource section of this online report, which is Appendix D. The subject matter experts who participated in the CDT project included Daniel Stein, President of SOCI.]

Against this backdrop – and because we steadfastly believe community engagement and the remediation of systemic bias and inequity are vital for our own work and far more broadly – we interviewed members of the Bronx Community Research Review Board about this report and some of the issues it addresses. The BxCRRB's mission is to "eradicate health inequities" in marginalized communities in the Bronx. We chose the Bronx for these interviews because it is the site of one of SOCI's partners in its consent work, the federally funded Integrated Care for Kids (InCK) project.

> **'There's no such thing as a single-issue struggle because we do not live single-issue lives," said one.'**

> **'Added another: "It should be about relationality, relationality, relationality. . . Data is not going to matter in the absence of remediating harm and shaping relationships.'**

This report is primarily about legal, technical and process-related considerations relating to consent. We thought it important to include this section on community-based observations and insights, however, as a first step toward far greater involvement by "people with lived expertise" (admittedly an imprecise term) in any subsequent planning or action steps we take as a result of what we've learned in conducting our scan and writing this report.

> **'And this third comment: "If I can't have an interactive relationship, I don't want it.'**

We interviewed BxCRRB Board members Michael Williams, LMSW, Chairperson; Dr. Monique Guishard, Vice Chairperson; Allison Cabana, Secretary; Dr. Devin Heyward; Dr. Lucretia Jones; and Dale Miller; as well as BxCRRB member Jewel Weber Brown. Their key points relating to consent, all of which were interrelated, included:

- Consent isn't just about the individual being asked to provide it. Though it is often viewed and treated as a process affecting just a person filling out a form, that individual may have family members with whom they want to discuss whatever they are being asked to consent to – and who could also be significantly impacted by the consent. That means the patient/client needs time to go home, think and talk, rather than having to immediately sign on the dotted line.

It is not just an individual's relationships with family and other important people in their lives that needs to be seriously considered; it's also their interactions with their doctors and/or other service providers. In other words, the consent process should also factor in the need to build relationships with those professionals, so they're about trust as well as transactions, and not just be about legal and technical issues.

- **It's a big problem if consent moves primarily to apps**, especially for people in disadvantaged communities who might not own smartphones, who don't have adequate wireless services and/or who lack technical knowledge. For them, paper may be preferable to electronics for other reasons as well, perhaps most significantly so that they can take the forms they've been given home, where they can read what they say, think about the benefits and risks of sharing their information and then decide whether they want to sign.

  Whether the consent forms and related materials are on paper or on a device, it's critical that they be written in language that is easily understandable and as devoid as possible of specialized (ex., legal or technical) wording or jargon. The information provided should also not assume the person reading it understands the functions or processes of the institutions that might be involved in the exchange of their personal information.

- **Professionals don't always understand the** implications and consequences of their requests for consent, whether for treatment, participation in a clinical trial or the sharing of personal and frequently sensitive information. In other words, they view the process as purely transactional – you sign here now and then we'll provide a treatment or a service. "It becomes sort of rote," said one of the interviewees.

  The patient/client, however, may reasonably wonder how and with whom their information will be shared (perhaps a service provider who they know harbors a racial bias?) as well as what the consequences may be (ex., if a years-old court record is shared with a child welfare worker). So the consent process needs to include clear explanatory language and thoughtful conversations to ensure the individual is genuinely informed.

- **There's an inherent power imbalance between** the people giving or denying consent – generally, but especially in marginalized communities – and the professionals providing social services or medical care. That means patients/clients can feel intimidated into approving the sharing of their personal information or believe (often rightly) that they have to do so to receive the treatment or service they require. So, consent-related policies and practices need to recognize this reality and mitigate its potentially negative impact.

  The professionals involved not only need to think less transactionally, but also should offer information aimed at ensuring that their clients/patients clearly understand the benefits of providing consent as well as any risks involved, again to ensure the individual is truly informed before making a decision. For example: "Will the person be notified each time someone asks for their record? If not, that should also be in the consent."

- **A history of racism and socioeconomic disparities** means the perspective of individuals being asked to provide their approval isn't shaped only by the questions relating to consent and information sharing per se. Rather, it's also based on personal and historical experience. So, for example, will they believe that all the people they're dealing with – or the ones receiving their data – have their best interests at heart? Will that information be properly used? Who will the real beneficiary be, the patient/client or the institutions requesting the consent and participating in the sharing?

The interviewees agreed that three keys to making progress on consent – and many other issues – are having a broad context, building trust and understanding the value of relationships.

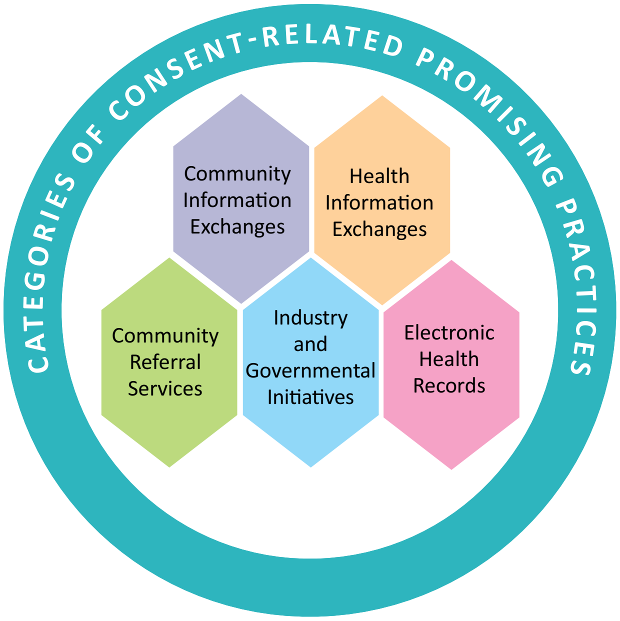
"There's no such thing as a single-issue struggle because we do not live single-issue lives," said one. Added another: "It should be about relationality, relationality, relationality. . . Data is not going to matter in the absence of remediating harm and shaping relationships." And this third comment: "If I can't have an interactive relationship, I don't want it."

Promising Consent-Related Practices

In conducting its nationwide scan of efforts to improve consent-related processes, SOCI and its partners identified numerous governmental and business-sector organizations engaging in promising practices. For the purposes of this report, that means they have created, are creating or are now using digitized/computable consent systems (as opposed to paper-based ones) that hold the promise of:

- Significantly enhancing operational efficiency and effectiveness, including by improving the secure cross-sector sharing of personal information.
- Giving individuals greater, more-granular control over who can access their personal data and under what circumstances.
- Demonstrably contributing to progress toward greater health equity and better outcomes related to health and well-being.
- Furthering cross-domain partnerships, creation of more-comprehensive patient/client records and/or better care coordination that addresses SDOH.
- Containing approaches, technologies and/or additional elements from which other organizations can learn, so they can initiate and/or improve their own consent-related processes.

It is important to emphasize that the systems, projects and other efforts described below are not the only ones devising and implementing promising practices; rather, they are examples of such work, which we've sorted into four "categories:" **Health Information Exchanges** (HIE), **Electronic Physical and Behavioral Health Record Systems** (EHR), **Community Referral Services** (CRS), and **Community Information Exchanges** (CIE). One additional category, **Industry and Governmental Initiatives**, focuses on examples of federal or industry-supported efforts that have highly applicable learning related to consent.


CATEGORIES OF CONSENT-RELATED PROMISING PRACTICES
Community Information Exchanges
Health Information Exchanges
Community Referral Services
Industry and Governmental Initiatives
Electronic Health Records

Our scan of promising practices included interviews with about two dozen senior officials of 13 organizations in the five categories, as well as an examination of materials on their websites and/or that they provided separately.

We also received extensive input from dozens of legal, technical and subject matter experts from around the country and across numerous disciplines and domains, all of whom volunteered time over several months and shared their knowledge of this work; we extend our deep gratitude to every one of them. Finally, we reviewed additional research and other online resources relating to the specific work of organizations in each category and to each system type more generally. Appendix D contains a sampling of resources relevant to consent, including ones pertaining to these highlighted systems.

Health Information Exchanges

The scan we conducted for this report indicates that HIEs – and, increasingly, CIEs (discussed below) – are at the forefront of promising practices that others can learn from, adopt or adapt. Broadly speaking, a growing number of HIEs appear to be making strong progress in securely sharing sensitive information, including by modernizing consent processes. So we're starting this section of our report with HIEs because they offer important insights that could be applied to ingesting and sharing data from and across other domains in addition to healthcare (ex., education, justice, housing and others).

An HIE is a type of software system that enables the broad exchange of patient health information. Patient records are shared with healthcare providers and, slowly but increasingly, so are SDOH and social services data. Information is shared through network-connected, enterprise-wide information systems or other data networks and exchanges. A large majority of U.S. residents have at least some of their information shared by an HIE.

A given HIE may manage a range of data, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics and billing information. Many of these data elements are considered Personally Identifiable Information (PII), the protection of which is governed by multiple industry rules and standards; in addition, Protected Health Information (PHI) is covered by the privacy protections of HIPAA, and some elements may also be covered by 42 CFR Part 2, a federal regulation that provides heightened protections for information related to SUDs.

HIEs Interviewed

- Bronx Regional Health Information Organization (RHIO)
- Chesapeake Regional Information System for Our Patients (CRISP)
- San Diego HealthConnect

HIEs Reviewed

- Michigan Health Information Network (MiHIN)
- Civitas Networks for Health – Merger of Strategic Health Information Exchange Collaborative (SHIEC) and Network for Regional Healthcare Improvement (NRHI)
- CyncHealth (Nebraska)

Consent is often required to enable access to sensitive information within an HIE or the exchange of such information between an HIE and another IT system. HIE systems implement services to manage the consent assertions associated with a patient's records. Often this is simply binary; that is, opt-in or opt-out of sharing information with all HIE participants, possibly including some role-based controls to ensure that only the minimum necessary information is shared with a particular person (e.g., clerk vs. doctor).

In these binary approaches, particularly the opt-out systems that presently dominate, information that is highly sensitive or intentionally protected under a particular law is generally excluded, limiting the utility of the HIE. The examples given below demonstrate how some vendors are increasing the sophistication of their systems to allow for the appropriate sharing of more-diverse information, including highly protected health data.

Key Information and Insights

- By their very nature as aggregators, HIEs are EHR agnostic. Most take data feeds from dozens of different EHRs – and sometimes Behavioral Health record vendors – using HL7 version 2 messages and/or version 3 consolidated Clinical Document Architecture (CDA) feeds. These standardize the data coming from different systems to allow for mapping, display and analysis of the data using normalization algorithms.

- The challenge for HIEs in expanding data ingestion to SDOH-related domains is that standardization of education and/or social services data is either different from HL7 standards or has not yet undergone the process of standards development for and use of their data. Implementation is therefore often unique, with each HIE independently mapping data for its warehouse and use by its clients; this is done locally, so each one may do it differently until standards are defined and implemented for every domain.

- As aggregators of health-related data – and in small but growing numbers, SDOH data – HIEs can facilitate the sharing of information across systems and domains. The records of patients who change providers or are referred to a specialist, for example, can be viewed or obtained through the HIE from all providers rendering care or services at once, eliminating reliance on patients' recollections of where they were treated and the cumbersome process of requesting copies of medical records from multiple sources.

- Though there is state-to-state variation, patient identity and consent management are core functions of most HIEs; that makes them ideal candidates (and perhaps models) for enabling and supporting data management across domains and sectors. The linkage of an individual's records for all their providers requires sophisticated software algorithms and related human processes to ensure all the linked information is truly the same person's. So this infrastructure could readily be expanded for sharing an individual's data across health, education, social services and other relevant systems/domains.

- HIEs generally operate on either an opt-in or opt-out framework, based on their business needs and/or state regulations. Even in opt-in models, however, only limited data, such as in-patient admission notifications, may often be sent to providers with treatment relationships with patients without affirmative consent on record at the HIE.

Opt-In models encompass affirmative consent for the sharing of sensitive data, including Part 2, HIV and other locally defined sensitive data types. In the opt-out model, affirmative consent must be obtained for sharing Part 2 and other sensitive data, which becomes a complicated, cumbersome process that most providers do not conduct. As a result, providers are often unaware of substance use by patients or services that may be affecting their physical or other behavioral health treatment and care plans.

- In the technical framework at HIEs that create a data repository, information of various types (relating to Part 2 and other sensitive data) is tagged to enable its segregation. This tagging enables implementation of rules governing when and with whom the tagged data may or may not be shared. For example, in New York State's opt-In model, alerts generated at a Part 2 treatment location may not be sent without recorded affirmative consent; existing HIE technology applies this rule to the tagged data.

  This ability to tag data on ingestion could be extended to other domains, such as education or child welfare, with the requirement of affirmative consent to share. This construct makes HIEs a natural platform for integrating data from a wide variety of sources across many domains, tagged based on the rules from non-healthcare domains, and exchanged accordingly.

  It should be noted that not all HIEs have data repositories. Those that do not: 1) may have a repository of clinical documents whose integrity cannot be tampered with; 2) take multiple clinical documents for a patient and combine them into a consolidated CDA document (where there may be an opportunity to filter data based on tagging if policies, laws, and use cases allow it); or 3) move data around without ever looking at what's inside the package and therefore could not tag data at all. HIEs of those types may need to use different strategies to capture and implement consent directives.

- HIEs are highly capable of providing community-wide services for emergency response and public health, situations where important SDOH data can inform actions. For example, HIEs are used to help police locate missing persons who may have been taken to hospitals in the aftermath of disasters such as fire, floods, tornadoes, etc.; to locate patients moved from nursing homes to other venues; and/or to provide medical histories to providers for emergency triage or care provision. In addition, HIEs are often the source of identification so next of kin can be notified.

  During the COVID-19 pandemic, HIEs have provided critical data to public health agencies about who has tested positive and contact information for tracing those exposed, as well as for tracking vaccinations, hospitalizations and deaths. If public health agencies could have accessed SDOH information from HIEs, such as high-quality race and ethnicity or census tract, income and household size and composition data – along with the clinical data described above – it would have greatly improved their ability to plan for safe, readily obtainable testing in the highest-risk areas.

  That would have been beneficial because, for example, socioeconomically disadvantaged individuals are less likely to have cars, especially in cities, so they cannot take advantage of such services as drive-through testing or distant vaccination sites. Moreover, those with young children often cannot easily access services because no childcare is available either at home or at the testing/vaccination site. Inclusion of this social information, integrated with health data in HIEs, would enable dramatic improvements for public health response planners.

- The 21st Century Cures Act explicitly promotes the sharing of patient data through the use of ONC's Certified EHR Technology (CEHRT) applications and other methods. As a result, HIEs nationally are expanding their interface abilities to respond to FHIR queries for specific and limited data, as well as to generate and respond to queries from national data-sharing networks such as eHealth Exchange.

  Many of these exchanges will take place within the Trusted Exchange Framework and Common Agreement (TEFCA) infrastructure, which was designed by the ONC to create an infrastructure model and governing approach for national information exchange.

Working within TEFCA, HIEs will still generally focus on increasing their capacity to move non-protected health information among a wider group of providers, but will also have the potential to become more granular and sophisticated in doing so. They may also be able to use the same mechanisms to incorporate and share SDOH data by applying the rules relevant to the various SDOH domains.

The following are brief descriptions of some of the HIEs examined during our scan, along with key points made in interviews with officials/leaders of each organization:

Bronx Regional Health Information Organization.
Bronx RHIO is an HIE established by leading healthcare organizations in that borough, including hospitals, health systems, ambulatory care centers, home care and community organizations that now constitute the RHIO's membership. Its intent is to make it possible for patients' medical records to follow them for care throughout the Bronx. We interviewed Kathryn Miller, Bronx RHIO Chief Operating Officer. She said:

- Achieving consistent, reliable consent is a key to the successful implementation and realization of InCK goals. The Bronx RHIO is an InCK site and an SOCI implementation partner for its development of a Consent Service Utility.

- NY State law mandates that RHIOs obtain individuals' affirmative Opt-In consent to allow access to their data for each RHIO member organization. Members can then send any data they have to the RHIO without specific patient consent. That includes 42 CFR Part 2 data, behavioral health data, etc. This model is about to change, however.

  The new model will retain organization-specific consent, but it will add an option for patients/clients to sign a consent allowing the RHIO to share their data with all of their current and future healthcare providers and/or health insurance plans.

- Unlike the RHIOs in some other boroughs, the Bronx RHIO has included community organizations (which are non-covered entities under HIPAA) as members. That is accomplished by having those organizations sign an agreement requiring them to comply with HIPAA regulations and act in other ways as if they were indeed covered.

  The community organizations' use and protection of data is then subject to audit by the Bronx RHIO, and each organization's staff must take annual HIPAA training. All of Bronx RHIO's member organizations have complied with these requirements.

- Community organizations such as housing organizations and children's services have contributed new data inputs, such as program enrollments and disenrollments, visits where applicable, care plans from some, and assessments.

- The experience of the Bronx RHIO is that it's generally easy to get people to consent to sharing their data once the value of doing so is thoughtfully explained to them; this process is far more effective when staff members are trained on how to ask for consent as part of their workflow. Within the Bronx RHIO, an estimated 95-98 percent of patients say "yes" to sharing their information, and those who do not consent are likely being asked at a substance-use treatment facility.

- Verifying patient identity is at the core of all this work, and it's hard. Through its Health Information Management Committee, the Bronx RHIO recently initiated a new process for ascertaining and implementing best/promising practices on spelling names correctly and getting the right address for each individual.

- Bronx RHIO's work could be replicated and could handle the flow of all kinds of data. During the NYS Medicaid Design System Reform Initiative Program, Bronx RHIO initiated dozens of new data feeds from community behavioral health providers, including depression screening scores that had never before been sent/ingested. Shelter addresses also were mapped, triggering a flag to inform providers of housing instability. The RHIO is starting a project to bring in SDOH assessment data from its members.

