Prepared for

Office of the National Coordinator for Health Information Technology

Office of the Chief Privacy Officer

Electronic Consent Management: Landscape Assessment, Challenges, and Technology

Contract # TIRNO-99-00005

Task Order #D12PD01489

October 29, 2014

Version 1.0

MITRE
7515 Colshire Drive
McLean, VA 22102

Executive Summary

Consent management is a system, process, or set of policies that enables patients to choose what health information they are willing to permit their healthcare providers to access and share. Consent management allows patients to affirm their participation in electronic health initiatives such as patient portals, personal health records (PHR), and health information exchange (HIE).[1] Electronic Patient Consent Management is an attempt to balance the risks to patient privacy with the benefits of health information exchange and interoperability. This report uses the term "consent" to mean a patient's decision to permit personal health information to be accessed and shared for treatment purposes (as opposed to sharing health information for research, payment, or other purposes). Specifically, this report focuses on patient consent (1) to participate in electronic health information exchange and (2) to share sensitive health information. Generally, patient consent is not required under federal law for a provider to share information for treatment, payment, or healthcare operations purposes.[2]

In United States (US) healthcare delivery, patient consent decisions are usually captured on a paper consent form (a paper consent directive), usually at a provider's office. By contrast, electronic consent management enables this process to occur in a fully electronic manner, whereby patient consent decisions are captured in a digital format (an electronic consent directive) and various laws, regulations, and policies for access and restrictions on sharing information—particularly sensitive information—are handled in an automated way by health information technology (IT) systems. Current technologies and standards are able to support full electronic consent management, but there is no clear consensus on the identification and use of a nationwide best practice, technical method, or technical framework for electronic consent for health care treatment. This current state of technology implementation is considered against the backdrop of a complex, US privacy rules environment, where the federal HIPAA Privacy Rule identifies the minimum privacy protections, and states may and have enacted more privacy protective laws that vary widely, even among states.

This report presents the results of a policy, technical, and process landscape assessment that The MITRE Corporation conducted to determine the current state of electronic patient consent management. The objectives were to describe the environment, discuss how certain stakeholders define sensitive information, identify gaps and challenges that hinder adoption of electronic consent management technology, and discuss technologies that facilitate electronic consent management.

MITRE held informal discussions with more than 20 contributors selected from three stakeholder groups: health information organizations (HIOs),[3] healthcare providers, and health IT developers. The MITRE team also held informal discussions with various subject matter experts from federal agencies, law firms, and nonprofit interest groups. MITRE collaborated with Office of the Chief

[1] See health information exchange, available at: http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie (health information exchange means the process that enables healthcare providers and patients "to appropriately access and securely share a patient's vital medical information electronically."); see also, Consent Management, Gartner IT Glossary, available at: http://www.gartner.com/it-glossary/consent-management/.

[2] See Health Information Privacy Law and Policy, available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

[3] HIOs are entities that oversee and govern the exchange of health information under nationally recognized standards and in an authorized and secure manner. See Overview: Knowing the HIE Basics, available at: http://www.himss.org/files/HIMSSorg/content/files/AmbulatoryHIEToolkit-OverviewKnowingtheHIEBasics.pdf (hereinafter HIE Basics).

Privacy Officer (OCPO) of the Office of the National Coordinator for Health IT (ONC) during all phases of this work, from data collection through drafting the final report.

Landscape Assessment

Our discussions confirmed that paper forms are still the primary means for collecting patient consent in healthcare delivery. These paper forms could constitute an initial definition of a standard that could define the requirements for electronic patient consent management. Healthcare providers may scan consent forms into electronic health record (EHR) systems as portable document format (PDF) image files, but discrete data from these scanned forms is not machine-readable. Scanned consent forms do not contain structured electronic data, which is data that can be tagged or occupies searchable fields (e.g., name or address fields).[4] Structured data is essential for electronic consent management because health IT systems must be able to accurately identify tagged data to process patient consent decisions in an automated manner. For example, if a patient chooses not to share information about certain infections or prescriptions, or limits sharing with certain providers, health IT systems must be able to identify and process these structured data elements or fields.

Today's electronic consent management landscape can be divided into three phases. These phases represent the application of different consent models and different levels of consent management maturity:

- **Phase I – Current State**. Consent is captured on paper forms and scanned into EHR systems. These forms do not contain structured data. Provider staff must read and analyze the consent form before information is shared.
- **Phase II – Current Growth**. Consent may be collected on paper and then entered into an electronic format, or consent may be recorded digitally from the start using a tablet or web portal. Consent management is semi-automated, but usually this is limited to a digital flag that enables either all or no health information to be shared. This report discusses three HIOs that apply different methods for sharing health information, two of which most closely represent Phase II maturity.
- **Phase III – Future State**. Consent is collected electronically and structured data is captured including milestones such as:

  – Health IT technologies are able to interpret and process patient consent decisions in electronic consent directives and enforce applicable federal, state, regional, and organizational laws, regulations, and policies.

  – Consent decisions can be applied with granularity (e.g., share sexually transmitted infection results only with the primary care provider).

  Phase III capabilities are not yet widely used, but several pilot initiatives have demonstrated that patient consent can be managed in an electronic manner, and some developers are creating more sophisticated solutions.

[4] See Structured Data, available at: http://www.pcmag.com/encyclopedia/term/52162/structured-data.