Chesapeake Regional Information System for Our Patients. CRISP is a nonprofit organization that facilitates the electronic sharing of clinical information between disparate health information systems to facilitate care, reduce costs and improve health outcomes. CRISP is the state-designated HIE for Maryland, and CRISP DC is the district-designated HIE for the District of Columbia. We interviewed Adrienne Ellis, a Senior Advisor to CRISP. She said:

- CRISP has consent processes for specific use cases. CRISP has been working to enable patients to consent to share their SUD treatment information under 42 CFR Part 2 in collaboration with other HIEs and is now piloting a consent tool to accomplish that objective. Currently patients who sign a consent form agree to have a small subset of their Part 2 information shared with any provider on their healthcare team who participates in the HIE. CRISP is planning to go live in 2022 with a form that will permit patients to consent for their payer to see that same, small subset of Part 2 information.

- **CRISP DC** is conducting an innovative project, the Community Resource Information and Exchange (CoRIE), that addresses SDOH. This effort includes three elements: a community resource inventory; a tool for healthcare providers to make referrals to community-based organizations (CBOs) that provide social services; and integration with referral platforms to expedite data sharing back to the providers. An ongoing challenge is getting community-based organizations to accept referrals through the tool. Their voluntary participation is critical, so a substantial outreach effort is underway.

- CRISP in Maryland and DC routinely ask their members what their priorities should be. The sharing of substance use treatment information and expansion to SDOH information are at the top of the list.

- CRISP has a tool for healthcare providers to make referrals to select CBOs, social service agencies and health-promotion programs. HIPAA allows for minimum necessary protected health information to be shared by the healthcare provider if the provider believes doing so will result in a referral or service that improves a patient's health. Using this provision, CRISP enables its provider members to capture a patient's oral consent, for instance to make a referral to a diabetes prevention program; if the patient says "yes," the provider documents the consent in the tool, and a referral is sent.

- CRISP is in the process of describing use cases and user stories for community-based organizations and social service agencies to determine how they would like to interact with the HIE. These interactions may need to be facilitated by patient-registered HIPAA authorizations, which could be captured in the same tool being used for SUD consents.

- CRISP's consent tool is mapped to a FHIR standard and could be configured to record consent to share child welfare and educational data if those systems were interested in using the tool and sharing information protected by FERPA and/or other limitations. CRISP's experience is that schools are reluctant to share information, so it's critical to get them on board before expanding use of the tool.

- Major obstacles for CRISP have included:

    - It is difficult for many mental health and SUD treatment providers to share clinical data. Even when a solution is found (with middleware, for instance), the EHRs often are not able to segment or parse sensitive data.

    - Asking providers to add SUD consent capture to their workflows can be tough, because it entails asking a busy professional to do "one more thing."

- Some key lessons learned have included:

    - Make sure that policy and technology can align before implementation.

    - Make sure all players are on board and roll out slowly, before a lot of the technology has been built. Get feedback from users, conduct pilots and do user testing.

    - Establish a way to capture consent signatures during telehealth encounters.

San Diego Health Connect. This sophisticated, countywide nonprofit organization identifies itself as a utility that "unifies the San Diego healthcare ecosystem." Health Connect links providers, patients, private HIEs and others, with the goal of improving the quality and cost of care in the community it serves. The HIE grew out of its predecessor, the San Diego Beacon Community, as a result of $15.3 million in funding from the ONC in 2010.

San Diego County's principal health systems rapidly signed up with the HIE, and the number of participants has continued to grow. In early 2013, UC San Diego transferred operational and oversight responsibility for the HIE to San Diego Health Connect, an independent, non-profit 501(c)(3) organization. The federal grant provided a jump-start for the HIE and, as a result, it has progressed more quickly than most HIEs in its development and technological sophistication.

In August 2019, San Diego Health Connect was awarded a LEAP grant to develop a FHIR-based Consent Decision Service (CDS) and a Consent Enforcement Service (CES).

More information about LEAP is in the Governmental and Industry Initiatives section of this report. The grant was awarded to San Diego Health Connect to address the following workflows:

- **Privacy Consent Directive.** Agreement to collect, access, use or disclose (sharing).
- **Medical Treatment Consent Directive.** Consent to undergo a specific treatment (or record a refusal to consent), including for mental health issues and substance abuse.
- **Research Consent Directive**. Consent to participate in research protocol and required information sharing.
- **Advance Care Directive**. Consent to instructions for potentially needed medical treatment (e.g, Do Not Resuscitate).
- **Social Services Consent Directive.** Consent to collect, access, use or disclose (sharing) of information between social services agencies and community-based organizations.

Given San Diego Health Connect's consent journey and evolution, it was a particularly fertile setting for development of this effort. We interviewed Dan Chavez, the HIE's former Executive Director. He said:

- California permits providers in the state to choose whether they want an opt-in or opt-out policy for themselves. San Diego, as a matter of practice, is an opt-out county for purposes of exchanging medical information for treatment; in other words, everyone's data can be shared unless they explicitly indicate they want out.
- The County of San Diego decided not to collect consents, with the exception of mental health and SUD care programs. That said, if you sign up for a health-related county program(s) – except for those two – your permission to allow your data to be shared is assumed. The other exceptions are Department of Defense and Veterans Administration programs, which do not share information for public health purposes.
- Two challenges San Diego Health Connect has encountered are that there is no single, broadly accepted interpretation of HIPAA and, more broadly, of privacy; and that the many systems in the county don't all record and document consent in the same way. If the lawyers of our local jurisdictions, hospitals and clinics all interpreted HIPAA in a similar manner our policy challenges would have been much simpler. Additionally, if we could have predicted the variety of ways and manners that consent would have been documented and selected a more consistent, uniform manner of documenting consent, information sharing could have been much more streamlined.
- One reason for Health Connect's success is its explicit engagement with the Health Information Management (HIM) function, because the keepers of medical records are key to making interoperability and information sharing work; i.e., HIM departments know what goes on in institutions and therefore can play a pivotal (if unrecognized) role.
- The HIE was an early adopter and key innovator of pre-hospital reporting, which is the interoperability between Emergency Medical Services and ambulances in route to emergency departments. Given the setting, consent is not required to share data. This workflow automates ambulance records into the corresponding ED and hospital medical records. It is not clear whether patients are properly informed of this inclusion and possible downstream sharing and interoperability of the ingested ambulance records.

Electronic Health Record Systems

Electronic Health Record (EHR) systems, as well as related Behavioral Health Record systems, are a type of software that can be used by clinicians to collect and manage patients' physical and mental health information in a digital format in support of delivery and coordination of care.

These records can be shared across different healthcare providers and increasingly, along with SDOH data, with providers of social/human services.

Records are shared through point-to-point connections (e.g., Direct messages, proprietary secure email services, electronic facsimiles [fax], vendor-managed alerts with admission, discharge, or transfer information from a hospital or health system to the attributed primary care provider listed in the EHR system, HIEs, vendor-managed exchange (e.g., Epic CareEverywhere) or national networks (e.g., Carequality, eHealth Exchange, CommonWell Health Alliance).

EHRs manage a range of data including demographics, medical history, medications and allergies, immunization status, laboratory test results, radiology reports, links to medical images, clinical notes, risk assessments (e.g., smoking status, depression screening, SUD screening and vital signs). Any information in an EHR system that is identifiable to a person, including demographics, is considered Protected Health Information (PHI) that is covered by the privacy protections of HIPAA, and some data elements may also be protected by Title 42 of the Code of Federal Regulations Part 2 (42 CFR, Part 2), which mandates heightened protections for information related to SUD treatment.

In addition to Part 2 data, psychiatric notes have special protections from federal requirements relating to informed consent for disclosure, and the U.S. Veterans Administration and the Department of Defense require consent for sharing any medical records outside of their systems of care. There is a patchwork quilt of state-specific consent regulations for sharing information about certain health conditions (e.g., HIV-related, sexually transmitted diseases) and certain populations (e.g., minors).

Individuals provide their consent many times for many reasons during care for a complex medical condition or for a simple out-patient surgery. Consent forms are captured in different systems within a large health system or hospital.

A consent to request prior authorization of payment or consent for a payment plan, for example, might be captured in a referral management module and in a revenue cycle system, respectively. For the same hospital, a consent form for treatment in the emergency department may be in a different EHR system altogether than the consent form signed by the same patient for anesthesia and for surgery during the same medical encounter.

A request for patients to provide consent permitting their healthcare organization to share information with one or more named individuals on the HIPAA Notice of Privacy Practices (NPP) form is standard. And, while large health systems are increasingly moving to digital forms, smaller practices typically collect consent on a paper form when patients are checking in for a clinical encounter or getting a medical test or treatment.

Once that is signed, it may be scanned into the EHR or practice management system but, for many if not most organizations, that may be the last time anyone sees the form. EHR systems are known for their "flexibility" regarding where scanned forms can be stored, meaning scanned forms with important information – such as a person's Advance Directive or the Physician (or Medical) Orders for Life Sustaining Treatment forms (POLST or MOLST) – can be difficult or impossible to locate when needed in an emergency.

Furthermore, when an individual chooses to change the named individual(s) on an NPP form, or change treatment preferences in an Advance Directive, there's little evidence this change/revocation is captured in a way that replaces the previously scanned form, leaving organizations at liability risk. Healthcare organizations with multiple sites may have conflicting NPP forms from the same patient, all scanned into the organization's EHR system by different people, in different clinics, without any version control to ensure fidelity of a single source of truth stating a patient's wishes.

In the behavioral health domain, the issues are even more acute because there are many providers who either do not use an EHR system at all or use a system that has not been certified by the ONC for standard functionality. This gap in technology adoption by behavioral health providers is understandable given that a large number of mental and behavioral health providers are solo practitioners, and that the vast majority were not deemed eligible by CMS for incentive payments to adopt and use certified EHR technology.

Alternative payment models requiring more integration between primary care and behavioral health are increasing the interest in data exchange between these provider types, but a somewhat paternalistic culture in the behavioral health specialty area still causes many providers in this field to lock down client information without offering options for more whole-person care approaches.

Accelerating data sharing from behavioral health providers' EHR systems for better care coordination holds promise, as do other types of software designed for behavioral health and SUD treatment. Adoption and implementation will be slow for both providers and their behavioral health clients, however, without a highly trusted approach to community-wide consent management to give individuals more agency around how their data is shared and used.

EHRs Interviewed

- Cerner Corporation
- Omnibus Care Plan (OCP)
- Healthcare Information and Management Systems Society's Electronic Health Records Association (EHRA)

EHRs Studied

- Epic Systems Corporation
- Allscripts Healthcare Solutions
- FEI Systems

Key Information and Insights

- EHRs have internal consents but usually no means for external systems to query them.
- Consent forms and consented forms (e.g., assessments, advance care plans) can be difficult to find when paper forms can be saved in different places in an EHR system.
- EHRs vendors and health systems partner with external systems (e.g. Aunt Bertha, UniteUs and other health IT systems) to exchange data, but consent to do so is not bidirectional. There is an internal EHR process for information pushed (one way) to the external systems.

  Aunt Bertha, for example, has an internal system to push consent for information (also one way) to the EHR. The exchange requires two separate consent functions, as EHRs do not typically support one common consent service for use by all the interoperating IT systems (e.g. Aunt Bertha, UniteUs, etc.).
- EHRs sometimes have two-way exchange of consent information with HIEs, but usually they are just doing a one-way push of patient and consent data from the EHR to the HIE.
- With pen pad technology now offered by some EHR vendors to capture consent from patients at registration, there must be concerted efforts to ensure patients are not asked to sign a consent without being able to see what is in the form they are consenting to.
- Financial support for behavioral health practices to adopt certified EHR systems and care-coordination platforms is very much needed before consent for electronic data exchange of behavioral health records can even be considered.
- Trends to combine business and clinical consent requests into a single form in the EHR can cause patients to have anxiety about whether they can receive treatment without providing blanket consent.

The following are brief descriptions of some of the EHRs examined during our scan, along with key points made in interviews with officials/leaders of each organization.

Cerner Corporation. Cerner is one of the major U.S. suppliers of health information technology services, devices and hardware; the other major one is Epic Systems Corporation, followed by AllScripts Healthcare Solutions and many other Independent Software Vendors. Working at the intersection of healthcare and IT, Cerner provides tools to support the clinical, financial and operational functions of hospitals and health systems worldwide. We interviewed four senior Cerner officials. They said:

- Cerner's role regarding consent is helping to advance and manage patients' ability to specify/record what can or cannot be shared, as well as to work with the user and provider communities to further understanding of what works or doesn't and what national or state laws or policies apply to them, such as Part 2 and HIPAA.
- When Cerner discusses consent, its first question is usually what is specifically being sought; i.e., is it consent to treatment, to share data, to participate in a research study, to permit a telehealth visit to be recorded or something else?
- Cerner's global footprint has allowed it to see a variety of consent approaches, including novel ones "at the bleeding edge" – in particular to achieve

greater granularity in consent. It's clear that consent is moving away from black and white (opt-in or opt-out) and recognizing there are 50 shades of grey in-between.

- A big issue is determining how to coordinate care between community behavioral health clinics and hospitals, and to stop thinking about acute and non-acute care. This means improving information-sharing and the consent processes that enable it. It's important because, if the continuum of care starts with community clinics providing outreach and helping people early on, then fewer of them will wind up in the ER.
- Challenges today include:
  - Determining the level of granularity for consent to be workable and documentable, so the process can become more automated and streamlined for both SDOH and clinical data. The biggest questions are what SDOH data needs to be shared with EHRs, where in the workflow they fit and what kinds of legal agreements need to be in place.
  - Reluctance of some providers to participate in data exchanges because of the patchwork of regulations at every level, which lead them to involve lawyers to determine what can be shared, with whom and under what circumstances.
  - The lack of regulatory uniformity makes cross-domain very difficult and expensive. Cerner would prefer regulations that align to Fast Healthcare Interoperability Resources (FHIR) and Health Level 7 International (HL7) so everyone "can play ball with everyone else," but that's not the case today.
  - It is currently difficult to capture policies and information in a consistent, computable format, with common vocabularies, tagging and coding. Such consistency is needed to ensure agreement on what data is sent in and out and what it means. These kinds of discussions need to be had to make consent truly work.

FEI Systems. Founded in 1997 by Dr. Jiao Gu, FEI is a market leader in the digital transformation of health and human service delivery, focused on enabling integrated, accessible and quality service delivery to vulnerable populations. FEI provides its solutions in 40+ counties and states and seven Federal Agencies. We interviewed Bill Kowalski, Principal Business Development Manager at FEI. He said:

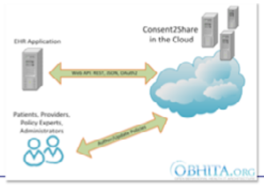
- FEI offers a proprietary suite of software solutions to support the full continuum of care in Behavioral Health, Home and Community-Based Services, and Long-Term Services and Supports (HCBS/LTSS). The LTSS platform, Carity, provides screening and assessment, waiver eligibility, service planning, service delivery, and claims and quality monitoring.
- FEI developed Web Infrastructure for Treatment Services (WITS), which focuses on SUD treatment, for the Substance Abuse and Mental Health Services Administration (SAMHSA); the company continues to maintain WITS in collaboration with federal, state, and local governments.
- WITS has evolved, now offering a wide variety of modules beyond SUD treatment to support social services that address behavioral health, problem gambling, substance abuse prevention, criminal justice and court problem-solving. It also interfaces with the primary health community through Integrated Screening, Brief Intervention and Referral to Treatment programs. WITS is an ONC-certified EHR solution.
- FEI built the Omnibus Care Plan (OCP) and Consent2Share (C2S) for SAMHSA (see below). Adoption of C2S has been slow, evidently because it lacks a governance structure and hasn't gotten needed data-sharing agreements.

Omnibus Care Plan and Consent2Share. OCP is an open-source software behavioral health case-management system developed by SAMHSA and built by FEI Systems. OCP was created as a prototype to demonstrate how to share sensitive mental health and substance-use information through enforcement of 42 CFR Part 2 and 38 USC 7332 (for veterans) consent.

An integral/complementary part of OCP is Consent2Share (C2S), an open-source software, consent management and redaction-based consent-enforcement system. OCP and C2S have been piloted by Arizona's Health-e Connection and Prince George's County (MD) Health Department. We interviewed Ken Salyard, former Information Management Specialist at SAMHSA, and Michelle Zancan with Zane Networks, both of whom worked extensively on OCP and C2S. They said:

Consent2Share

Consent2Share: Developed by SAMHSA utilizing FHIR consent resource to provide consent management for date tagged using DS4P. Allows patients to make meaningful choices about how to share their sensitive data.


EHR Application
Consent2Share in the Cloud
Web API: REST, JSON, OAuth2
Patients, Providers, Policy Experts, Administrators
Author/Update Policies
OBHITA.org

Credit:PP2PI

- C2S has two parts, a front end that allows a patient to create a FHIR consent directive and a back end system that uses the consent to parse through data content that is being expected to share. The back end does a two-pass process; the first pass marks everything that is Part 2-protected information, and in the second pass, the Part 2 information is redacted, thereby only allowing permitted information to be shared.

- Cost is a roadblock for implementing C2S, despite its open-source development. Most substance use disorder treatment providers can't afford to buy and deploy systems, let alone pay to have them implemented and maintained.

- There may be more C2S implementations by county and state providers once Part 2 becomes opt-in/ opt-out. Even then a significant amount of work will need to be done for broader implementation. A nationally accessible application programming interface (API) will be needed to facilitate validating opt-ins/opt-outs.