Sensitive Health Information

In addition to advancing broader health information exchange, electronic consent management plays a particularly important role in the exchange of sensitive health information because it enables healthcare providers to use technology to comply with existing laws and empowers patients with the ability to decide how this information is accessed and shared. Our discussions revealed that there is no formal or common definition of sensitive information; federal and state laws usually identify what information is "sensitive enough" to require patient consent for its release. Although these laws are numerous, sensitive information usually includes information related to the following: domestic violence, genetics, mental health, reproductive health, substance abuse, and sexually transmitted infections.

Challenges

MITRE's discussions identified several challenges that may hinder greater adoption of electronic consent management:

1. *Technological Gaps*: Our discussions did not reveal gaps in technology as the sole challenge hindering the adoption of electronic consent management. Some electronic consent management can be implemented with existing technology; however, full capabilities will likely require additional standards or harmonization of existing standards. The MITRE team also identified two technology-related challenges. First, the lack of machine-readable, structured data in consent forms makes electronic consent management very difficult. Second, certain interoperability challenges are hindering adoption. For example, consent management is handled differently among providers and HIOs due to the different technologies deployed in each environment. More specifically, some providers may use EHR systems that process consent in Admit, Discharge, and Transfer (ADT) messages, while other providers may use EHR systems that use the eXtensible Access Control Markup Language (XACML), thereby potentially complicating the transfer of consent information. Additionally, the adoption of electronic consent management may be hindered by difficulty normalizing multiple semantic vocabularies.
2. *Compliance Complexity*: Our conversations identified various compliance challenges related to federal, state, and local laws, regulations, and policies; specifically, patients and providers must follow multiple compliance regimes that may conflict with one another. The compliance requirements cover both how consent is collected and what qualifies as sensitive health information. For example, existing health IT must account for multiple consent models, such as full *opt-in* or *opt-out* to participate in a health information exchange as well as *opt-in* or *opt-out* with restrictions (i.e., more granular consent). Additionally, a patient's consent rights to protect sensitive information may vary depending on jurisdiction. For example, human immunodeficiency virus (HIV) information is defined differently by state, and requirements in one state may be more relaxed or more restrictive than requirements in another state, thereby posing implementation challenges.
3. *Identity and Access Management*: Authentication and identity proofing are important when patients want to update their consent decisions remotely, especially via web portals. Patient-facing software tools that facilitate patient consent may be unattractive to providers because identity management solutions, such as multi-factor authentication, are perceived as expensive and difficult to technically implement.

4. *Cost and Sustainability*: A significant financial investment is required to deploy and maintain health IT. In particular, small practices/providers often face a disadvantage compared to larger providers, who tend to have more financial resources for technology investment and maintenance.
5. *Workflow, Trust, and Education*: Electronic consent management often requires providers to alter their customary workflows and trust in the ability of health IT systems to share health information appropriately. Additionally, our conversations revealed the need to educate patients and providers about the benefits of electronic consent management to allay privacy, security, and litigation concerns.
6. *Policy Challenges*: Although consent management technology is the focus of this report, many discussions identified policy challenges driven by federal consent rules. Specifically, consent requirements under 42 C.F.R. Part 2 (Part 2), concerning the disclosure and redisclosure of mental health and substance abuse information, are partly responsible for the exclusion of Part 2 providers from many HIOs.

Consent Management Technology

From our discussions, it is apparent that although electronic consent management is not yet common practice, organizations can leverage already existing technologies to facilitate health information sharing in accordance with patient consent decisions. One method is to convey patient consent decisions in electronic consent directives, which use structured data to help IT systems decide whether to grant or withhold consent to collect, access, use, or disclose patient health information. Electronic consent directives can be applied to existing health IT standards, like clinical document architecture (CDA) documents and XACML documents. But electronic consent directives are only one part of the larger electronic consent management process. Fully automated electronic consent management requires the use of numerous other technology standards for transport, messaging language, and vocabulary.

Pilot programs, such as the Data Segmentation for Privacy (DS4P) initiative pilots and the Substance Abuse and Mental Health Services Administration's (SAMHSA) Consent2Share Pilot Project, have demonstrated that existing technology standards can support electronic consent management, if not at the granular, data-element level, then at least at the document level. Section 5 also briefly describes three health IT solutions currently poised to provide full electronic consent management.

Suggestions

This report concludes with several suggestions that participants offered for overcoming barriers associated with implementing electronic consent management. These may be considered for further research and discussion, as they are not formal recommendations. Several participants suggested that the federal government take the lead in developing a model technical framework to address electronic consent management, given that a commonly used technical model for sharing consent information does not yet exist. Other suggestions included centralizing services, increasing patient and provider education, expanding financial incentives to adopt health IT for consent management, and reforming the Part 2 regulation.

Summary

Electronic consent management is an important objective as patient health information becomes increasingly digitized and shared. Electronic consent management can be achieved using existing technologies and standards. Various pilot programs and a growing number of developers have

demonstrated that a patient's electronic consent directive can be processed to share health information appropriately. Nevertheless, broad adoption of electronic consent management faces certain challenges. These challenges include (1) the continued reliance on paper consent directives that do not provide the necessary structured data for end-to-end automated electronic consent management, (2) an HIE ecosystem occupied by a multitude of EHR systems that may process consent differently and may lack adequate interoperability, and (3) HIOs that may employ different patient consent models. Overlay this complexity with a web of federal and state confidentiality/privacy and consent laws that lack consistent definitions of certain sensitive information that requires patient consent. The result is the currently low adoption rate for electronic consent management among HIOs, providers, and developers.

Table of Contents

1 Background 1

1.1 Purpose 1

1.2 Scope 1

1.3 Patient Consent 2

1.4 ONC Consent-Related Efforts 3

1.5 Consent Management 5

1.6 Confidentiality/Privacy Laws and Consent Laws 6

1.7 Consent Models 7

1.8 Electronic Consent Management Models 8

1.9 Sensitive Health Information 8

2 Methodology 10

2.1 Stakeholders 10

2.2 Contributors 10

2.3 Discussions 10

2.4 Limitations 11

2.5 Findings 11

3 Landscape Assessment 12

3.1 Phase I – Current State 13

3.2 Phase II – Current Growth 14

3.3 HIO Architectures and Electronic Consent Management 15

4 Gaps and Challenges 21

4.1 Technological Gaps 21

4.2 Compliance Complexity 22

4.3 Identity and Access Management (IDAM) 25

4.4 Costs and Sustainability 25

4.5 Workflow, Trust, and Education 25

4.6 Policy Challenges 26

5 Consent Management Technology 28

5.1 Consent Directives 28

5.2 Conceptual HIO Architecture 28

5.3 Common Technology Standards 30

5.4 Pilot Programs 33

5.5 Federal Efforts 35

5.6 Developer Solutions 40

6 Suggestions 42

6.1 Federal Electronic Consent Management Framework 42
6.2 Standard Sensitive Information Consent Form 42
6.3 Centralized Services 42
6.4 Education 43
6.5 Identity and Access Management (IDAM) Solutions 43
6.6 More Financial Incentives 43
6.7 42 C.F.R. Part 2 (Part 2) Reform 44
Appendix A Glossary 45
Appendix B Contributors 49
Acronyms 50

List of Figures

Figure 1. Continuity of Care Document Structure 14
Figure 2. Centralized HIO Architecture 15
Figure 3. Decentralized HIO Architecture 16
Figure 4. Decentralized NEHEN Architecture 17
Figure 5. Mass HIway Methods of Connecting 18
Figure 6. HIE Implementation Architectural View 30
Figure 7. Consent2Share Ecosystem Diagram 35

List of Tables

Table 1. Consent Models 7
Table 2. Electronic Consent Management Models 8
Table 3. Three Phases of Consent Management Maturity 12
Table 4. Common Technology Standards 31
Table 5. Glide Path for Senders of Part 2-Protected Data 34
Table 6. Glide Path for Recipients of Part 2-Protected Data 34

1 Background

1.1 Purpose

The Office of the National Coordinator for Health Information Technology (ONC) recently reiterated the need to protect the privacy and security of health information in its 10-year vision for an interoperable health information technology (IT) infrastructure.[5] This vision includes the ability to manage patient consent decisions regarding the use and disclosure of health information electronically. As health information[6] is increasingly maintained and exchanged electronically, it becomes critical to have the means to electronically obtain patients' consent to use and disclose their health information and communicate that consent along with the related health information.

For example, organizations that facilitate exchange among healthcare entities may need to obtain patients' consent before sharing their information to comply with state law or local policy. In addition, federal and state laws require that patients have the ability to express their consent before sharing certain health information that is considered "sensitive" (such as substance abuse treatment, reproductive health, mental health, or human immunodeficiency virus (HIV) information) in an electronic environment. These legal requirements risk leaving some patients on the "wrong side of the digital divide"[7] with regard to participation in health information exchange because current health IT networks and systems are not able to process complex consent decisions in an automated way.

To overcome this, ONC "will work to improve standards, technology, and workflow that enable the electronic collection and management of consent as well as the electronic exchange of related information within existing legal requirements (including notice of redisclosure restrictions)."[8] With this objective in mind, this report discusses the policy, technical, and process landscape; explains how certain stakeholders define sensitive information; identifies gaps and challenges that hinder adoption of electronic patient consent management technology; and discusses technologies that facilitate electronic consent management.

1.2 Scope

This report is based on informal discussions with various stakeholders, including health information organizations (HIOs), healthcare providers, and health IT developers. The report seeks to identify how some HIOs, providers, and developers manage patient consent when they share health information via health information exchange. We use the term health information exchange (HIE) to describe the process that enables healthcare providers and patients "to appropriately access and securely share a patient's vital medical information electronically."[9] In practice, the term HIE is sometimes used synonymously with the term HIO to describe an entity

[5] See Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure, p. 10, available at: http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf (hereinafter 10-Year Vision). The definitions of patient consent and electronic consent management are discussed later in this section.

[6] Health information is data in any form relating to the physical or mental health of an individual, the provision of healthcare, or payment for healthcare. See 45 C.F.R. §160.103, available at: http://www.law.cornell.edu/cfr/text/45/160.103. Health information includes individually identifiable health information (IIHI) and protected health information (PHI).

[7] 10-Year Vision, p. 10.

[8] *Id.*

[9] See What is HIE?, available at: http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie.

that oversees and governs the exchange of health information, but, in this report, we use HIE to describe the process of sharing health information electronically.