- The strong focus on protecting data, while critical, also has the effect of obstructing the exchange of information that could improve treatment and outcomes for a sizable number of patients. They are falling through huge gaps in care created by siloed data, so systems and a "culture of sharing". The good news is that ONC is updating HIPAA and Part 2 toward that end.

- Changes in the Coronavirus Aid, Relief, and Economic Security (CARES) Act in some ways make things easier for treatment providers and in other ways add difficulties. On the up side, once the implementing regulations are published, SUD data can be shared like HIPAA-covered data if a patient opts-in – and the sharing is indefinite unless consent is revoked. Once those data are considered for sharing, however, the tracking of consent status will be necessitated; that is because, when a patient opts out, from that time on, no new data covered under Part 2 can be exchanged (unless consent is later provided).

- The current, fragmented environment makes it difficult to know a patient's latest consent status across multiple healthcare providers, EHRs and geographically specific HIEs. Will there be a centralized place for the status to be stored, so providers can find out? Will this be an HIE; at the provider level; at a national level? If such issues aren't addressed, organizations are likely to decide not to share to avoid the risks.

HIMSS' Electronic Health Record Association. The HIMSS EHRA is a trade association of Electronic Health Record companies that addresses national efforts to create interoperable EHRs in hospital and ambulatory care settings. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care, as well as the productivity and sustainability of the healthcare system.
The following information is directly derived and condensed from EHRA's website:

- Established in 2004, the EHRA brings together companies that develop, market, and support EHRs to collaborate on issues that impact our businesses and our collective customers – hospitals and providers that represent the majority of EHR users in the U.S. We work together to speak with a unified voice on these topics in a non-competitive, collegial effort to understand, educate and collaborate with all stakeholders.

- The EHRA operates on the premise that the rapid, widespread adoption of EHRs is essential to improve the quality of patient care, as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation.

- Core objectives focus on collaborative efforts to accelerate health IT adoption, advance interoperability, and improve the quality and efficiency of care. EHRA strives to engage the EHR software developer community and other stakeholders regarding EHR and health IT standards development, certification processes and criteria, interoperability, patient safety, usability, privacy

- and security, electronic performance and quality measures (eCQMs), health IT-focused public policy, and other EHR-related issues that are the subjects of growing government, payer and provider focus.

In June 2013, the EHRA introduced the EHR Developer Code of Conduct. The EHRA maintains and updates the Code as needed, and it provides a forum for educating EHR developers on the importance of these principles. We encourage all EHR developers, regardless of membership in EHRA, to adopt the Code.

Community Referral Services

These software systems primarily include referral platforms and referral software vendors. Their aim is to enable providers of healthcare and social services to identify community resources (e.g. food pantries, homeless shelters); to refer individuals/families who need those resources; and to "close the referral loop" by tracking referral outcomes.

While that last step is considered best practice, however, organizations that provide information and referral services, like 211s don't have the funding or capability to close the loop. So, instead, they usually focus on providing a list of community resources based on a self-navigation model, but they do not typically know or record whether services were actually received.

A primary difference between various types of CRS approaches is the type of directory they provide of available resources in their community. **Focused directories** describe the services of the resources/organizations listed within them. This model works particularly well for networks of healthcare providers with strong partnerships where one platform is embraced across an entire community. **Comprehensive directories** aim to maintain a database of human services irrespective of whether the listed organization is a paying subscriber to the CRS. Comprehensive directories often provide free, self-service websites for individuals to use to discover community resources that meet their needs.

The challenges that adopters of these technologies face across the industry are not the result of the limitation of any one product or technology but, rather, are due to the lack of maturity and adoption of open standards that would make tracking consent and interoperability affordable at scale. For example, while each of the platforms provides mechanisms for healthcare IT systems to integrate using REST APIs or healthcare standards, point-to-point integration models often make it financially infeasible for social services organizations to integrate their individual Case Management systems with each other. As a result, clinicians and case managers often end up using multiple systems. Because social services providers often use a Community Referral Service chosen by a hospital system as part of a contract, those providers – with multiple healthcare partners – often have to use two to five CRSs to serve the same patients.

Services Interviewed

- NowPow
- Aunt Bertha
- Unite Us

Services Studied

- 211 Services
- United Way Services
- Alliance Information and Referral Systems (AIRS)

Key Information and Insights

- Community Referral Services vary in their orientation toward healthcare and self-navigation or their focus on regional care coordination networks. While the best practice is to identify whether a referred service was delivered and what its impact was, mature standards and sufficient resources for documenting outcomes are lacking.
- While some CRS software is described as creating "care coordination networks," the consent data recorded is primarily around consent for sharing referral data and not information aimed at care coordination itself. In contrast, EHRs and Care Management software are the primary stewards of HIPAA consent records and have far more clinical data and integrations than is typical in CRS software.
- Default consent functionality varies significantly between platforms. Aunt Bertha, for example, provides highly granular patient-directed control over which provider can access which referral record; concerns are emphasized of potential harm that could occur if a patient's information is too widely shared within a group of providers. For referrals initiated by providers, consent needs to be collected before each referral. NowPow and Unite Us, on the other hand, emphasize the ability for

‘Without consent-driven interoperability across healthcare and human services systems, closing the referral loop and enrolling patients in programs remain particularly difficult for the most-vulnerable, transient and low-income populations.’

multiple cooperating providers to coordinate care across a single record of a patient’s referrals.

- All the CRSs support both proprietary and FHIR-based APIs and are participating in the Gravity Project to advance standards for defining social risk data. The adoption of Gravity’s recommended standards for assessment, diagnosis and interventions to address patient social needs represents an important step toward supporting potential interoperability across CRSs and EHRs. CRSs are making headway in adopting SDOH assessment, diagnosis and intervention codes, but use of the FHIR Consent resource as prescribed in Gravity Implementation Guide is in the testing phase.

- The exchange of SDOH data within CRSs follows clinical workflows that most often don’t involve leveraging existing data in non-clinical systems. This includes identifying social needs through some time-consuming assessments (surveys) and diagnosing the social need and implementing the intervention (referral). Provider data sharing from human services to healthcare, outside the context of closing the loop on the referral, is rare.

  Other than compliance with HIPAA, the collection of SDOH data via assessments needs no additional consent – but consent is sometimes required for leveraging shareable SDOH data from social services providers. Two examples of common workflows: Asking patients if they are enrolled in the federal Supplemental Nutrition Assistance Program or receiving updates from a community-based organization that has assisted patients in the eligibility and application process for SNAP.

  In contrast, if an EHR/CRS received SNAP eligibility/enrollment data from a state’s Department of Social Services, additional consent to release the SNAP data would be required. The lack of a Consent Service Utility (CSU) impedes more-advanced SDOH use cases, whereas having a CSU could reduce the amount of followup required to ensure that the patient gets enrolled in the program.
  Consent functionality that enforces the sharing of information within a system is common. For example, Unite Us provides notifications reminding users to not redisclose Part 2 information when a patient has received a referral from a Part 2 program. However, the exchange of consent data across systems, or the reliance on a third-party organization or application to programmatically enforce consent, does not exist outside of regional implementations of Consent2Share.

- Without consent-driven interoperability across healthcare and human services systems, closing the referral loop and enrolling patients in programs remain particularly difficult for the most-vulnerable, transient and low-income populations. For them, housing insecurity may mean their address is more likely to change, and financial insecurity may mean their phone service gets disconnected or they have less access to a computer.

- Without the ability to reuse data across systems (with consent) to streamline program eligibility and enrollment, Community-Based Organizations (CBOs) have to do far more to duplicate data entry, eligibility screening and manual patient followup.

  This is particularly problematic for service navigation programs, which are very underfunded. So patients have to retell their story and take duplicative assessments for each provider. And everyone has to follow a more-painstaking process to assemble a comprehensive longitudinal record that patients can control and share with their care teams.

- While they support common FHIR-based referral standards for social care referrals that have been proven to work with EHRs, CRS software systems have not demonstrated this same type of interoperability with one another. Due to the 21st Century Cures Act, since April 5, 2021, the “Information Blocking Rule” requires healthcare providers, health IT developers, health information networks and health information exchanges to share electronic health information with other systems that have legal right to request it.

  During a September 2021 webinar. ONC staff outlined scenarios that would likely or unlikely be considered information blocking. The scenario:

"If I direct my EHR developer to configure the technology so that users cannot easily send referrals/EHI to unaffiliated providers whose Direct address the user has,"[22] was marked as a likely violation of the provision. The implication is that healthcare and human services providers using different CRSs or EHRs should be able to make referrals across software platforms if they support common standards like FHIR or Direct Secure Messaging.

The following are brief descriptions of some of the CRSs examined during our scan, along with key points made in interviews with officials/leaders of each organization. *Important note: Since we conducted these interviews, Unite Us has acquired NowPow.*

Unite Us – Unite Us is a technology company that provides both an end-to-end, person-centered care coordination platform and a hands-on community-engagement process to improve health-related service delivery. Unite Us brings together networks of health and social service providers, enabling them to connect people with the care they need and to use data-driven insights to identify and address community needs. We interviewed Carlos Uriarte, Vice President and Regulatory Counsel; and Cody Johansen and Jake Thomson, from the Unite Us Interoperability product team. They said:

- The Unite Us Platform is a closed-loop referral system wherein network partners can only see information about the clients they serve.
- Unite US is a participant in the Gravity Project and a proponent of standards-based exchange of data.
- Unite Us leverages a short, one-time consent form that each client must agree to before any referrals can be made for that client.
- The Unite Us consent does not replace subject-matter specific consents, such as 42 CFR Part 2 organization consents, which are collected separately and can be stored on the platform.
- Unite Us has an equity-driven consent process with an emphasis on ensuring people understand what they're agreeing to. The consent is written at an accessible reading level. The consent form links to the privacy notice, which is available on the company's website and provides a deeper dive into how client information is used and shared to connect clients with services in accordance with applicable law.
- Consent can be captured in over 30 languages and through various means, including via email, text message, document upload of signed paper copy, audio upload of verbal consent, on-screen by user attestation or on-screen signature.
- Client consent may be withdrawn at any time.
- Unite Us trains its users on the consent process and provides notifications in its platform on consent rules; for example, by reminding users that certain information should not be redisclosed.

NowPow. NowPow (derived from Knowledge is Power) is a community referral platform that is customizable, evidence-based, person-centered and supports organizations of all sizes in healthcare, human and social services, and sometimes in education and justice.

NowPow works with payers, providers and community coalitions. Its software helps communities address the full spectrum of needs, including linkage to primary care services, chronic disease prevention or support, support for parenting and childcare, connection to vital resources like food and housing, and research projects. We interviewed Cathryn Crookston, Vice President of Sales, and Joe Hinderstein, Senior Account Executive. They said:

- NowPow tracks consent to share patient data such as contact information, demographics, previous referrals, screening results and consent to contact the patient.
- After consent is obtained and captured once, it is not required before each referral.
- Sensitive referrals are configured by admins based on service types. NowPow has a default list of sensitive service types. A sensitive referral is only seen by the sending and receiving organization.
- The platform integrates securely with EHRs, HIEs,

[22] "What Clinicians and Other Health Care Providers Need to Know: An Introduction to Information Sharing Under the Information Blocking Regulations," The Office of the National Coordinator for Health Information Technology, September 14, 2021, pg. 17, https://www.healthit.gov/cures/sites/default/files/cures/2021-09/ONC%20Provider%20Webinar_508.pdf

patient and member portals, and care- or case-management systems.

- One-way referrals let patients search for community resources with NowPow's tools or are presented with a personalized list of services recommended to them. These make up 80% of referrals.
- Closed-loop referrals take place between two organizations or within an entire network based on sensitivity and network setup.
- Consent can be captured with an in-app signature, digital e-signature (via text, email), PDF/document upload or with a care professional, who can turn their computer around and allow a patient to provide consent on the spot.
- HIPAA, 42 CFR Part 2 and FERPA compliant.

Aunt Bertha (being renamed Find Help). Aunt Bertha's mission is to connect all people in need to the programs that serve them with dignity and ease. Aunt Bertha created a social care network that connects people to programs, making it easy for them to find, connect to and receive social services in their communities, for nonprofits to coordinate their efforts and for customers to integrate social care into the work they already do. We interviewed Jaffer Traish, Chief Operating Officer, and Erine Gray, Chief Executive Officer. They said:

- Their connection models include scheduling, texting, emailing, service applications and screeners, e-referrals and self-navigation.
- In permission-based consent models, access is based on who should be party to each referral; this is considered consumer-directed privacy. Aunt Bertha supports coalitions of organizations doing coordinated care, seeker control of private data, and organization-to-organization sharing through appropriate legal agreements.
- Consent is collected before each referral to protect the seeker. This is different from an all-in or one-time consent that makes assumptions about who can look up a person's private information and has the potential to cause harm or stigma over the long term.
- Patient Health Information can be shared because the software is certified by the Health Information Trust Alliance (HITRUST).
- Seekers can grant access, remove access and see who has access to their private referral history (different from staff-generated referrals that customers create).
- Navigators, or helpers, can request access to private referral history; the submission goes to the person who can approve or deny it.
- Their APIs use existing FHIR resources such as ServiceRequest, Task and DocumentReference to transmit referral information in a bi-directional manner. Aunt Bertha is upgrading to the Gravity Project's recommendations and US Core.
- In its Proxy Project, Aunt Bertha will enable more functionality for proxies to have access to appropriate information through its permission-based model. This includes functionality for tracking households and heads of households.

Community Information Exchanges

A CIE is an ecosystem made up of multidisciplinary network partners that use a shared language, a resource database and an integrated technology platform to deliver enhanced community care planning. By definition, a CIE must integrate data systems, facilitate a single "person record" across multiple sectors, be locally led and governed, and include authentic community engagement.

Care-planning tools enable partners to integrate data from multiple sources and make bidirectional referrals to create a shared longitudinal record. By focusing on these core components, a CIE enables communities to shift away from a reactive approach toward providing proactive, holistic, person-centered care.

CIEs combine features of HIEs and CRSs, with a broader goal of improving well-being that is not necessarily focused on health. Within this holistic and ideally pro-active framework, CIEs enable the sharing of a wide range of healthcare, social services, housing, homelessness, childcare, education, and other information associated with health and well-being.

They serve as partnerships that embrace the technical goals of creating a common community care plan and a longitudinal record for individuals seeking a variety of supportive services in order to achieve a vision of thriving individuals and communities.

CIEs create a tool within which health and social/human services providers can collaborate and coordinate the full spectrum of care for individuals and families.

They do so by combining (1) the capability of an HIE to pull together standardized data and free text documents from multiple different electronic records systems and (2) the ability of a CRS to customize and track referrals for an individual or family to the most-appropriate resources.

To do so, they require definitive capacity to support either broad or fine-grained consent for sharing information across multiple systems, domains and geographies. Fine-grained consent can take the form of strict organizational or role-based controls or can incorporate both the data segmentation and tagging capacities discussed in this report's sections on EHRs and HIEs, with a highly detailed consenting process through which the individual being served gives consent for the types of information to be shared with specific organizations and/or roles.

CIEs Interviewed

- 211 San Diego
- ONC Leading Edge Acceleration Projects (LEAP)

CIEs Studied

- Monroe County United Way
- University of Texas, Austin (ONC LEAP 2)

Key Information and Insights

- Because CIEs are striving to implement such a comprehensive approach, optimizing autonomy for their service beneficiaries, including for providing consent, is key to the CIE model. This includes autonomy for patients/clients to use the CIE's tools for their own benefit. Enabling individuals to use these tools sets the stage for giving them the ability to give and revoke consent directly and at will.

- Equity appears to be a growing focus of CIEs. The goal is to use technologies, produce data and achieve outcomes that narrow disparities in health, wealth, education, foster care placements, incarceration and other areas where inequality is systemic.
- CIEs are also working to address the "digital divide" in access to technology and are keenly aware they must structure consent options so the most vulnerable individuals are not denied services when they want to protect private data – for example, information that could lead to a child welfare investigation (the vast majority of which are dismissed or resolved) or to the denial of housing or a job.

- Our scan indicated CIEs are working on a "start small, then expand" model. They are experiencing the same challenges found in other categories of data sharing, including multiple sets of regulations and cultures that do not align to enable and expedite information sharing. There is strong recognition in the CIE community that reengineering business processes will be critical to their success.

The following is a brief description of 211 San Diego (which is featured alone here because it is widely considered to be the most-advanced CIE in the country), along with key points from information provided by CEO Bill York and other senior officials of the organization. 211 San Diego offers a Toolkit for developing a CIE.

211 SAN DIEGO. 211 San Diego leads the San Diego CIE, a multidisciplinary network of 109+ partner agencies across the numerous, diverse sectors that serve San Diego and Imperial County residents in California. The approximately 1,400 service providers in the CIE include local government entities, healthcare systems, social and human services organizations, educational institutions and the local health information exchange.

Those agencies match individuals with appropriate care providers based on their needs. This is accomplished through shared screening linked to a resource database that includes standardized listings of health, human and social services providers' service offerings, eligibility and intake information. This interoperable database and longitudinal "person record" helps establish a closed-loop, bidirectional, electronic referral process and shared community-care planning. For this scan report, 211 San Diego officials said:

- The CIE's authorization form allows 211 San Diego and CIE partner agencies to use, store and share personal, financial and health information to assess needs, coordinate care and provide services for members of the San Diego and Imperial County communities who may benefit from having their needs addressed across multiple health, human and social services domains.

- The authorization form allows individuals to opt in by consenting to share their information with and between San Diego County and its CIE partner agencies, as allowed by federal and state regulations.

  The form is available in hard copy and electronically, and it can be uploaded to the individual's CIE record through the CIE's website; it is also available telephonically for verbal consent. Authorization is valid for 10 years or by a date specified by the individual on the form, who can revoke it at any time.