Specifically, this report has four objectives:

1. Identify how sensitive information value sets and terminology are defined and how these value sets are maintained.
2. Conduct a landscape assessment, including the identification of workflows, industry technical standards, and descriptions of the architectural environments in which patient consent data is shared. Identify how technology is currently used to identify, capture, track, manage, and transmit patient consent preferences when sharing clinical information.
3. Identify gaps in current technology and other challenges that may hinder the growth of managing patient consent electronically.
4. Describe the technologies and standards used if there are existing systems that can identify, capture, track, manage, and transmit patient consent preferences. Explain how these systems enable compliance with privacy laws or regulations and the granularity of patient consent decisions.

1.3 Patient Consent

This report uses the term "consent" to mean a patient's decision about how his or her personal health information is accessed and shared for treatment purposes. This report focuses on patient consent (1) to participate in health information exchange and (2) to share sensitive health information. The report does not discuss specific types of consent, such as consent to provide health information for research or marketing purposes.

Patient consent is synonymous with the term "meaningful consent," which is an informed decision by a patient that is properly recorded and maintained. A meaningful consent decision contains the following six characteristics:

1. Made with full transparency and education.
2. Made only after the patient has had sufficient time to review educational material.
3. Commensurate with circumstances for why health information is exchanged.
4. Not used for discriminatory purposes or as a condition for receiving medical treatment.
5. Consistent with patient expectation.
6. Revocable at any time.[10]

Patient consent may be represented as a "privacy consent directive" (or just "consent directive"), which is an expression of a patient's decision regarding how personal health information is to be accessed and shared (e.g., share my health information with Doctor A, but not with Doctor B). In a traditional paper document setting, the consent directive may be the patient's paper consent form (a paper consent directive).

[10] What is meaningful consent? Healthit.gov, available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange.

In the contemporary HIE setting, the consent directive is a digital form or other document (an electronic consent directive) that provides a technically implementable specification that enables a patient to control the collection, access, use, or disclosure of his or her health information. Specifically, HIO and provider IT systems are able to read and apply information from the electronic consent directive to direct the appropriate end-to-end exchange of patient health information.

Electronic consent directives can be implemented in various ways. For example, an electronic consent directive may be represented as a flag in an Admit, Discharge, and Transfer (ADT)[11] message. ADT messages are usually used to keep patient demographic and visit information synchronized across healthcare systems, but they can also indicate a patient's decision to share, not share, or withdraw consent to share health information.

1.4 ONC Consent-Related Efforts

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[12] directs ONC to manage the development of health IT, which includes hardware, software, integrated technologies or related licenses, intellectual property, or packaged solutions that help healthcare entities and patients electronically create, maintain, access, or exchange health information.[13] HITECH also directs ONC to ensure "that each patient's health information is secure and protected, in accordance with applicable law."[14] Under the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs, the federal government provides financial support to eligible healthcare providers and eligible hospitals to acquire and demonstrate "meaningful use" of health IT systems.[15] But the acquisition of technology is not the ultimate end-state; instead, the government's vision is to create an effective health IT infrastructure that can exchange health information in a manner that improves healthcare quality, reduces medical errors, and "improves the coordination of care and information among hospitals, laboratories, physician offices, and other entities through an effective infrastructure for the secure and authorized exchange of healthcare information."[16]

To help achieve that end, HITECH directs the Health Information Technology Policy Committee (HITPC) to consider and make recommendations to ONC about the following:

> Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law, and for the use and disclosure of limited data sets of such information.[17]

---

[11] See HL7 Version 3 Standard: Patient Administration, available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=92.

[12] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj *et seq*; §§17901 *et seq*., available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf (hereinafter HITECH).

[13] HITECH, § 3000(5), Definitions, available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

[14] HITECH, § 13101.

[15] HITECH, § 4101(a).

[16] HITECH, § 3002(b)(6).

[17] HITECH § 13101, Sec. 3002(b)(B)(i), available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

In 2010, the HITPC held a hearing on policies related to (1) patient consent for taking part in health information exchange and (2) the technology needed to implement electronic consent.[18] Subsequently, the committee recommended that ONC conduct further research into data segmentation and other related technologies in pilot studies to determine their feasibility and scalability.[19] To date, ONC has supported various projects focused on developing and adopting consent management-related technology. These include the following efforts:

- Data Segmentation for Privacy (DS4P)[20]
- Aspiring to Awesome (A2A) Pilot (Health Information Exchange Challenge Program)
- Strategic Healthcare IT Advanced Research Projects on Security (SHARPS)
- eConsent Trial Project
- Data Segmentation Based on Provenance
- Behavioral Health Data Exchange Consortium[21]

In November 2012, ONC, in coordination with the HITPC, issued a Request for Comments (RFC) for Meaningful Use (MU) Stage 3,[22] which included the following questions:

1. How can EHRs and HIEs manage information that requires patient consent to disclose so that populations receiving care covered by these laws are not excluded from health information exchange?
2. How can MU help improve the capacity of EHR infrastructures to record consent, limit the disclosure of this information to those providers and organizations specified on a consent form, manage consent expiration and consent revocation, and communicate the limitations on use and restrictions on redisclosure to receiving providers?
3. Are there existing standards, such as those identified by the Data Segmentation for Privacy (DS4P) Initiative Implementation Guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIOs?[23]

In August 2013, as part of its continuing efforts to facilitate the adoption of health IT, ONC developed a Strategy and Principles to Accelerate HIE[24] informed by stakeholder input received through a Request for Information (RFI). In responding to the RFI, many commenters expressed concerns about being able to follow state and federal privacy laws in an electronic environment, particularly those that require express patient authorization to disclose sensitive health information. They recommended HHS undertake additional work on developing standards and technology to facilitate electronically obtaining patient consent to disclose their health information and communicating that consent along with the related health information. Commenters also expressed reluctance to exchange health information due to concern about the

[18] See: http://www.healthit.gov/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf.