- Partner agencies have integrated the CIE authorization into their own consent processes and documents, resulting in joint authorizations (e.g., US Housing and Urban Development Department-funded providers using the regional Homeless Management Information System, Sharp Healthcare, etc.).

- A critical technical element of the CIE is the ability to integrate data through middleware software, allowing multidisciplinary partners at diverse levels of sophistication to use their existing systems to contribute individual-level data into the community-wide client record.

  The technological infrastructure enables closed-loop referrals between network partners, providing various search functionalities and an integrated, longitudinal client record with SDOH data relevant to the services each organization's system provides.

- The CIE has both health and social data, enabling it to identify and correlate health disparities for racial and ethnic minorities. When disaggregated by race, CIE data across domains holds the potential to demonstrate how inequities across systems interact and compound, as well as their impact on affected populations.

  The CIE's governance structure is designed to monitor how principles and commitments to health equity are operationalized in protocols, privacy agreements, metrics and policies, with the goal of promoting health equity in three ways:

  - Creating data ownership for directly impacted communities of color by allowing them to participate in the data narrative and to inform the understanding and value of the data.
  - Highlighting the multi-level system challenges/opportunities about systemic racism within the system of care.
  - Changing direct service practices and seeking investments that will allow for tailored, person-centered services and supports based on their current state.

Governmental and Industry Initiatives

In addition to vendor and non-profit information exchanges requiring consent, there are a growing number of government agencies and industry organizations investing in efforts to solve both domain-specific and multi-domain consent problems. These efforts include:

Efforts Interviewed

- ONC LEAP 1 (San Diego)
- SAMHSA and OCP and Consent2Share
- Midato Health's ShareApprove
- HEART
- PP2PI
- HIPAAT

Efforts Studied

- ONC LEAP 2 (University of Texas, Austin)
- Center for Democracy and Technology (CDT)

Key Information and Insights

- Government agencies and industry consortia have long been concerned with the challenges of consent between IT systems. EHRs and HIEs have functionality for determining consent to share within their systems and are generally able to conclude whether an entire patient record can be shared with an external system. However, there is limited ability to then determine whether the shared record can be reshared or dealt with in a manner different from the original consent.
- In 2019, San Diego Health Connect received an ONC LEAP grant for Clinical Decision Service (LEAP-CDS) to enable more-sophisticated shared consent

CDS) to enable more-sophisticated shared consent services across multiple systems.

A critical feature of LEAP-CDS is a centralized, end-user management of consent assertions across multiple consent stores and multiple health and social services IT systems. This approach addresses one of the most-challenging privacy and consent issues: How do individuals know what systems hold their sensitive information and how do they track down and manage consent for all their far-flung, sensitive data?

Of special concern has been how to specify fine-grain consent for highly sensitive information about such matters as mental health, substance use, sexually transmitted diseases, HIV/AIDS, interpersonal violence or familial abuse.

Over the past decade, such issues have led to the definition of HL7 standards for Data Segmentation for Privacy (DS4P). The Protecting Privacy to Promote Interoperability (PP2PI) Workgroup has been defining user stories and use cases to guide and encourage implementing support for DS4P in EHRs and HIEs. In addition, SAMHSA funded an open-source implementation and pilots for an Omnibus Care Plan and Consent2Share services (see Page 33).

As greater understanding of the importance of SDOH is growing, so is interest in enabling the management of consent beyond its dominant focus on physical and behavioral health. For example, the CIE of the University of Texas, Austin, has received an ONC LEAP grant to support work on providing consent for social services interventions through community-based organizations (LEAP 2).

- During the past few years, a new industry effort called the Health Relationship Trust (HEART, described on Page 43) was created within the OpenID consortium. HEART is a set of profiles based on FHIR, OAuth, OpenID Connect and User-Managed Access (UMA) that aims to enable patients to control how, when and with whom their clinical data is shared. By demonstrating how to use existing standards to manage consent, HEART has created a foundation for future shared-consent services.
- Of interest in the near future is industry work on "self-sovereign identity." This is a next step in the continuum from centralized and federated identity models to self-managed identity. A related set of industry research focuses on self-managed and self-controlled healthcare data based on block-chain representations of that data. These technologies would enable broader personal control over healthcare and social care data, potentially resulting in putting individuals in direct control of consent to access their information.

The following are brief descriptions of some of the Governmental and Industry Initiatives examined during our scan, along with key points made in interviews with officials/ leaders of some organizations conducting the work:

Leading Edge Acceleration Projects in Health IT. LEAP is a program of the Office of the National Coordinator for Health Information Technology (ONC). It provides guidance, funding and collaboration opportunities for innovative initiatives to develop, refine and implement standards, methods and techniques that advance information sharing and interoperability.

ONC LEAP Consent Decision Service. LEAP-CDS is an open-source project that enables patients to manage their consent decisions across multiple healthcare IT systems, and then enables systems to request patient consent by providing context for the type of workflow for which the patient information would be used. One of the main goals of LEAP-CDS was to create "computable consents," meaning consent processes that are highly automated and require minimal or no human participation to capture, implement and enforce them.

Mohammad Jafari, the LEAP Project Director for San Diego Health Connect, said in an interview for our scan that computable consents are now possible in healthcare through a User Interface (UI) that can capture consumer preferences and store them. Decision assistance to the data can then be applied to make it automatically enforceable within a federated environment. San Diego's LEAP-CDS is explicitly about healthcare, but Jafari indicated the technology could be transferred/adapted to accommodate social services and perhaps other domains.

From the Online Description of LEAP-CDS

This project is focused on Standardization and Implementation of Scalable HL7® FHIR® Consent Resource by creating a FHIR-based platform that simplifies consent management and ensures interoperable services for these four use cases: 1) privacy consent, 2) medical treatment consent, (3) research consent and (4) advance care directives.

The research team includes participants from San Diego Health Connect and Saperi Systems, a company spun off from Cognitive Medical Systems, Inc. for this project. The team leverages these organizations' collective strengths to meet ONC's research objectives by creating a common, FHIR-based authorization framework capable of management and enforcement of patient consent, as well as organizational and jurisdictional policies.

It will also review additional privacy- and security-related standards to ensure they support the current FHIR Consent Resource.

This work will build on previously successful FHIR Consent Resource demonstrations at HL7, ONC Pilots, and sponsored HIMSS Interoperability Showcase demonstrations, where the San Diego Health Connect Team has already addressed three of the four use cases.

Following a research phase to study the standard, current implementations, and the related standards and business requirements, the team will develop a proposed set of improvements and will build APIs to enable the consent use cases which have important implications for patient-centered care, informed consent and shared decision-making. The API will be tested with each of the LEAP use cases in live exchanges at the SDHC HIE.

The SDHC team also plans to build a FHIR Consent Implementation Guide (IG), including examples derived from these use cases as well as additional implementation, legal, and security concerns raised within the project testbed. The IG will come with a package of open-source prototypes and documentation to assist partners in deploying the framework as a RESTful service and to address the consent workflow.

Project Results

The LEAP Project has completed the first version of a LEAP-CDS. It enables clintians to ask about the patient's consent decision applicable to a specific workflow context, such as processing a request for exchange of a medical record. The CDS responds with a permit/deny decision, as well as applicable obligations. The CDS relies on consent stores (FHIR servers where patient consents are stored and can be looked up). Currently, the LEAP-CDS supports query interfaces based on eXtensible Access Control Markup Language (XACML) and a CDS API.

The LEAP project team has successfully tested this service to enforce patient consent in an HL7v2 exchange use case and is currently working on integrating and testing this service in an eHealth Exchange scenario.

ONC LEAP 2 UT Austin CIE. The University of Texas Austin in August 2021 was awarded an ONC LEAP grant to extend its work on integrating its healthcare system in a closed-loop referral system with local social services. According to the ONC, UT Austin will accomplish that work by creating an API-enabled social and health information platform using the HL7 FHIR standard.

The referral system will be available to EHR systems in all federally qualified health centers to help manage the SDOH needs of patients in pursuit of health equity.
ONC officials said the system will leverage use cases developed by the Gravity Project for the collection of SDOH data related to food security, housing stability and transportation access.[23]

ShareApprove™. This is the product name for the new Midato Health™ document management and communication solution for scalable consent. This B2B solution gives healthcare, social service organizations and government agencies the ability to ensure individuals' sensitive and personal data can be shared pursuant to their permissions and preferences, with consent options for 1:1 (person or organization), multi-organizations or attributed care teams, as well as one-time or time-bound approvals and revocations.

[23] Elise Sweeney Anthony, Thomas Mason, MD, Rachel Nelson, JD, "What Clinicians and Other Health Care Providers Need to Know: An Introduction to Information Sharing Under the Information Blocking Regulations," The Office of the National Coordinator, 2021, https://www.healthit.gov/cures/sites/default/files/cures/2021-09/ONC%20Provider%20Webinar_508.pdf

ShareApprove is an HL7-compliant SaaS (Software as a Service) technology with a consent rules engine consistent with federal and state regulations regarding data-sharing limitations. Midato Health was formed in January 2020 after three years of incubation under the umbrella of its sister company, CedarBridge Group.

ShareApprove interface engine services are able to interface with external systems to facilitate data transport via standard or FHIR APIs, based on the capacity of the source and target systems. Additionally, ShareApprove offers a range of extract-transfer-load modalities enabled by the interface engine and integrated master data-management services, powered by Gaine Solutions, allowing for flat-file retrieval, validation, matching, resolution and transport of data. These built-in services combine to offer a flexible approach to integrating data to and from a variety of potential data sources and source systems.

Utilizing a mobile or responsive web-based app, individuals can authorize the sharing and use of personal information with organizations involved with the care and services they receive. ShareApprove is consent form and platform agnostic and can be easily customized to allow individuals and organizations to communicate through a variety of mechanisms to share person-generated data. For example, Bamboo Health (formerly Appriss Health) selected ShareApprove to enable a streamlined consent process for SUD treatment in their new behavioral health platform.

The ShareApprove server-less architecture is highly scalable and secure. Individuals and business users of ShareApprove have the ability to view pending, active and inactive (expired and revoked) consents in the system. ShareApprove™ is positioned to enable data to be used for purposes beyond what state and federal regulations currently allow.

Health Relationship Trust. HEART (Health Relationship Trust) is a set of profiles that enables patients to control how, when and with whom their clinical data is shared. The model builds on existing state-of-the-art security and adds components to ensure that patient clinical data is securely exchanged. In addition, HEART defines the interoperable process for systems to exchange patient-authorized healthcare data consistent with open standards, specifically FHIR, OAuth 2, OpenID Connect and UMA.

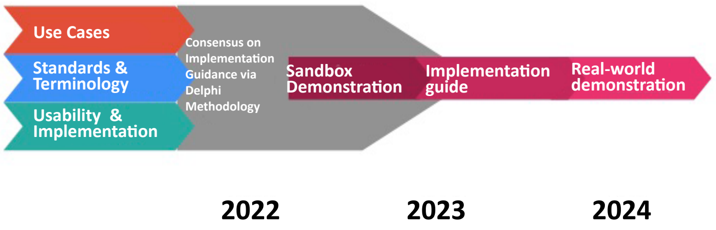
HEART also paves the way to support patient-defined electronic consents for the sharing of sensitive data. Consents are interpreted and converted to a secure authorization workflow to dynamically deliver clinical data, via FHIR, based on the patient’s “computable” consent. It further delivers data with fine-grained options, so a patient has much more choice than just to opt-in or opt-out. These are seven key HEART benefits:

- Patient-directed sharing across a wide ecosystem.
- Patient control of who can access their data.
- Works in conjunction with Best Practice Security Standards.
- Provides more-granular management over protected resources.
- Leverages existing open standards.
- Ease of use by patient and provider clients.
- Supports Data Segmentation for Privacy.

The HEART workgroup was originally sponsored by ONC to define a standard and interoperable process for patient-directed clinical data exchange. Implementations are normally integrated with high-trust identity providers and best-practice security standards. In sum, HEART and UMA provide the secure authorization workflow to enable a consent to be computable and with fine-grained choices where applicable. This process supports patient privacy and reduces clinical burden, while improving interoperability and trust.

PP2PI Workgroup. This is a multidisciplinary, national, volunteer body of expert stakeholders addressing the problem of how to granularly segment sensitive data to protect patient privacy and promote interoperability and care equity.
The group includes more than 160 representatives from healthcare organizations, professional societies, standards-development organizations, health IT vendors, HIEs, Interoperability Frameworks, payers, governments, government and non-government contractors, privacy law and ethics experts, patient advocates and others. PP2PI is supported by HIMSS, IHE USA and the Drummond Group, but it is independent and does not receive financial backing from any organization.

PP2PI Roadmap



CREDIT: PP2PI

The PP2PI group was founded under the following principles, recognizing that support for them requires addressing the policy drivers and shortfalls in current technology enablers:

- Sharing of patient data between clinical providers in many instances can meaningfully improve patient care. Sharing of patient data at the population level can meaningfully inform government officials, health care organizations and non-profits, and it can improve the health of communities, reduce costs and enable research that promotes a learning health system. Finally, patients should have the option to provide proxy access to their electronic health data to non-clinical caregivers who help manage their health and care.

- Empowering patients and including them as partners in care decisions – including with the ability to control their own personal health data and how it is shared – has been shown to improve the provider-patient relationship, which in turn has been shown to improve outcomes.

- In certain instances, state and/or federal law gives patients have the right to withhold specific, sensitive data. In other instances, a patient's living situation, culture, values, relationships or other factors may warrant a clinician withholding health information from others, such as personal representatives.

PP2PI Challenges:

- Lacking adequate technical standards for granular segmentation of sensitive data, many organizations resort to blunt algorithms or manual processes to withhold sharing for broad populations in order to comply with state and federal law.

  This may result in care inequities and potential information blocking because patients with conditions that are stigmatized, when given the option, may be less likely to consent to having their data shared across care systems. As some sensitive conditions are more prevalent in disenfranchised populations, this contributes to disparities in care.

- Current standards for granularly segmented data are improving but are still insufficient. For some time, there have been normative standards for granular segmentation of health information using HL7® version 2 and CDA, and the FHIR® Data Segmentation for Privacy (DS4P) Implementation Guide (IG) is moving toward normative status.

  Although the HL7, CDA, DS4P IG standard and the related Consent2Share (C2S) tool (which is not a recognized standard and is no longer supported by SAMHSA) have been successfully piloted by a handful of sites, widespread implementation has lagged for a number of reasons.

  Those include a lack of regulatory impetus for adoption and failure of the current standards to meet a number of high-priority use cases. There has also been a lack of implementation guidance, particularly around controversial issues such as how to balance patient safety with privacy considerations.

A key deliverable of the PP2PI workgroup, formalized in May 2020, involves developing a set of nationally acceptable use cases, which will be leveraged to support standards revision and development. As of June 2021, the following clinical use cases had been developed:

- Maternal substance-use data shared in an infant record.

- Adolescent reproductive health data shared by clinicians, with portal proxy, and payers.

- Geriatric patient behavioral health data shared among clinicians, with health information exchange, accountable care organization, payer and portal proxy.

- Adult patient with SDOH data on intimate partner violence (IPV), shared by clinicians, CBOs and a third-party mobile app (in process, in conjunction with the Gravity Project).

Standards development is focused on DS4P, Privacy Consent and security labels using HL7 2, CDA and FHIR resources. This process includes defining a nationally available, steward-maintained terminology value set for sensitive conditions and addressing a means to define privacy policies and identify patient-consent preferences through a consent-management engine and security-labeling service. The PP2PI group will develop an implementation guide (IG) with consensus-driven guidance for areas identified as barriers to implementation, including but not limited to:

- Recommendations for role-based vs. attribute-based access control provisioning.
- Policies and procedures for break-the-glass access to data.
- Visualization of redacted data and utilization in decision support algorithms.

Clinicians have expressed significant concern about the patient safety implications of withholding data. There are similar implications related to the inability to appropriately withhold sensitive data, which has the potential to lead to both immediate and long-lasting harms. Those include a loss of trust in providers and in the system's ability to safeguard private data, as well as potential risk to the patient of harms outside the healthcare setting (e.g., IPV resulting from inappropriate data sharing).

A primary goal of the PP2PI group is therefore to develop an implementation guide with authoritative guidance/ recommendations backed by clinical professional societies, ethicists, and authorities in user experience and patient safety.

In these ways, the PP2PI workgroup aims to facilitate the appropriate standards revision and implementation guidance necessary to drive the widespread adoption needed to empower patients to share their data with appropriate protections and decrease disparities in care. Future work will include advocacy for and sponsorship of governmental policy to promote such applications nationwide to promote equitable interoperability across the healthcare ecosystem.

HIPAAT. HIPAAT is a healthcare software provider of consent-management and auditing solutions to enable health information privacy wherever the data is shared – between healthcare providers, organizations, regions and nationwide – mindful of the balance between privacy and clinical access to health information. We interviewed Kel Callahan, President of HIPAAT, and Patrick Pyette, Delivery Lead (internal and external). They said:

- HIPAAT provides granular, patient-controlled consent management using HL7 FHIR (R4) and OASIS XACML standards.
- There's flexibility in their Privacy eSuite(PeS) product for handling different use cases relating to public health, SDOH or factors that relate to the care of a child. If there's an important element a client's use case doesn't have, the product allows for attributes to be added. HIPAAT has experience with drug courts and has a demo of how its product could work in them.
- The problem HIPAAT is trying to solve is to essentially provide an electronic system that would enable data/information governance that would be controlled by the patient and enabled by a healthcare, state or federal system. They want to provide something that is patient-centric from a best-practices perspective and is useful for organizations operating within differing jurisdictions.

Amazon Web Services (AWS) Consent Management Approach. The core purpose of consent is to limit or allow data sharing based on the patient's determination. Yet, in most cases, the process for capturing consent is not connected to the process for controlling data access. The AWS Consent Management Approach tightly couples the determination with data access.