[19] For a full history of ONC action, see: http://www.healthit.gov/providers-professionals/data-segmentation-overview.

[20] See: http://www.healthit.gov/providers-professionals/enabling-privacy.

[21] More information regarding these efforts is available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-it.

[22] Request for Comment Regarding the Stage 3 Definition of Meaningful Use of Electronic Health Records (EHRs), 77 Fed. Reg. 70444 (Nov. 26, 2012), available at: http://www.gpo.gov/fdsys/pkg/FR-2012-11-26/pdf/2012-28584.pdf.

[23] See Comment Period Now Open: Help Set the Stage for Meaningful Use Stage 3, and associated RFC link, Health IT Buzz, available at: http://www.healthit.gov/buzz-blog/meaningful-use/set-stage-meaningful-stage-3/.

[24] See http://www.healthit.gov/policy-researchers-implementers/accelerating-health-information-exchange-hie.

potential breach of electronic protected health information (PHI), potential liability, and the assignment of responsibility. Based on these responses, the strategy identified a set of principles to guide a comprehensive effort across HHS agencies to accelerate HIE, which included developing standards and policies to enable electronic management of consent and HIE among providers treating patients with sensitive health information such as those with behavioral health conditions or HIV.

In October 2013, the HITPC responded to public comments received on the patient consent questions in the MU Stage 3 RFC.[25] The HITPC referenced its previous recommendation that data holders and requestors must comply with applicable law and policy and should have a technical way to communicate applicable consent or authorization needs and requirements.[26] They should also have a means to maintain a record of such transactions. The HITPC recommended that the Health Information Technology Standards Committee (HITSC) further consider technical methods for giving providers the capacity to comply with applicable patient authorization requirements or policies.

In March 2014, ONC updated the Federal Health IT Strategic Plan[27] and identified a number of the Secretary's strategic initiatives, including one focused on protecting patients' health information and their privacy rights. As part of this initiative, HHS stated its commitment to encouraging the development and use of policy and technology to advance patients' rights to access, amend, and make choices for the disclosure of their electronic health information. HHS also reiterated its support for the development of standards and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, or HIV) in an electronic environment.[28]

In July 2014, ONC published a vision paper that outlines a 10-year plan for achieving an interoperable health IT ecosystem that lowers healthcare costs, improves population health, empowers patients, and drives innovation. Under Building Block #3 (Privacy and Security Protections for Health Information), ONC acknowledges its role in facilitating the development of electronic patient consent.[29]

1.5 Consent Management

Consent management is the ability to maintain patient health information in accordance with a patient's meaningful consent decision. Gartner, an IT research and advisory company, provides the following definition of consent management:

> Consent management is a system, process or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access. It enables patients and consumers to affirm their participation in e-health initiatives (patient portal, personal health record or health information exchange) and to establish privacy preferences to determine who will have access to their PHI, for what purpose and under what

[25] See http://www.healthit.gov/sites/faca/files/Tiger%20Team%20Recommendation%20Transmittal_MU3RFC_FINALv3.docx.

[26] See http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Transmittal_08212013.pdf.

[27] In December 2014,ONC released the draft Federal Health IT Strategic Plan 2015-2020. See http://www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf

[28] See http://www.hhs.gov/strategic-plan/patient-privacy.html.

[29] 10-Year Vision, pp. 2-3, 10.

> circumstances. Consent management supports the dynamic creation, management and enforcement of consumer, organizational and jurisdictional privacy directives.[30]

In a traditional setting where health information exists only in paper form, consent management requires (1) an authorized person (usually a provider's administrative staff) to (2) read the patient's consent form (e.g., a paper consent directive) to identify what health information the patient is willing to share and with whom, (3) consider any controlling federal, state, regional, and organizational laws, regulations, or policies that may apply, (4) identify and extract the appropriate health information in the patient's record, (5) make a copy, (6) attach a warning against redisclosure without additional patient consent (if required), and then (7) mail or fax the information to an authorized recipient.

In the future health IT setting, the goal is for consent management to leverage automated processes that rely on a patient's electronic consent directive and an IT architecture that employs various access control and policy enforcement services to share health information appropriately. We refer to this automated process as "electronic consent management."

Electronic consent management begins when a patient expresses his or her consent decisions in an electronic manner (e.g., an electronic consent form on a tablet or via a web portal). This electronic form contains structured data, which means a computer can understand discrete data elements such as the name of the providers in the HIO to whom health information may be sent. The form containing these structured data elements can be used to create an electronic consent directive. The electronic consent directive may be stored in various locations, including locally in the provider's health IT system and/or centrally by an HIO. When a provider organization requests a patient's health information, the supporting health IT systems negotiate the entire transaction in an automated way that enforces the patient's electronic consent directive; ensures the sender and receiver are authorized to engage in the exchange; enforces applicable federal, state, regional, and organizational laws, regulations, and policies; and attaches a redisclosure warning if required.