The approach illustrated on the next page has two primary functions:

- Capturing consent
- Controlling user access to data

Although the diagram depicts a paper consent form, the process could easily be electronic using a signed form. In either case, patients begin by indicating what data they are willing to share with which providers. The data is organized in high-level categories, such as Behavioral Health, Criminal Justice, Education, Public Assistance, Healthcare, Financial and Demographics.

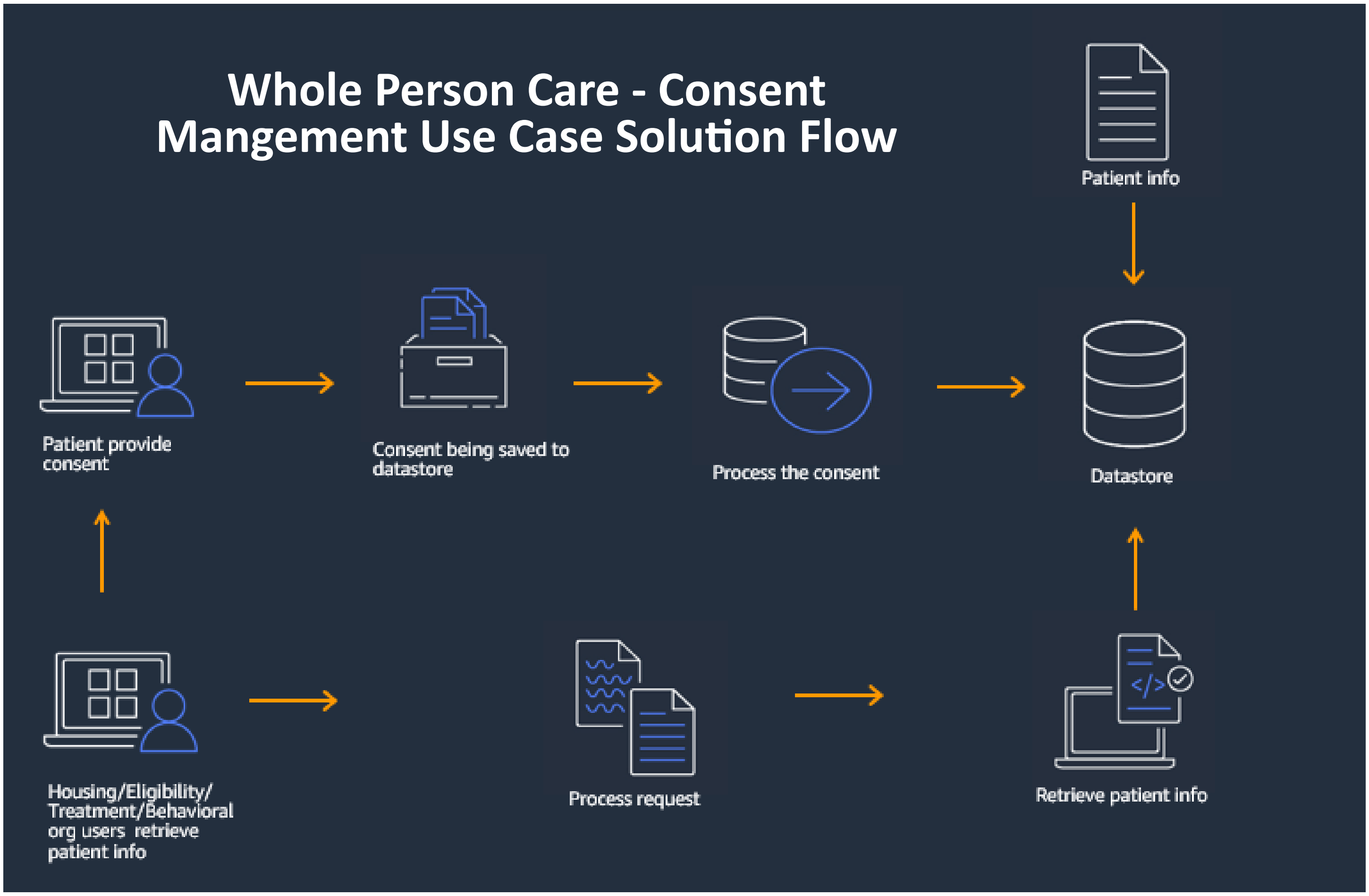
Many models manage data based on the system in which the data resides. Patients, however, may not know which system includes what data. They also likely do not know all the different data elements captured within a single system. Managing consent by data categories improves the patient's ability to make an informed decision.

Further supporting the patient, the consent determination is not all or nothing. The patient has the ability to share a specific category of data with a specific provider. For example, one can agree to share healthcare data with a Care Coordinator, but also decide not to share criminal justice data.

Fine-grained consent management is essential to support informed consent for policies such as 42 CFR Part 2. Once the patient completes the consent determination and signs the form, the document is uploaded to the system, which captures the patient's information in a data store. Before a user retrieves a patient's data, the system checks the store to review consent determination. Only data consented to by the patient for that user will be retrieved.

The determination becomes the gate controlling access to the data at a user- and data-category level of granularity. The AWS Consent Management Approach is not technically a solution. It is simply a model leveraging several AWS services to support the desired business process. The approach can be used to complement existing AWS solutions and as a service for non-AWS environments such as Azure and On premise solutions.

It is simply a refined, role-based approach. As such, the risks and limitations are limited to updating the roles as legislation and datasets change. The level of effort may be higher than a tiered approach, which leverages attributes to apply policy.


Whole Person Care - Consent Mangement Use Case Solution Flow
Patient info
Patient provide consent
Consent being saved to datastore
Process the consent
Datastore
Housing/Eligibility/ Treatment/Behavioral org users retrieve patient info
Process request
Retrieve patient info

CREDIT: AWS Consent Management Approach

Legal Issues and Considerations

The adage of the law being both a sword and a shield applies to the myriad privacy laws in the United States. Laws shield personal information from unwanted exposure but, at the same time, they can impede or prevent the data sharing that consumers, patients, clients and other individuals actually want. In the healthcare sector, for example, as more providers have recognized SDOH and partnered with social services to address patients' non-clinical needs, like access to quality and affordable food, housing and other social needs, the balance between protecting private information and sharing it has had to be reevaluated.

There are several legal impediments to greater data sharing. The primary legal obstacle to exchanging data across sectors is the array of unaligned federal, state, tribal, local and territorial privacy statutes and regulations that govern data sharing and related consent processes in different sectors; there is no universal data-sharing legal privacy framework in the U.S.

Among those who must abide federal health privacy requirements in particular, there is confusion and overly broad application of the legal requirements, which often leads to less data sharing than needed or wanted by patients. This is in part because the relevant statutes often do not expressly state how they are to be complied with when more than one statute applies.

Researching all those privacy laws was beyond the scope of this scan due to their sheer volume; the lengthy list of privacy laws and regulations by sector below are, thus, all federal. The list is not exhaustive, and many other laws exist that can and do impact data privacy.

- Health (physical, behavioral, oral): Health Insurance Portability and Accountability Act of 1996 (HIPAA); 42 Code of Federal Regulation (CFR) Part 2 on SUDs.
- Education: FERPA; Protection of Pupil Rights Amendment (PPRA); Individuals with Disabilities Education Act (IDEA); Head Start, school milk and food programs regulations; Higher Education Act for student loans; McKinney-Vento Act for homeless students.
- Veterans: Federal regulations on confidentiality of quality assurance review, claims and substance use, HIV infection and sickle cell anemia records.
- Human Services: Individuals with Disabilities Education Act (IDEA); regulations for Medicaid, Supplemental Nutrition Assistance Program (SNAP), Special Supplemental Nutrition Program for Women, Infants and Children (WIC); Title X Family Planning; Homeless Management Information Systems' Violence Against Women's Act (VAWA).
- Criminal Justice: Federal Prison Inmate Management System requirements.

There is currently no widespread agreement across sectors for a data-sharing legal privacy framework in the United States, and existing laws reflect that fact. While all the above-referenced privacy statutes and regulations protect personal information, they diverge on to whom they apply, when explicit consent to share information is required, how consent can be revoked, and what exceptions apply and under what circumstances, among other issues.

A primary objective of our consent scan Is to drive progress on the sharing of data to improve health outcomes. Therefore, it is important to focus particular attention on the legal challenges that arise when sharing health data. HIPAA, which places protections on health information generally, and 42 CFR Part 2, which places additional privacy protections on treatment records for SUDs, are the primary privacy legal authorities in healthcare.

Misapplication and confusion abound among those who must abide by them. Prior to the implementation of the Part 2 regulations, in fact, many clinicians treating patients with SUDs expressed concern that the complexity of complying with them would impede care coordination.

Any discussion of HIPAA must begin with the recognition that it is widely misunderstood, despite having been enacted over 25 years ago, and is too often inappropriately invoked as a barrier to data sharing. There are several causes for this reality, the primary one being providers' fear of financial penalty for unauthorized disclosure of protected health information.

That concern has created a culture within the compliance community that defaults too readily to advising "no, you can't share the data." Changing that culture is essential to creating an environment in which providers are more comfortable sharing patient data. The HHS Office of Civil Rights' pending clarification of HIPAA could go a long way toward achieving that aim by including language clarifying when data can be shared, rather than focusing on when it cannot.

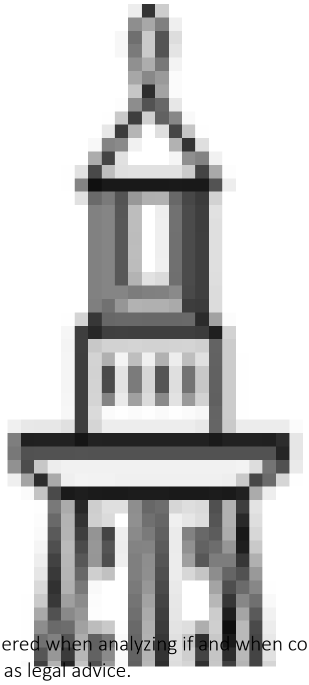
There is also widespread confusion around when 42 CFR Part 2 protections apply. The Part 2 privacy protections for SUD records were authorized due to concerns that such information could be used in non-clinical settings (e.g., criminal hearings), and could have adverse outcomes on hearings related to divorce, employment disputes or child custody.

The regulation covers records created in Part 2 programs and those entities defined in the regulation. And it requires consent that identifies individuals and organizations able to receive the information, the type of information that a Part 2 Program may be able to share, and the purpose of the disclosure.

However, the same patient data (for example, name, address and age) coming from a Part 2 program will require a patient's express, written consent to share, but from a HIPAA-Covered Entity that is not a Part 2 program, no authorization to share the same data would be required. Patients receiving treatment at a Part 2 Program may tell that program's provider that they want their information shared (for example, with a social service organization) but those patients frequently run into providers' consent policies and practices, which slow down or even prevent sharing or receiving the information needed to receive care or assistance.

A separate but related wrinkle Is that few privacy statutes or regulations explicitly speak to how they interact with others when more than one law or regulation may apply to the information to be shared. For example, while the Head Start regulatory privacy protections explicitly defer to the confidentiality provisions in FERPA and IDEA (on the occasions when the Head Start program is subject to either statute), the more-common scenario is the awkward dance of the health information privacy regulations relating to 42 CFR Part 2 [Code of Federal Regulations] and the HIPAA Privacy Rule.

Thus, the opaque nature of the laws' interconnectedness, along with concern by those who share the data that they will be liable for non-compliance, combine to restrain greater data sharing within healthcare and across all sectors.



This graphic is intended to show that multiple factors should be considered when analyzing if and when consent is needed to share data. It does not necessarily include all relevant factors or applicable laws, and it should not be relied upon as legal advice.

CREDIT: Intrepid Ascent, Aurerra Health Group

Evolution of Technologies: Balancing Distrust with Desire to Share

As laws were passed and regulations evolved to create additional levels of consent needed to share specified types of information, like the confidentiality of SUD patient records called for in 42 CFR Part 2, standards and technologies have needed to evolve.[24] Many HIEs initially refused to support the exchange of Part 2 records due to the lack of mature technologies that could enforce consent and redact information from Part 2 providers, effectively impeding the maturity of adopting new data-consent standards.

> **'The move to pay for healthcare based on outcomes (value-based care) has led more providers to recognize SDOH and to partner with social services to address non-clinical factors such as nutrition, housing and other social needs.'**

While adoption has been slow, a variety of healthcare open-data standards have emerged to track and enforce patient consent across health IT systems. The Integrating the Health Enterprise (IHE) Basic Patient Privacy Consent (BPPC) (now revised as the Advanced Patient Privacy Consent), as well as Health Level Seven (HL7) version 2, version 3 and FHIR standards, have emerged to meet the needs of the industry.

In January 2013, the first version of Consent2Share was released by SAMSHA to enable Part 2 providers to track consent and redact Consolidated Clinical Document Architecture (CDDA) documents when substance use data should not be sent. In 2019, the LEAP initiative selected San Diego Health Connect to build a FHIR-based consent decision service for enforcing patient consent authorization, which included consent privacy (share, or update patient data), consent for treatment, consent for research and consent directives.

More information about San Diego LEAP is in the Promising Practices section of this report.

The move to pay for healthcare based on outcomes (value-based care) has led more providers to recognize SDOH and to partner with social services to address non-clinical factors such as nutrition, housing and other social needs. At the same time, sophisticated and increasingly ubiquitous technologies for the collection of personal data, as well as numerous large-scale data breaches, have kept privacy and security at center stage.[25] The combination has resulted in more distrust of data-collection efforts even as more sensitive individual data is collected.

From a legal perspective, the following recommendations would enable an environment in which data sharing across sectors could become less precarious:

- Develop and institute a legal standard and technical process – such as the CSU – for sharing personal data across sectors when individual consent is required.
- Include language in pending HIPAA Privacy Rule amendments to clarify and reinforce the permissible sharing of health-related PHI for care coordination with non-covered entities
- Standardize the consent provisions of HIPAA and CFR Part 2 to reduce SUD stigma.
- Provide model language/consent forms that meet requirements for multiple state and federal laws and include the roles of healthcare and human services providers, schools, and other organizations, systems and domains that address individuals' social needs.
- Advocate for a FERPA exception that allows for bulk reporting of attendance data ("record of student absences") to enable routine transfer of personally identifiable attendance data for all children in a district. Perhaps using an opt-out approach, this exception could facilitate a way to operationalize a computable consent API for use by all the various school information system providers securely, efficiently and responsibly.

[24] McCarty D, Rieckmann T, Baker RL, McConnell KJ. The Perceived Impact of 42 CFR Part 2 on Coordination and Integration of Care: A Qualitative Analysis. Psychiatr Serv. 2017;68(3):245-249. doi:10.1176/appi.ps.201600138

[25] Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," MIS Quarterly, https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Beyond_the_Privacy_Paradox_Objective_Published.pdf

SHIG: A Possible Framework for Consent Laws and Regulations

The California State Health Information Guidance (SHIG) provides a useful, extensible model and templates for addressing federal and state privacy requirements for a group of complicated and relevant use cases. This approach provides guidance to help agencies and programs understand their requirements and to translate them into solutions.

> **'A framework for collecting and defining applicable laws and regulations would improve clarity about their implications, and it would thereby reduce the time and cost of collecting information across multiple systems.'**

Part of the challenge in coming to broad agreements like SHIG for consent and data access is the lack of a shared language. A framework for collecting and defining applicable laws and regulations would improve clarity about their implications, and it would thereby reduce the time and cost of collecting information across multiple systems. A review of the laws and data included in consent standards indicates the following healthcare and social services information is often addressed:

- **Data Category.** What type of data is being requested?
- **Data Stewards.** What organizations and people (by job title) are bound by this law as the stewards of the data? This usually limits the organizations receiving federal or state funding for a type of program (e.g., FERPA for educational programs).
- **Data Requester.** What organizations, or people (by job title) are making a request or receiving data from the data steward? These organizations are clearly broken down by who can access the data with or without consent.
- **Allowable Purpose(s) for Data Request/Use.** For what purpose(s) may certain organizations or people access the data with consent?
- **Consent Type.** What type of consent is being regulated by this law: privacy (i.e., personal data), treatment or research?
- **Consent Actions.** If privacy, consent actions that are governed: collection, access, use, disclosure, correction.
- **Consent Exceptions.** For what purpose(s) may certain organizations or people access the data without consent?
- **Compound/Separate Consent.** Can this consent be combined with other consent agreements, or must the person authorizing consent sign separately?
- **Obligations (Systems Exchanging Data).** Regulations sometimes outline obligations systems exchanging data must comply with. These could range from security measures like type of encryption, redaction, pseudonymization or deidentification of the personal identifiable information and standards for that deidentification.
- **Obligations (Organizations)**. What obligations must the organizations sharing or receiving the data meet in order to share? For example, a written data-sharing agreement must be in place, or an annual review must be conducted.
- **Law or Regulation Governing Consent**. What federal or state statutes apply?
- **Authority**. What body is the regulating authority (e.g., a government agency)?

The above is a straightforward framework for how laws and regulations could be summarized in a readable, easily understandable and computable way, and could be used by systems to update a person's consent.

While identifying potential value sets that align with the laws and regulations across education, human services and criminal courts may seem infeasible, the FHIR Consent resource incorporates most of the legal components identified above. It includes value sets relevant to healthcare consent interoperability, which can be a model for other domains.

Technical Issues and Considerations

As previously discussed, data sharing and enhanced interoperability depend on obtaining informed consent from individuals and/or guardians to enable management of the disclosure and revocation process over the life of a case. Effectively testing and building consent services – ones that act as a ubiquitous utility to manage consent across multiple service domains, such as healthcare, public health, social services and education – will require addressing a variety of technical issues essential to virtually all interoperability efforts.

> ‘A common consent service could dramatically reduce the costs of auditing potential violations of HIPAA and other laws impacting consent and data access.’

These include the establishment of one or more standards for nailing down personal and organizational identity. A broadly accepted National Provider Directory, for example, would support multiple “endpoints” (e.g., FHIR, HL7v2, Direct Secure Messages, etc.) of standards for exchanging data across systems.

Such a directory could provide standardized definitions of organizational types, which would align with those governed by related privacy and consent laws. For example, an organization may provide educational services, but if its federal funding is through Head Start without Education Department funds, the privacy regulations guiding consent and data access fall under the Head Start Act.

Health Level 7 International is defining a standard for a federated directory of healthcare providers based on requirements defined by the ONC FHIR at Scale Taskforce. This standard could be extended to enable an operational National Provider Directory to store the consent policies by which each organization is able to access data.

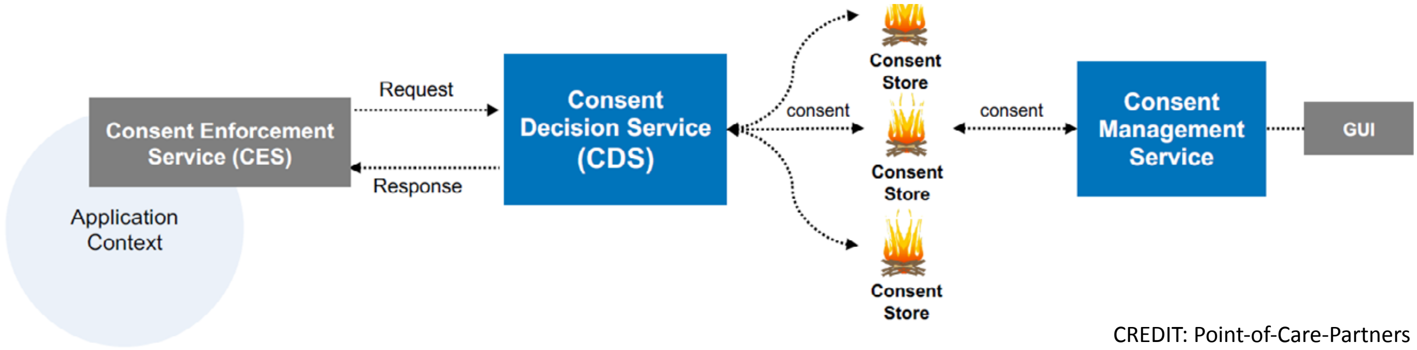
Based on the interviews we conducted across SDOH industry segments for the Promising Practices section of this document, as well as our own work with current standards efforts and industry consortia, the contributors to this report conclude that common consent services could address several interrelated challenges:

One-Stop Destination for Managing Consents. A common consent service could provide individuals with a single interface to view existing consents, approve or decline requests to access information, and revoke ongoing access to their personal information. Currently, patients/clients aren’t aware of which or how many systems have their information, how their information is being used by those systems, or how to manage their privacy preferences and consents for their information in those systems.

Consent Enforcement. A common consent service could enforce consent across systems. Currently, because the use of and access to PII and PHI often relies on consent collected (and not revoked) in one system, revocation can create inconsistencies in assertions across those systems, and thus not enforce a person’s decisions.

Such a service would reduce human errors that violate privacy and security laws by providing a common, trusted enforcement of data exchange across systems. Currently, the sophistication of consent functionality varies across software applications. Therefore, enforcement often relies on legally binding agreements for being aware of and following complex consent and data-access laws and regulations.

Automated Algorithm-Driven Audits. A common consent service could dramatically reduce the costs of auditing potential violations of HIPAA and other laws impacting consent and data access. Relying on an external authority means there is a single source of truth, built in data provenance, that identifies what information was authorized to be sent to whom, for what purpose and with



CREDIT: Point-of-Care-Partners

what obligations (e.g. redaction, encryption etc.), according to what laws.

While audits via dashboards for regulators and algorithmic audits would not cover all possible violations, they would minimize the type of computer forensic analysis, which is more costly because consent functionality is implemented differently on each system.

Recent work in the healthcare industry suggests that distributed consent "stores" associated with individual end systems can be federated by a common consent-management service. This solution would give individuals one means through which to manage all their consents across all organization-specific, geography-specific and/or domain-specific information systems.

The same federation would enable common consent-decision services to aggregate individual consent decisions from across the many consent stores, and thus enable them to calculate consent assertions for organizations that wish to access or share protected information. Bringing together these distributed, federated services as a common virtual utility would enable simplified consent management by the individual, while permitting more-sophisticated consent determination by the systems charged with protecting that person's far-flung personal data.

As envisioned by "HL7 Services Functional Model: Consent Management Service, Release 1," common consent services would be based on industry technical standards, as well as relevant federal, state, local and agency laws, regulations and policies for each consented domain (e.g. child welfare).[26]

Dependent Standards

In the absence of other domain-specific standards, a multi-domain common consent service would be based on some subset of the following healthcare consent standards, with possible extensions or profiles to meet the needs of non-health domains. These include, but are not limited to:

[26] HL7 International, "HL7 Services Functional Model: Consent Management Service, Release 1," 2021, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=571

- HL7 FHIR Security and Privacy Module (http://hl7.org/fhir/secpriv-module.html)
- HL7 FHIR Security (http://hl7.org/fhir/security.html)
- HL7 FHIR Consent Resource (https://www.hl7.org/fhir/consent.html)
- HL7 FHIR Data Segmentation for Privacy (https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/)
- HL7 FHIR Security Labels (http://hl7.org/fhir/security-labels.html#6.1.1)
- HL7 Consent Management Service Functional Model [based on CDS LEAP] (https://confluence.hl7.org/download/attachments/82910587/HL7_SFM_CONSMGMT_R1_D1_2021Jul.
- Consent2Share FHIR Consent Implementation Guide (https://confluence.hl7.org/download/attachments/58657234/Consent2Share%20FHIR%20%20Profile%20Design.
- (CDA) HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 (http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345)
- (CDA) HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (http://www.hl7.org/implement/standards/product_brief.fm?product_id=354)
- IHE Basic Patient Privacy Consents (https://wiki.ihe.net/index.php/Basic_Patient_Privacy_Consents)

Dependent Technologies

A common consent service would also be dependent upon and require standards and technology from a range of associated services and sub-components, such as:

Privacy and Consent Assertions and Rules. Sensitive health information includes conditions and related treatment data that receive special protection under specific laws, beyond the protection afforded to all electronic health data under HIPAA. An example of sensitive health information is SUD treatment data protected under 42 CFR Part 2. As adoption of standards-based information exchange grows, sensitive health data is too often excluded from electronic exchange, meaning a healthcare provider may not have all the relevant information at the point of care. This can lead to a lower quality of services for the patient and/or to redundant, unnecessary or harmful care.

The Data Segmentation for Privacy (DS4P) standards allow a provider to tag a healthcare record (FHIR Resource or Consolidated-Clinical Document Architecture document) with privacy security labels (metadata) that express data classification and possible redisclosure restrictions placed by applicable law. Using security labels is an essential part of the Share with Protection paradigm by enabling information to be exchanged after assigning the security labels specifying how it can be used and the restrictions to which it may be subject.[27]

These tagged records and documents may then be interpreted by a common consent service based on assertions created by the individual associated with the information and on rules defined for the associated information domain laws, regulations and organizational policy. Consent assertions may be created through the FHIR Consent Resource, but they may be represented internally as XML Access Control Markup Language (XACML) rules.

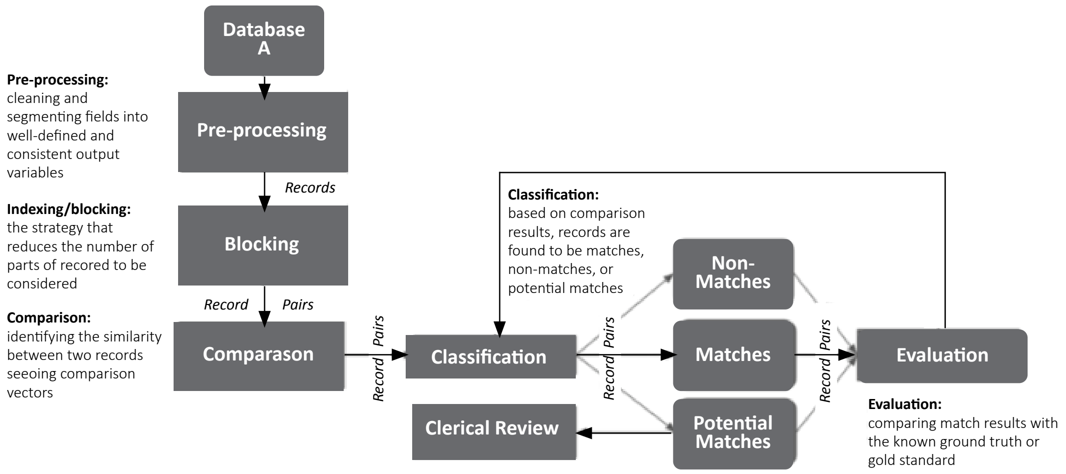
Other rules systems, such as Drools, may be used for managing business rules associated with the enforcement processes of the information and its associated consent assertions. These rules representations are internal to the implementation of any common consent service.

Identity Management. Trusted solutions for patient and provider identity are central to the creation of a comprehensive record that reflects a patient's medical history, current care team, and all education and human services programs/services that person is receiving.

Within the healthcare industry, the federal government maintains a National Provider Identity (NPI) registry for individuals practicing as sole proprietors (NPI Type 1) and organizations when an individual incorporates into a group practice. These data can be freely downloaded or accessed via an open API. The HL7 Patient Administration Workgroup has sponsored a project to establish a federated National Healthcare Directory that would use the FHIR standard to represent validated endpoints for healthcare and non-clinical providers involved in patient care.

[27] Kathleen Connor, "Share with Protections White Paper Project," 2021, https://confluence.hl7.org/display/SEC/Share+with+Protections+White+Paper+Project

Basic Record Linkage



Pre-processing: cleaning and segmenting fields into well-defined and consistent output variables

Indexing/blocking: the strategy that reduces the number of parts of recored to be considered

Comparison: identifying the similarity between two records seeoing comparison vectors

Classification: based on comparison results, records are found to be matches, non-matches, or potential matches

Evaluation: comparing match results with the known ground truth or gold standard

(Adapted from Christen et al. 2002, 2004, 2012)

These could be used in combination with an electronic endpoint that is associated with updating the system with any new consent status or request to access records. Such a standard could be extended to support the systems and standards used in non-clinical domains. Each domain would need to design a process to validate new organizations wishing to participate in a common consent service. This process could include new standards for organizational identifiers comparable to healthcare's NPI number, which could be issued to human services providers, school systems, courts and other participating entities.

Challenges in matching patient identities across health records lead to a number of problems:

Inconvenience for patients because they are asked to sign additional consent forms.

Violations of privacy when, for example, breaches lead to the wrong patient being billed or the wrong next of kin being notified if the patient experiences an emergency.

Lack of care coordination because a clinician is not able to obtain a patient's record, even though consent has been provided.

Harmful medical mistakes, such as when a medication is prescribed to which the patient is allergic because an identity match was done incorrectly.[28]

Person/Patient Identifiers

A digital identity is the unique representation of an entity within a particular digital context. The National Institute of Standards and Technology (NIST) defines digital identity as "the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known."[29] The International Telecommunication Union (ITU) definition is: "A digital representation of the information known about a specific individual, group, or organization."[30]

Kim Cameron defines digital identity as "a set of claims made by one digital subject about itself or another digital subject."[31] He also introduces the Seven Laws of Identity, which are:

[28] AHIMA. "Limiting the Use of the Social Security Number in Healthcare" Journal of AHIMA 82, no.6 (June 2011): https://library.ahima.org/doc?oid=104465, 52-56.

[29] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, "Digital Identity Guidelines," NIST Special Publication 800-63, Revision 3, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html

[30] Uyen Trang Nguyen and Aijun An, "A Survey of Self-Sovereign Identity Ecosystem," Security and Communications Network, 2021, https://www.hindawi.com/journals/scn/2021/8873429/

[31] Kim Cameron, "The Laws of Identity," Architect of Identity and Access Microsoft Corporation, http://www.ict-21.ch/ICT.SATW.CH/IMG/Kim_Cameron_Law_of_Identity.pdf

1. Users should be in control of how their identity information is shared.
2. The amount of information disclosed should only be the minimum necessary amount required, and data should not be kept longer than needed by the other entities.
3. The user should be well informed about which entities manage their identity information.
4. The user's information should not be created or exposed in such a way as to allow data correlation, pattern recognition or entity identification by unauthorized entities.
5. Interoperability and seamless integration among various entities supported by different architecture should be possible.
6. Reliable, secure integration between human users and machines should be empowered.
7. There should be consistent user experience across multiple contexts and technologies.

Currently, patient identifiers are created by each health IT system and reconciled by Enterprise Master Patient Indexes (EMPIs) based on matching demographic information that patients provide at the point of care. Health IT systems use algorithms to probabilistically match patient records.

Proprietary patient-matching algorithms mean the degree of confidence in patient matching cannot be verified. Moreover, there are no nationally agreed-upon standards about which identifiers, (e.g., name, date of birth, address, phone number, etc.) or how many identifiers should be required for the matching of patient records.

The 21st Century Cures Act and Patient Access Rule requires providers and health IT systems to make patients' medical data available in an app of their choice. However, the lack of a common way of authenticating patient identity (i.e., single sign-on) makes the process of accessing data across systems very burdensome for patients.

That problem could be addressed by an agreed-upon person identifier that contains enough PII that it could be used to verify identity assertions, but would be otherwise independent of that individual's records. As a "source of truth," such a system – whether at the local, regional or national level – would need to be able to reissue a new identifier to all relevant systems if a person's identity was stolen.

An additional challenge to enabling trust and digital identity is the lack of a unique patient identifier (UPI). The passage of HIPAA in 1996 called for the creation of a UPI to accurately identify patients. However, due to ongoing confusion over privacy and security concerns, Congress has included language in every HHS appropriations bill since 1999 prohibiting the agency from spending any federal dollars to promulgate or adopt a national UPI.

Social Security numbers were created for an entirely different purpose, so there is strong opposition to using them in this way, though some providers do so as a default. To minimize public concerns regarding privacy and identity theft, the federal government and many states have enacted laws to restrict the use and disclosure of Social Security numbers.[32]

Since 2020, the **Patient ID Now Coalition** has been actively advocating to rescind the current legislative barriers and pursue the establishment of a national UPI. The US House recently passed legislation to allow HHS to fund the evaluation and adoption of a national UPI but, as of this writing, the Senate has not followed suit.

The Kantara Initiative is a consortium that works to develop standards for identity and personal data management. Kantara's Identity Assurance Framework (IAF), updated in October 2020, details levels of identity assurance and an associated certification program called Trust Marks, which is based on de-jure standards under its Trust Framework program.[33] Kantara includes digital identity and personal data User-Managed Access (UMA). UMA is an Open Authorization (OAuth)-based protocol designed to give individuals a unified control point for authorizing recipients of their digital data, content and services.

OAuth (Open Authorization) is an open standard for access delegation; it is used to grant access to an individual's information between systems without providing access to the individual's authentication information for any of the interoperating systems.

[32] AHIMA, "Limiting the Use of the Social Security Number in Healthcare," 2011, https://library.ahima.org/doc?oid=104465#.YWssTBrMK44

[33] Kantara Initiative, "Identity Assurance Framework," 2020, https://kantarainitiative.org/identity-assurance-framework/

Identity Matching. One of the most challenging aspects of consent for interoperability is person matching, meaning the ability to identify different records for the same person across multiple systems, so they can be linked to provide a more-comprehensive and holistic view of that person. Patient matching is a vexing problem even within just the domain of healthcare.

Accomplishing this critically important objective is even more challenging across domains (education, courts, etc.) because they often use different data systems, each with its own ways of identifying individuals. So, it can be very difficult to discern if Jon A. Smyth in one system is the same person as Jonathan Alex Smyth in another (much less if the last name is misspelled "Smith" in one of them). Current approaches to addressing this problem include applications of machine learning as well as human intervention.

Improvements in identity management, such as the work of Kantara, UMA and HEART, could help with cross-domain identity matching.

Trust Frameworks. When sensitive information is to be accessed or exchanged, it is the responsibility of the data steward to determine if the party that is to have access to the information is "trusted" – i.e., well-known, validated and a consented recipient of the information. Absent this trust, consent to share the information is significantly weakened.

To determine whether an information recipient is trusted can require negotiation of common mechanisms to authenticate the end-systems of a data exchange, policies and rules for the exchange, APIs and protocols for the exchange, legal contracts defining each participant's responsibilities for protecting the data, etc.

Such bilateral or multilateral agreements are time-consuming and costly to negotiate and implement because of the variety of laws governing privacy and consent across geographical jurisdictions (e.g., between systems based in California and New York), as well as for the information domains across which the data is to be exchanged (e.g., a student information system sending attendance records to a health information system).

Trust Frameworks establish a minimum set of requirements, legal obligations, policies and technical standards for interoperability between systems that wish to participate. They sign legal agreements regarding practices for security, data protection, identity proofing and interoperability. Systems can be certified that they have met these legal, policy and technical requirements for exchanging data based on a specific Trust Framework. As a result, they can reduce costs for their customers, who might otherwise need to negotiate data-sharing agreements with each of the providers with which they want to exchange data.

Elements of Trust Frameworks

Systems Integration. To enable the application and enforcement of consent, consent services need to be integrated with existing domain-specific systems (e.g., EHR, HIE, SIS, HMIS, CCWIS, etc.). The "HL7 Services Functional Model: Consent Management Service, Release 1" proposes the creation of system-specific Consent Enforcement Services that use interfaces appropriate to the information system to integrate consent enforcement with the system requiring consent.