1.6 Confidentiality/Privacy Laws and Consent Laws[31]

Generally, patient consent is *not* required for providers to share health information for treatment, payment, and healthcare operations purposes.[32] The Health Insurance Portability and Accountability Act (HIPAA) creates baseline privacy protections, but other federal and state privacy laws and regulations may be more "privacy-protective."[33] Specifically, various federal and state laws require patient consent for sharing sensitive health information. For example, at the federal level, 42 C.F.R. Part 2[34] (Part 2) requires patient consent to share health information held by federally funded substance abuse treatment providers. A Part 2 patient consent form must provide the following:

1. The specific purpose for which disclosed information can be used.

[30] Gartner IT Glossary, available at: http://www.gartner.com/it-glossary/consent-management/.

[31] This report discusses but does not address all confidentiality/privacy and consent laws.

[32] See HIPAA Administrative Simplification, available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (specifically, see 45 C.F.R. §§164.506 and 164.508).

[33] Are There Privacy Laws that Require Patient Consent? available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

[34] See 42 C.F.R. Part 2, available at: http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2.

2. The specific information being disclosed.
3. The expiration date, condition, or event when the consent is terminated.
4. To whom disclosures can be made.

A Part 2 disclosure also must be accompanied by a narrative informing the recipient that records cannot be redisclosed without additional patient consent.

In one example at the state level, Massachusetts law requires patient consent to disclose HIV test information. Specifically, healthcare providers must obtain the following types of consent:

1. Verbal informed consent from the patient before conducting an HIV test.
2. Written consent before disclosing the results of an HIV test to any person other than the subject of the test.
3. Written informed consent before identifying the subject of an HIV test to any person. The written consent form must identify the purpose for which HIV information is being requested, and the form must be distinguished from other written consent forms that permit the release of medical information.[35]

1.7 Consent Models

The specific requirements of federal and state law provide that patient consent usually requires a degree of granularity. Consent granularity means that patients are able to share only those parts of their health information that they are willing to share. Despite this need for granularity, some health IT architectures enable either all or none of a patient's health information to be shared.

A white paper prepared by the George Washington University Medical Center for ONC in March 2010 outlines five consent models (Table 1) by which patient health information may be shared in networked electronic exchange.[36]

Table 1. Consent Models

Model	Explanation
No Consent	Health information of patients is automatically included in and available through electronic exchange; patients cannot opt out.
Opt-out	Default is for all or some set of patient health information to be eligible for electronic exchange automatically, but the patient can opt out completely.
Opt-out with exceptions	Default is for health information of patients to be included in electronic exchange, but the patient can opt out completely or allow only selected data to be included.
Opt-in	Default is that **no** patient health information is automatically made available for electronic exchange; patients must actively express consent to participate, but if they do so, then their information must be all in or all out.
Opt-in with restrictions	Default is that **no** patient health information is made available for electronic exchange, but the patient may allow a subset of select data to be included.

[35] M.G.L. ch.111 § 70F. Massachusetts uses the term "informed consent," which has a specific meaning under certain federal rules. See 45 C.F.R. § 46.116 and http://answers.hhs.gov/ohrp/categories/1566.

[36] Consumer Consent Options of Electronic Health Information Exchange: Policy Considerations and Analysis, 23 March 2010, available at: http://www.healthit.gov/sites/default/files/choicemodelfinal032610.pdf (hereinafter Consumer Consent Options).

The white paper discusses the value of enabling patients to have more granular control over their health information rather than participate in an all-or-nothing data-sharing system. Granular consent provides patients with greater control. The white paper acknowledges that patient choice may come at a cost because some providers may be frustrated by incomplete data, but the paper also suggests that failing to provide more granular control may lead patients to avoid medical care or only to seek care if they can pay out-of-pocket.[37]

1.8 Electronic Consent Management Models

ONC identified three models by which patient consent is captured and maintained electronically. Table 2 provides an overview of these models. To date, "no one operating model has emerged as the best practice."[38]

Table 2. Electronic Consent Management Models[39]

Model	Explanation
Consent Bundled with Information	Collecting patient consent at the place where healthcare is delivered and then transmitting the consent and corresponding health information when it is requested by others. For example, in some models, a consent document (such as a PDF of a paper consent form) is sent along with the patient's health information.
Metadata Tagging	Adding a code to the health information to "tag" it with details related to the patient's consent choice. When this tagged information is sent from one health IT system to another, the sending and receiving organizations' health IT system needs to be able to read and understand what the tag means. The tag may also be a reference to a separate consent document that is stored locally or in a centralized database, showing the health IT system where to look for the most up-to-date consent choice for that piece of information.
Centralized Approach	Managing patient consent through a central database or repository that can be queried to decide how information may be accessed based on the patient's choice.

1.9 Sensitive Health Information

Consent management plays a particularly important role in the exchange of sensitive health information because it enables healthcare providers to use technology to comply with existing laws and empowers patients with the ability to decide how their health information is accessed and shared. MITRE's discussions revealed that there is no uniform definition for sensitive health information. Instead, federal and state confidentiality and privacy laws and healthcare organizational policies often shape what gets defined as sensitive information.

A June 2010 memorandum by the Consumer Partnership for eHealth (CPeH), a non-partisan coalition led by the National Partnership for Women & Families, affirms that the body of laws

37 Consumer Consent Options, p. 8-12; see also 78 Fed. Reg. at 5626 - 5630 (January 25, 2013).

38 Health Information Technology, How Can Consent Decisions be Captured and Maintained Electronically? available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-it (hereinafter Consent Decisions Captured Electronically).