Data Standards. The data elements available for fine-grained consent depend upon the data standards associated with health, human services and other SDOH domains. HL7 FHIR® has provided a new standard to communicate clinical, administrative and SDOH information.

FHIR is named as the required clinical interoperability standard in both the ONC 21st Century Cures Act Final Rule and the CMS Interoperability Final Rule. The role of FHIR in SDOH has not yet been explicitly addressed by ONC, but it is the basis for the newly standardized Gravity Project FHIR ClinicalCare SDOH Implementation Guide for closed-loop referrals for social services interventions.

By representing SDOH health data using the standard terminologies described above, as well as the new FHIR standard, there is the opportunity to exchange and incorporate SDOH data in clinical systems in a manner that will provide both syntactic and semantic interoperability. Nonetheless, it should not be assumed that medical systems are the hub of a community's wheel. There are systems in use by social services and behavioral healthcare providers nationally that already use native non-FHIR standards.

Some domain-specific data standards for which consent control and/or content redaction should be applied include Access 4 Learning Schools Interoperability Framework (SIF) student records, HUD Homeless Management Information System (HMIS) records and National Information Exchange Model (NIEM) messages, as well as HL7 Content Document Architecture (CDA) documents, HL7v2 messages and HL7 FHIR Resources.

SDOH-Related Terminology Standards. This portion of our scan report is derived from "Information Standardization and Use," from the HIMSS SDOH Guide.[34]

Health information and technology systems capture both data (discrete elements that are representations of physical state or direct observations such as blood pressure, lab results or heart sounds) and information (summaries of data or semantic interpretations of data such as a diagnosis of hypertension, diabetes or tachycardia).

Data and information that capture attributes of SDOH are often available in both clinical and social contexts, but the manner in which these attributes are captured will frequently differ across domains, as will the structure, syntax, taxonomy and transmission format.

While the health information and technology in use by medical providers has undergone a sequence of standardizations over the last 20 years, the tools in use by social and behavioral health service providers have not yet become standardized in the same way. Yet, in order to properly identify social needs, implement interventions and measure the positive (or negative) impact of these interventions, there needs to be a way to standardize the social, health and well-being information used in all settings, not just those in use by medical providers.

To ensure SDOH can be used by all members of the community working to address these factors, the data must be captured, represented in and exchanged using standards. The Interoperability Standards Advisory (ISA), a resource curated by the ONC, exists to "coordinate the identification, assessment and determination of recognized interoperability standards and implementation specifications for industry use to fulfill specific clinical health IT interoperability needs."

When incorporating SDOH information, it is important that the data is structured and encoded based on standard code systems and that it uses appropriate value sets. By doing so, the information becomes not only part of an interpretable resource, but also can be used by decision-support tools and provides the ability to alert service providers to social risks that may change treatment decisions.

The ISA contains a section for social, psychological and behavioral data, including code sets for factors such as food insecurity, exposure to violence, level of education and transportation insecurity. If this represents all health-related information in terminologies – such as Logical Observation Identifiers Names and Codes (LOINC), Systematized Nomenclature of Medicine (SNOMED), Current Procedural Terminology (CPT), Healthcare Common Procedure Coding System (HCPCS), International Classification of Diseases (ICD-10) and RXnorm – then clinical systems will be able to parse and interpret it.

The challenge of such a medical-centric approach is that the social and behavioral health systems used by food pantries, SUD treatment facilities, transportation providers and housing agencies may not speak in the medical domain's vocabularies.

While some of these terminologies have recently incorporated elements that represent SDOH, these efforts are nascent and have not yet fully captured the breadth of observations that will be necessary to capture and communicate the full breadth of social needs and interventions. Examples of clinical terminologies include:

1. LOINC typically represents observations and, where appropriate, the results of the observations (e.g., laboratory tests, vital signs; and, for SDOH, housing instability).
2. SNOMED-CT is used to represent medical conditions and interventions primarily for health concerns, problems and diagnoses (e.g., diabetes and chronic obstructive pulmonary disease, or COPD), services and procedures (e.g., hip replacement and immunization).
3. ICD-10-CM codes typically represent the administrative equivalent of health concerns, problems and diagnoses when communicating with a healthcare insurer.
4. CPT and HCPCS are used to represent services and procedures when communicating with a health plan.
5. RXnorm codes are used to represent a specific medication and/or allergy to a medication.
6. 211 LA County Taxonomy of Human Services (211taxonomy.org) is a classification system

[34] HIMSS, "Social Determinants of Health Guide," 2021, https://www.himss.org/resources/social-determinants-health#Part3

maintained by 211 LA County and is required by the social services information and resources industry organization AIRS as a common language for the industry. The 211 LA Taxonomy is used to index and facilitate retrieval of social resource information and associated social services interventions.

Standard syntax to exchange encoded data is essential for using SDOH by all members of a community-wide service team. Several exchange standards could support the exchange of both clinical and SDOH information. Those in use today include various health-specific HL7 standards such as HL7v2, FHIR, CDA and C-CDA, as well as the ASC X12 standards for administrative transactions (e.g., eligibility and billing).

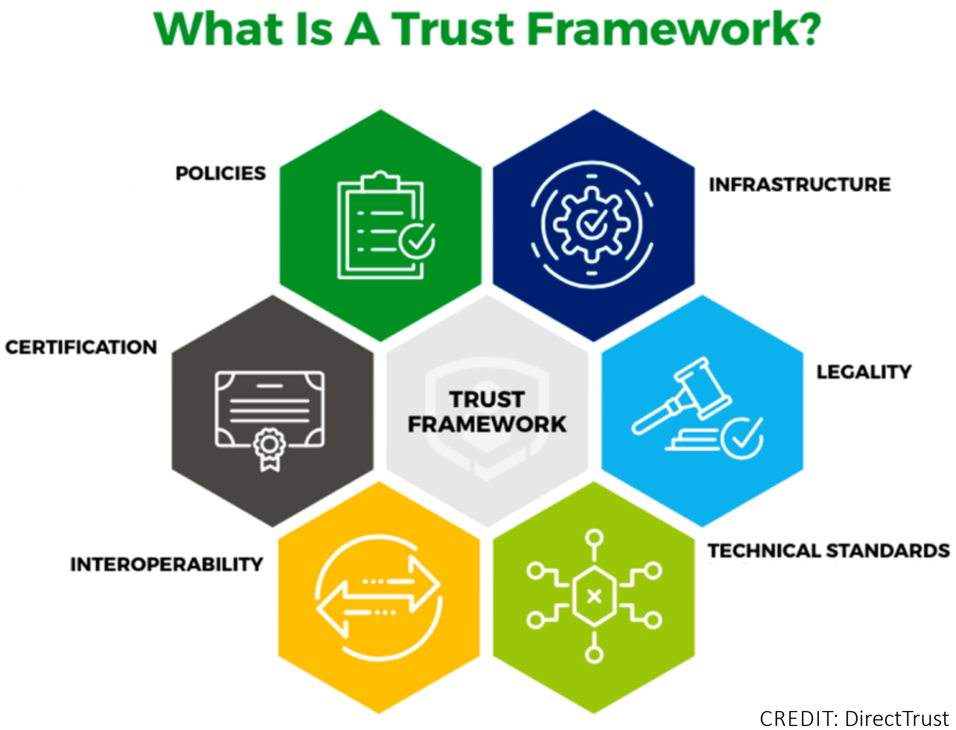
Consent Technologies

Based on the above technical standards, dependent technologies and associated open-source software efforts (e.g**.**, SAMHSA's Consent2Share, San Diego's CDS-LEAP) assessed for this report, we identified the following most-prevalent components and services required for a multi-domain common consent service:

- Consent Management Apps
    - Individual (patient/client/student/etc.) Domain Data Consent Management App
    - Provider (healthcare/social services/etc.) Domain Data Consent Management App
    - Consent Utility Administration Consent Management App
- Common Consent Services
    - Consent Management Services
    - Consent Decision Services
    - Consent Evaluation Services
    - Consent Discovery Services
    - Consent Store Services
    - Federated Consent Distributed Services
    - Consent Enforcement Services
    - Consent Redaction Service.

Consent Management Apps

A common consent service has three basic management interfaces: **apps that enable individuals to manage their privacy preferences and consent assertions** for the various domain-specific data controlled through a common consent service; **apps that enable providers of domain-specific data** to further manage provider-based policy for the access and sharing of their patients' or clients' information; and **apps that allow common consent service administrators to** manage individuals, providers and other users, as well as to enable override management of the privacy and consent information and policies managed by the utility.



CREDIT: DirectTrust

Common Consent Services

Common Consent Services provide consent management, consent decisions and consent-enforcement functionality. These services are interdependent in that their functionality depends on all of them working together. Any one service may be replaced with a new implementation, however, without impacting the system as a whole.

Consent Management Service. This is for managing multi-domain consent and privacy assertions independent of "source of truth" consent stores. There may be many consent stores for an individual's data, each representing a different provider and/or information domain. Individuals need a central service with which they can manage all their consents and privacy assertions, independent of where each is stored.

Consent Decision Service. This is for inquiring about a patient's consent in the context of a specific purpose or workflow, such as an inter-system record exchange. The Consent Decision Service uses the Consent Evaluation Service to determine responses to requests.

Consent Evaluation Service. This is for evaluating the Consent Decision Service inquiry context against the set of discoverable consent assertions to determine responses to requests for consent. It makes use of the Consent Discovery Service to identify applicable consent assertions across multiple potential consent stores.

Consent Discovery Service. This is for identifying local consent stores applicable to the context of the inquiry, then finding relevant consent assertions in those stores that match the patient/client, and then retrieving and caching those assertions.

Consent Stores Services. These enable access to relevant consent stores within existing reference information systems.

Federated Consent Distribution Services. These define and implement support for local, regional, state and federal federated, distributed common consent services based on existing consent services and consent stores.

Consent Enforcement Service. This is generally integrated with a domain-specific legacy information system (e.g., EHR system) to enable point-of-use enforcement of consent.

Consent Redaction Service. This is generally local to an information source and appropriate to the data representation of the domain (e.g., healthcare C-CDA documents). It provides a form of enforcement service by redacting information from a record or document at the time it is requested, exchanged or displayed.

Considerations for the Future

The ONC states that patients need to understand their roles and options so they make genuinely informed consent decisions; ONC refers to this as ***meaningful consent***. If patients do not fully participate, they risk having too much or too little information shared, leading to potentially negative consequences to their health and private lives. Even if consent is granted, however, there are many issues to consider and balance relating to the numerous interactions of organizations in caring for individuals and their data.

Proliferating Players and a Growing Patient Role. Stakeholders that need to manage consent effectively include health systems, providers, EHRs, HIEs, health information networks (HINS), labs, pharmacies and payers/ health plans. Organizations do not necessarily have to have direct patient interaction to be concerned with consent, as is the case with many HIEs that are not patient-facing. Patient portals and the newer world of consumer apps are access vehicles in which consent can also come into play. The recently finalized interoperability rules from CMS and ONC have a lot to say about data exchange and patient access; while they have yet to be tested, they clearly put a greater responsibility on the patient for managing consent.

More Complexities and Serious Consequences. Organizations implementing an effective consent process, including appropriate sharing among multiple stakeholders, face an increasingly complex task. Those without the needed policy/regulatory knowledge, systems, technologies, processes and workflows to enable meaningful patient consent may suffer serious repercussions such as lawsuits, fines, loss of accreditation and reduction in public trust. They may also experience losses of revenue, patients, value-based care payments and other incentives. Even more broadly, poor consent management by industry players could fuel the establishment of even greater future barriers and regulations for the sharing of important data.

Finding the Right Balance to Optimize Results. Effective, meaningful consent that supports data sharing requires a balance between patients' willingness to allow sharing of their private information; the need for providers and other stakeholders to access data to impact clinical outcomes, population health and the patient experience; and patients' desire and ability to play a larger role. Better use of technology and processes for consent can enhance effectiveness and efficiency for stakeholders at all levels.

Leveraging the expertise of a team that understands stakeholder alignment and consent-management strategy, while also being skilled in development and deployment, contributes greatly to the success of a consent program.

Applying Healthcare's Lessons to SDOH and Social Services Domains. The considerations outlined above (proliferating players, growing patient/individual roles, more complexities and consequences, finding balances) are drawn primarily from healthcare. But they clearly also apply to other programs, systems and domains that impact people's health and well-being. Indeed, as SDOH factors are increasingly accepted as pivotal – and are increasingly integrated into holistic, person-centered care as a result – consent-related concerns and processes will have to be discussed, decided and incorporated more extensively.

In other words, things are likely to get more complicated in the years to come, so establishing more-efficacious, replicable processes sooner rather than later will benefit everyone concerned.

> **'SSI is a model in which identity holders have broader control over their information and are more empowered to decide how and under what conditions it can be shared.'**

Health-centricity of Current Consent Sharing Artifacts. The majority of existing consent sharing artifacts, and their current trajectory, have been created by the health standards community for health applications. However, participatory inclusion of social services representatives is critical to the wider applicability of common consent services. For example, FHIR consent terminology may not have clear analogs to other social services domain terminology. To address this potential technical standards problem, social services stakeholders (representing housing, workforce development, child welfare, education, nutrition, victim services, legal assistance, etc.) need to be included in efforts to define common consent sharing.

A Model for Future Consideration: Self-Sovereign Identity. One of the most-promising consent approaches we identified during our scan – that's not yet in practice – is self-sovereign identity (SSI), which its developers describe as the next step in the continuum of centralized, federated identity models. Also known as self-managed identity and user-controlled identity, SSI is a model in which identity holders have broader control over their information and

are more empowered to decide how and under what conditions it can be shared.

In a 2016 blog, “The Path to Self-Sovereign Identity” by Christopher Allen, the technologist/entrepreneur describes SSI’s intent as follows: “. . . The user must be central to the administration of identity.[35] That requires not just the interoperability of a user’s identity across multiple locations, with the user’s consent, but also true user control of that digital identity, creating user autonomy.

To accomplish this, a self-sovereign identity must be transportable; it cannot be locked down to one site or locale. A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying information or facts about personal capability or group membership. It can even contain information about the user that was asserted by other persons or groups.”

Allen lists 10 principles for an SSI system, which are abbreviated here:

1. Users must have an independent existence.
2. Users must control their identities.
3. Users must have access to their own data.
4. Systems and algorithms must be transparent.”
5. Identities must be long-lived.
6. Information and services about identity must be transportable.
7. Identities should be as widely usable as possible (interoperability).
8. Users must agree to the use of their identity.
9. Disclosure of claims must be minimized.
10. The rights of users must be protected.

[35] Christopher Allen, “The Path to Self-Sovereign Identity,” 2016, https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Discussion and Analysis

TEFCA is an important consideration for the future of data sharing, but it is not yet operational. The Common Agreement part of it is not yet drafted; only now are the elements of what the agreement might contain being opened for stakeholder feedback. It is also yet to be seen who exactly will sign up to be a Qualified Health Information Network (QHIN), as very specific requirements will have to be met. Not every organization will have the ability to jump in as a QHIN. Some HIE's are actively focused on TEFCA and positioning themselves to become QHINs once that opportunity is real. This work has mainly been focused on health data.

A Consent Service Utility (CSU) would accelerate data-driven partnerships by healthcare, social/human services providers, schools and other organizations to deliver more holistic, person-centered care. A CSU would also provide people with a single interface to authorize, review and revoke their sharing of data, enabling people to control their data and authorize individual apps of their choice to use it. Existing efforts have focused on standardizing social needs and interventions data, including identifying proven assessments for identifying needs and standardized program definitions and models for closed loop referrals.

To maximize the opportunities for these partnerships, future standards efforts should identify other types of data exchange, like alerts in a school nurse's software on a student's COVID-19 diagnosis, or consent-driven data exchange initiated outside of the clinical organization that must comply with non-clinical consent laws.

While a variety of semantic standards exist to define education and human services data, the immaturity of these standards may make it difficult for people to easily share non-healthcare data with the level of granularity that can be the case with healthcare data because standards are more mature.

Consent2Share and CDS LEAP offer the robust ability to enforce granular patient consent decisions, but they rely on data to be coded/standardized, so that sensitive information can be identified and redacted.

When data is not coded/standardized, like unstructured notes, the data are eliminated. Moreover, even accurate redaction of words or phrases may not be enough to protect a person's privacy because human readers, based on context, can often guess what words were redacted. Because data standards in social and education domains are less comprehensive and used, providing granular level control will be more challenging.

Leveraging and extending machine learning and natural language processing approaches, which are being developed by the PP2PI Workgroup, remain promising areas of technology that could begin to address these challenges. Until people's consent wishes can be enforced on a granular level, those with sensitive information will face health inequities because they may have to decide between protecting their privacy and improving their care.

Modernizing consent requires policymakers, standards development organizations, technology companies, service providers, and other stakeholders to solve a number of related and interrelated trust and data governance challenges that will enable highly secure, affordable, data exchange. Within healthcare IT systems, consent functionality is enforced without consistently embracing consent data standards. The exchange of health information is constrained by data-sharing agreements or trust frameworks that outline associated legal and policy requirements.

> **'Until people's consent wishes can be enforced on a granular level, those with sensitive information will face health inequities because they may have to decide between protecting their privacy and improving their care.'**

Consent2Share and San Diego Health Connect's Consent Decision Service were created as external services that could be used within health IT systems or as external trusted consent authorities that can receive updates to consents provided by a regional or statewide consortium of providers. Relying on an external source for tracking and enforcing consent has significant benefits, but this model may be difficult for others to adopt or adapt, as it goes against the current culture of controlling data sharing within a technology team building a Health IT system or a clinical team using a Health IT system.