39 See http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-it.

and regulations regarding sensitive health information is neither comprehensive nor consistent.[40] Instead, sensitivity is subjective and varies based on an individual's situation and context. Additionally, factors such as "cultural and political norms, individual life circumstances, and the emotional and health status of an individual" help determine sensitivity.[41] The disclosure of sensitive health information poses significant risks to the patient, such as embarrassment and negative social stigma associated with being in a substance abuse treatment program.

The CPeH memorandum provides the following list of common categories of sensitive information:

- Domestic violence
- Genetics
- Mental health
- Reproductive care, including abortion
- Substance abuse
- Sexually transmitted infection information, including HIV/acquired immune deficiency syndrome (AIDS)
- Records for patients that have a personal (e.g., family member) or professional (e.g., coworker) relationship with a facility employee[42]

Additionally, besides subject matter, other factors may determine whether health information is sensitive, such as the type of provider (e.g., substance abuse facility) or the specific type of health information (e.g., psychotherapy notes).

Finally, our discussions identified an industry-wide bias for over-inclusion of health data as sensitive. Some providers suggested that all patient data is sensitive, but some information is more sensitive than others (e.g., mental health or reproductive health information). Providers also mentioned concerns regarding the possibility of litigation or fines if this information is mishandled or stolen, which strengthens incentives to maintain as much direct control over health information in their systems as possible. Together, this bias and the lack of uniform definitions for sensitive information pose a challenge to wider and more rapid adoption of electronic consent management.[43]

[40] Protecting Sensitive Health Information in the Context of Health Information Technology, Consumer Partnership for eHealth, June 2010, available at: http://www.nationalpartnership.org/research-library/health-care/HIT/protecting-sensitive-health.pdf (hereinafter CPeH Memo).

[41] CPeH Memo, p. 2.

[42] CPeH Memo, p. 2-3; see also, National Committee on Vital and Health Statistics letter, February 20, 2008, p. 5, available at: http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/080220lt.pdf.

[43] See Challenges in Section 4 below.

2 Methodology

2.1 Stakeholders

This report reflects the content of discussions with three stakeholder groups—HIOs, healthcare providers, and software developers—as well as subject matter experts (SMEs) in the healthcare field. These stakeholders share a deep understanding of the laws, regulations, and policies that govern health information exchange and access to sensitive information.

HIOs are critical entities that oversee and govern the exchange of health information under nationally recognized standards and in an authorized and secure manner.[44] HIOs may provide various electronic services, such as web portals, personal health records (PHRs), clinical messaging, clinical interoperability, and exchange of data from EHRs, as well as the common administration of security services to ensure that data is used and disclosed appropriately.[45] HIOs themselves are as diverse as the states, laws, and policies that govern them. This diversity impacts the ability of HIOs to share sensitive and non-sensitive health information.

Healthcare providers are key players in producing and consuming patient health information. Additionally, providers are "agents of trust for patients" and they are "responsible for maintaining the privacy and security of their patients' health information."[46] Providers also must comply with use and redisclosure restrictions under Part 2, and other state health, confidentiality, and privacy laws.

Finally, software developers design, develop, and sell health IT systems, including EHR and PHR software, which healthcare organizations, providers, and patients use to conduct health information exchange.

2.2 Contributors

From these stakeholder groups, MITRE conducted discussions with various individuals and organizations (referred to herein as contributors or participants). The team strove for diversity among the contributors by accounting for their size (large and small), type (public and private), geography (urban and rural), market share (major players and minor players), and technology maturity (old and new).

MITRE also spoke with SMEs in the health information exchange field. These SMEs included engineers from federal government agencies, former healthcare providers who now work for nonprofit organizations and patient advocacy groups, and attorneys who list HIOs and patients as their clients.

For a list of contributor organizations, please see Appendix B.

2.3 Discussions

MITRE conducted telephone discussions with 25 contributors over the course of 7 weeks, and each discussion lasted about 1 hour. MITRE's discussions were open and unstructured; no

[44] See HIE Basics, supra.

[45] See Health Information and Management Systems Society (HIMSS) Guide to Participating in a Health Information Exchange, p. 8, available at: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf (hereinafter HIMSS HIE White Paper).

[46] See Meaningful Choice: Patient-Centered Decision Making in Electronic Health Information Exchange, available at: http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/meaningful-choice-electronic-health-information-exchange/.

formal surveys were provided. Several contributors offered written information, including documents, diagrams, videos, web links, and presentations.

Participants volunteered their time to discuss their personal experiences, perceptions, and viewpoints. To respect the candor of these discussions, this report does not attribute statements or perspectives to any individual contributor.

2.4 Limitations

This report should not be interpreted to describe the entire landscape of electronic consent management or its related technologies. This report considers consent within a limited scope; we looked at consent to participate in HIE for treatment purposes, not for payment, research, or other purposes. Furthermore, this report represents only a snapshot of individual perspectives on the current electronic consent management landscape, the existing challenges, and the technologies that are available or being developed.

2.5 Findings

This report does not make formal conclusions or recommendations that the federal government should act on but instead summarizes key findings from our discussions. Participants also offered suggestions to address various challenges identified during the course of our conversations. These suggestions may be considered for further research and consideration, but they are not presented as recommendations endorsed by either MITRE or ONC.