Recommendations

1. The dozens of participants in this project, led by SOCI, should collaboratively plan and carry out a series of activities throughout 2021 and 2022 (and beyond) to advance the information, insights and learnings reflected in this report. These activities will lead up to an SOCI-organized symposium in mid-2022 and will include but not be limited to:

   - Extensive dissemination of this report through social media, blogs and webinars, among other channels, by SOCI and its extensive network of partners, collaborators and supporters.
   - Continued regular meetings of the extraordinary, expansive group of participants in this project to maintain and expand cross-sector relationships/communities; develop and advance ideas and initiatives; and ensure that the work already done will continue to grow and become increasingly impactful over time, rather than be allowed to dissipate.
   - Regular updates to this scan report, which will be posted on SOCI's website. This is necessary because the work it discusses and highlights is dynamic, fluid and ongoing; that is, it only provides a snapshot in time if it isn't regularly updated.

2. Remediating socioeconomic and racial disparities, as well as furthering trust and health equity, should be built into the framework of all the activities outlined in these recommendations. In order to surmount the hurdles that cultural, racial, economic and social disparities have erected over time, an integral component of this effort should be the related recommendation immediately below.

3. The participation of "People with Lived Expertise" should be increasingly, meaningfully incorporated into current and future efforts relating to consent (as well as other efforts affecting them) to assure that their insights and influence are integral to programmatic planning, decision-making and implementation of this work. To ensure progress on Recommendations #2 and #3, the following activities – among many others – should be undertaken:

   - Organize and regularly convene community voices/advocates and people with lived expertise in all possible, relevant elements of our individual and collective work.
   - Develop and promote policies and practices that explicitly provide the most benefits to those who have had the fewest advantages and opportunities.
   - Obtain funding to ensure that the above steps, and others to further the same aims, can be taken by (for example) providing stipends for participants – as well as funding for community-based organizations that serve marginalized populations.

4. A widely marketed webinar "learning series" should be organized to begin soon after publication of this report, and to continue until the 2022 symposium, and hopefully longer dependent on resources. This series should include but not be limited to:

   - A "launch" webinar to highlight key content and potential impact of the scan.
   - Individual, targeted webinars on the scan's sections, including Legal and Technical Issues and Considerations.
   - At least one "connect-a-thon" giving attendees the opportunity to "play in the sandbox" of ideas, technologies and proofs of concept reflected in this report.
   - A webinar focusing on the Consent Service Utility being developed by SOCI and its partners (discussed in this report and in a separate recommendation below).
   - At least three webinars relating to the symposium – to help shape its content, to provide a preview of it and to recap it (and present it to new audiences) afterward.

5. SOCI and its collaborators should continue and accelerate development, testing and proof-of-concept implementations of its open-source, standards-compliant Consent Service Utility (CSU) as a key part of implementing the legal, governance and technical guidance in this report. The goal is to make the CSU available to all patients/clients in our

country and to every authorized provider, payer and government agency offering them assistance.

6. A symposium should be planned, organized and staged in mid-2022 to share the ideas and insights reflected in this report, as well as additional ones generated by the activities above. The primary objectives of the symposium should include but not be limited to:

    - Shaping actionable next steps, just as SOCI's last symposium (the National Action Agenda to Advance Upstream Social Determinants and Health Equity) led to its consent efforts, including the scan and this report.

    - Highlighting, promoting and evangelizing the importance of integrating social services into education, policy and practice at all levels to truly improve outcomes and further equity. Indeed, this should be an objective of all our associated efforts.

7. The ONC and other federal agencies, pointedly including ones that focus on SDOH and not just healthcare, should launch regular meetings on consent and data sharing. The new SDOH Congressional Caucus should be a key participant, along with others in government and industry. The goals of these discussions would include but not be limited to:

    - For the first time, bring to the table all the high-level players who significantly impact health and well-being. The optics and reality of doing so would be powerful.

    - Elevate and highlight the importance of cross-sector data sharing to an unprecedented level, including the pivotal role of informed consent, and accelerate progress as a result.

    - Develop policy and practice recommendations – as well as specific actions – to "set the playing field" and help steer states and others seeking guidance from the top.

    - Develop policy and guidance recommendations to accomplish specific goals, such as minimizing and eliminating silos (in funding and functions); re-educating relevant professionals in and out of government about HIPAA, FERPA, Part 2 and other statues that are too-often mistakenly used to obstruct responsible data sharing.

    - Discuss the allotment of federal dollars for organizations and projects that are conducting the transformative work discussed throughout this report.

8. The InCK sites should be utilized as a national model for developing, testing and implementing the modernization of consent practices across programs, systems and domains – as well as for cross-sector information sharing more broadly. A host of actions would need to be undertaken to make this happen, including but not limited to:

    - Increased funding to the sites, primarily from federal sources.

    - Collaboration and learning with others doing comparable work; examples include juvenile justice and social services programs around the country.

9. The SHIG collaboration in California should be explored as a potential model for customization by other states (using their own laws) to expedite their ability to understand and train staff about their privacy requirements.

10. States and federal agencies, as well as industry, should provide funding to further all of the work suggested above, starting with dissemination of this report and the activities leading up to and including the symposium in mid-2021. At that point, there should be an assessment to gauge efficacy and determine what level of support should continue.

APPENDICIES FOLLOW

APPENDIX A: GLOSSARY

42 CFR Part 2. This is an abbreviation for Section 42 of the Code of Federal Regulations, Part 2. It is the federal law protecting the confidentiality of Substance Use Disorder (SUD) patient records, enacted in the 1970s to encourage people dealing with addiction to start and continue treatment. View more information here, including an explanation of recent revisions to the law.

Accountable Care Organizations. These are groups of doctors, hospitals and other healthcare providers who come together voluntarily to provide coordinated care to their Medicare patients. View more information here.

Authentication and Trust Services (EU eIDas). This is a regulatory framework defined by the European Union for electronic IDentification and authentication services (eIDas). View more information here.

Blockchain. This is a technology that enables the recording of data so that sensitive information (e.g. patient records) is resistant to change, can be verified and can be protected. View more information here.

Blue Button 2.0. This is a standards-based application programming interface (API) that delivers Medicare Part A, B and D data for over 60 million people in the Medicare program. View more information here.

California Consumer Privacy Act (CCPA). This landmark law, which took effect on January 1, 2020, provides enhanced privacy rights for state residents relating to the collection and use of their personal data. View more information here, including the obligations CCPA places on entities that collect data.

CARIN Alliance. This is an abbreviation for the Creating Access to Real-time Information Now through Consumer Directed Exchange. It is a bipartisan, multi-sector group – made up of consumers, HIPAA-covered entities and non-covered entities – working collaboratively to advance the ability of individuals and their authorized caregivers to share digital health data. View more information here.

Clinical Document Architecture (CDA). This is a base standard that provides a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents. View more information here, including about Consolidated CDA (C-CDA).

Code Set. This is a shared list of codes used in place of longer names or explanations. For example, the US Department of Health and Human Services adopted specific code sets to reduce confusion about which codes should be used in electronic healthcare transactions. View more information here.

Consent. In the context of the SOCI scan report, this is the process by which individuals (patients/clients/customers) provide their approval or denial for actions relating to four "categories." They are: consent to share personal information; consent to a treatment, procedure or service; consent to participate in research; and consent to a directive for future medical care. View more information here and here and here.

Consent Service Utility. This is a systems-change technical approach being developed by SOCI and its collaborators to modernize the processes by which individuals allow or deny the sharing of their personal information across programs, sectors and domains (healthcare, behavioral health, education, social services, etc.). View more information here.

Consent Store. This is a definitive source of consent records associated with potentially sensitive information. View more information here.

eXtensible Access Control Markup Language (XAML). This standard defines a fine-grained, attribute-based access-control policy language, an architecture and a processing model describing how to evaluate access requests according to rules defined in policies. View more information here.

Family Educational Rights and Privacy Act (FERPA). This federal law gives parents the right to access their children's education records, to have those records amended and to have some control over the disclosure of personally identifiable information. Rights under FERPA transfer to students when they turn 18 or enter a postsecondary institution at any age. View more information here.

Fast Healthcare Interoperability Resources (FHIR). This is a standard describing data formats and elements and an API for exchanging electronic health records. The standard was created by the Health Level 7 International (HL7) standards organization. View more information here.

FHIR at Scale Task Force (FAST). This initiative of the Office of the National Coordinator for Health IT (ONC) brings together healthcare **industry** stakeholders and health information technology experts to identify FHIR scalability gaps and to define solutions to address barriers and identify needed infrastructure for scalable FHIR solutions. View more information here.

Fine-Grained (or Granular) Consent. Fine-grained Consent enables decisions about access to record or document level and the data element level within a record or document. Fine-grained Consent is often implemented using integral privacy marking of data. View more information here.

General Data Protection Regulation (GDPR). This is a tough privacy and security law that went into effect in the European Union in May 2018. Though it was drafted and approved by the EU, it imposes obligations onto organizations anywhere if they target or collect data related to people in the EU. Significant fines can be imposed for violations. View more information here.

Health Insurance Portability and Accountability Act (HIPAA). This federal law required the creation of national standards to protect sensitive health information from being disclosed without the patient's consent or knowledge. View more information here, including about the HIPAA Privacy Rule, HIPAA Security Rule, Covered Entities and Permitted Uses and Disclosures.

HIPAA Treatment, Payment and Operations (TPO). These are HIPAA exceptions in which a medical covered entity can share patient data with other covered entities or business associates to treat the patient, receive payment for services or engage in case management. View more information here, including specifics about HIPAA exceptions.

HL7 Da Vinci Project. This is a private-sector initiative that leverages the Health Level 7 International (HL7) FHIR platform to advance value-based (rather than fee-for-service) care. The project's goal is to help payers and providers improve clinical, quality, cost and care-management outcomes. View more information here.

Identity Management. This process includes all activities related to establishing and verifying the identity of individuals (patients, clients, etc.), as well as providers, caretakers and other stakeholders in order to accomplish aims such as controlling access to the individual's personal data; meeting legal and regulatory requirements. View more information here, particularly relating to the healthcare ecosystem.

Leading Edge Acceleration Projects in Health Information Technologies (LEAP). These are initiatives funded by the ONC to address challenges that inhibit progress in interoperable health IT. The goal is to further the development, implementation and refinement of standards, methods and techniques to overcome barriers and fuel innovation. View more information here.

Trusted Exchange Framework and Common Agreement (TEFCA). This is an ONC initiative working to outline a common set of principles, terms and conditions to support development of a single legal agreement; its goal is to enable the nationwide exchange of electronic health information across disparate health information networks. View more information here.

Trust Framework. This is a common set of agreed-upon standards for disparate entities to establish trust. Ensuring all organizations meet the same agreements and requirements allows for forgoing additional legal contracts or peer-to-peer agreements. View more information here.

Patient-Centered Medical Homes. This is a model/approach for delivering high-quality, cost-effective primary care. It is designed to provide coordinated, person-centered, culturally appropriate and team-based services across a health system. View more information here.

Social and Human Services. Collectively, these are interdisciplinary assistance programs that range from mental health counseling to child welfare work to food and shelter assistance. They are primarily offered through government and nonprofit agencies. View more information here about social services and here about human services.

Social Determinants of Health and Well-Being (SDOH). These are the environmental, societal and cultural conditions in which people are live, learn, work and play (ex., education, housing) that affect a wide range of functions relating to quality of life. SDOH are estimated to influence as much as 80 percent of a person's health and well-being outcomes, with healthcare contributing to the rest. View more information here.

Substance Use Disorder (SUD). This is a term that encompasses addiction to any legal or illegal medication or drug, including alcohol and nicotine. View more information here, including on the frequently occurring connection between SUDs and mental disorders.

Taxonomy. A taxonomy is a formal system of classification such as the different types of social services offered through a 211 (defined by the 211LA Taxonomy) or the different types of healthcare services managed through an electronic health records system (defined by SNOMED, ICD10, LOINC or NUCC taxonomies). These taxonomies are often documented in a coding system value set. View more information here

Value Sets. A value set represents the possible values of a coded data element in an information model. View more information here.

APPENDIX B: Project Methodology

To con and produce this report, SOCI took the following steps, among many others:

- Assembled dozens of subject-matter experts, technologists, organizational leaders and other relevant professionals from across the country representing industry and government at all levels, all of whom contributed their time, knowledge and resources to this effort. SOCI President Daniel Stein led this group – and the overall effort – along with a senior SOCI consultant, Adam Pertman. Two additional SOCI personnel also assisted in various aspects of the work. A list of project participants is in Appendix A.
- Held 90-minute zoom meetings weekly for several months – with about 20 participants representing multiple domains/sectors at each – to discuss and advance the numerous aspects of this work; these were in addition to regular, separate meetings of several workgroups focusing on specific aspects of the project, including identity management, authentication, security, person matching, governance and technology.
- Conducted a technical evaluation of several open-source software consent-service implementations. Those included Consent2Share by the Substance Abuse and Mental Health Services Administration (SAMHSA) and the Leading Edge Acceleration Project (LEAP) of San Diego Health Connect's Health Information Exchange.
- Created and staffed three teams of volunteer experts to examine Legal Issues, Technologies and Promising Practices. They advised SOCI and participated in many aspects of the work, such as conducting reviews of literature, practice and federal/state privacy laws; identifying resources and providing content for this report; and engaging in interviews with additional subject matter experts.
- Solicited and received agreement from two implementation partners, the federally funded Integrated Care for Kids (InCK) sites in New Jersey and New York, to incorporate members of their established networks and advisory committees of People with Lived Expertise into our work. We also reached out to additional potential implementation partners for future consent-related work, with "warm" responses from projects in California, Arizona and Connecticut.

APPENDIX C: Consent Project Participants

Christine Alibrandi, Esq., Public Health Senior Attorney, Network for Public Health Law

Noam H. Arzt, PhD, FAMIA, FHIMSS, President, HLN Consulting

Pooja Babbrah, Practice Lead, PBM Services, Point-of-Care Partners

Jennifer Bernstein, Deputy Director, Network for Public Health Law

Matt Bishop, President and CEO, Open City Labs

Duane Brown, Senior Business Analyst, Common Education Data Standards

Dan Chavez, Senior Consultant, Health Tech Solutions

Kay Chopard, Executive Director, Kantara Initiative Inc.

Jim St. Clair, Executive Director, Linux Foundation Public Health

Ed Daniels, Consultant, Point-of-Care Partners

Dr. Hannah Galvin, MD, Chief Medical Information Officer, Cambridge Health Alliance

Sid Gardner, President, Children and Family Futures

Jennifer Hall, Interoperability Product Manager, Community Partnerships, CO

Brian D. Handspicker, Managing Partner, PracticalMarkets, Inc.

Mohammad Jafari, Project Director and Principal Investigator, San Diego Health Connect

Eric Jahn, CTO/Data Architect, Alexandria Consulting

Mary-Sara Jones, State & Local Government Health & Human Services, AWS

Jung Kim, Director, Health and Human Services & Analytics, Gainwell Technologies

Bill Kowalski, Principal Business Development Manager, FEI Systems

Mary Kratz, Executive Vice President, Interoperability Institute

Nancy Lush, President, Patient Centric Solutions, Inc.

Dr. Kristine McCoy, Chair, Children and Family Health Institute, VNA Central NJ

Paul Meissner, Director, Research Program Development, Montefiore Care Management

Kathryn Miller, COO, Bronx Regional Health Information Organization

Dr. Paul Nelson, Retired Primary Care Physician

Adam Pertman, Senior Consultant, Stewards of Change Institute

Carol Robinson, CEO, CedarBridge Group, Midato Health

Kenneth Salyards, Information Technology Specialist, Administration for Children and Families

Tony Schueth, Founder, CEO & Managing Partner, Point-of-Care Partners

Michael Solomon, Practice Lead, eCare Management, Point-of-Care Partners

Daniel Stein, CEO, Stewards of Change Institute

Amanda Taylor, Consultant, Stewards of Change Institute

Madelynn Valu, Program Manager, HIMSS

Dave Walsh, Chair, Medicaid Information Technology Architecture -- Technical Architecture Committee

Michelle Zancan, RN, Health IT Outreach Specialist, Zane Networks, LLC

APPENDIX D: Resources

2014 FACA letter- Granular consent should be a priority for ONC

2015 HITSC Roadmap Transmittal Letter

211 San Diego CIE Data Equity Framework

211 San Diego CIE Toolkit

211 San Diego Presentation: Sharing Information is Easier Than You Think

Arlington County Shared Authorization to Use and Exchange Information

Breaking Down Silos: How to Share Data to Improve the Health of People Experiencing Homelessness

Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis

Covered Entities and Business Associates

Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis

Electronic Consent Management: Landscape Assessment, Challenges, and Technology

Health Care Delivery and Research Consent

Healthy People 2030: Social Determinants of Health

HHS HIPAA Information

HIEs Seeing More Reasons for States to Treat Them as Utilities

HIPAA FAQs for Professionals

HIPAA FAQ: PHI and Continuity of Care

HIPAA Privacy Rule and Care Coordination

Leveraging Community Information Exchanges for Equitable and Inclusive Data

Patient Consent for Electronic Health Information Exchange

Patient Consent for Electronic Health Information Exchange and Interoperability

Privacy, Security, and HIPAA

Privacy and Security Framework for PatientCentered Outcomes Research (PCOR): Enabling Granular Choice for

Scalable Consent Framework for the Advancement of Interoperability with FHIR-based APIs

Special Topics in Health Information Privacy

Tackling Data Dilemmas in Social Care Coordination

Toolkit for Communities Using Health Data: How to collect, use, protect, and share data responsibly

Trusted Exchange Framework and Common Agreement (TEFCA) Draft

We are working to keep the Consent Scan up to date – please visit this site for additional resources that have been identified since publication.