3 Landscape Assessment

The stakeholder discussions confirmed that current consent management practices are not fully automated and that full electronic consent management is still a goal for providers, patients, and HIOs. Contributors confirmed that most patient consent decisions are still collected using paper documents. As more providers and HIOs embrace the use of EHRs and PHRs, developers, providers, and HIOs are considering solutions that can electronically capture, maintain, and process patient consent preferences in an automated way.

The discussions further indicated that today's electronic consent management landscape can be divided into the three phases outlined in Table 3, which represent different levels of current and future consent management maturity.[47]

Table 3. Three Phases of Consent Management Maturity

Phase	Paper / Electronic	Structured / Non-Structured	Explanation
I – Current State	Paper consent form	No structured data in consent form.	• Consent is collected on a paper form. • Paper form is scanned into a patient EHR (usually as a PDF image file). • Consent form does not contain structured data. • Consent form travels with patient information, but it must be read and analyzed by a human being to comply with patient consent choices. • Consent decisions are not applied with granularity.
II – Current Growth	Paper and electronic consent forms	Some structured data. Electronic consent may contain digital flags or markers that are machine-readable.	• Consent is collected on a paper form and then a human enters data into an electronic form, or consent is recorded electronically by a patient (either via a tablet or web portal). • An electronic server is able to make basic share/ do not share decisions based on a digital flag or marker that reflects the patient's consent decision. • Consent decisions are not applied with granularity. Usually the share/do not share decision applies to all patient health information, not discrete portions of the patient's health record.
III – Future State	Electronic consent form	Structured data in consent form	• Consent is collected in an electronic form that contains structured data. • Structured data is used to create consent directives. • Health IT systems can interpret and process patient consent decisions from structured data and consent directives. • Health IT systems can interpret and process federal, state, regional, and organizational laws, regulations, and policies about consent and sensitive information. • Consent can be as granular as the applicable laws, regulations, and policies provide.

[47] This chart does not provide an exhaustive list of all consent models or methods; instead, it reflects the models discussed during MITRE's conversations.

This section addresses the current landscape (Phase I – Current State) and then turns to current advancements by illustrating how some HIOs manage patient consent (Phase II – Current Growth). Phase III – Future State has not been achieved yet, but Section 5 – Consent Management Technology addresses existing technology standards that can support full electronic consent management.

3.1 Phase I – Current State

Contributors agreed that current standard practice is for patients to indicate their consent preferences on paper forms at the provider location. Paper consent forms are scanned into EHR systems by a provider's staff, usually as Portable Document Format (PDF) files. These PDF consent forms are often machine-readable and searchable only at the document level—in other words, they are electronically tagged as a consent form within the patient's electronic health record, but none of the discrete data within the form exist as structured data (e.g., discrete data could include the name of the patient or treating provider, the medications prescribed, or the decision to participate in electronic health information exchange). Therefore, the discrete data cannot be electronically recognized by another system.

Structured data is important because health IT systems require it to process discrete patient consent decisions (such as which providers may access health information, or which diagnoses are sensitive and should not be disclosed). The American Medical Association defines structured data in the following way:

> . . . information that is organized in a structured manner, making it computer 'processable' and identifiable for data-mining and analytic purposes. Structured data that resides in fixed or discrete fields within a record or file can also be classified as discrete. Commonly, structured data is captured by the use of standard vocabularies, templates, drop-down lists, radio buttons, and check boxes to capture discrete data; whereas free text . . . is not structured. [48]

Standard health IT document specifications, such as the Continuity of Care Document (CCD), use structured data. Providers use the CCD to share administrative, demographic, and clinical information about a patient with other providers. The body of the CCD contains important structured data fields, including things like medications, conditions, and procedures.[49] Figure 1 shows an example of the CCD structure.

[48] Kim Futrell, *Structured Data: Essential for Healthcare Analytics & Interoperability*, Orchard Software, October 2013, citing the American Medical Association definition, available at: http://himss.files.cms-plus.com/FileDownloads/2014-05-29%20Orchard%20Software%20Structured%20Data.pdf (hereinafter Structured Data).

[49] See CCD-Continuity of Care Document, available at: http://www.corepointhealth.com/resource-center/hl7-resources/ccd.

Figure 1. Continuity of Care Document Structure[50]

In sum, it is not possible to correlate the granular consent decisions recorded in a PDF image of a patient's consent form with the structured data in the CCD. For that to be possible, there would need to be a relationship or mapping between the consent data in the consent form and the data in the CCD. Without structured data on both sides that can be correlated, it is impossible to automate the consent process with deeper granularity than at the individual document level.

3.2 Phase II – Current Growth

Discussions revealed that some HIOs and providers are developing methods for managing patient consent in a more automated manner. Providers may offer consent policies that permit patients to choose whether their health information may be shared electronically, either directly between providers or through an HIO.[51] At the provider level, consent policies can be managed within the provider's health IT system (such as the EHR system); at the HIO level, the HIO's health IT systems can perform this function.

Nevertheless, even in Phase II, most HIOs offer *opt-out* or *opt-in* consent models (either they receive all of the patient's health information or none of the patient's health information). Generally, HIOs have not embraced more sophisticated electronic consent models that offer greater granularity and patient control, such as *opt-in with restrictions* or *opt-out with exceptions*. Several factors account for this, including state laws and regulations and the absence of structured data in consent forms. Section 4, Gaps and Challenges, provides a more detailed discussion of HIO complexity.

Phase III – Future State developments are discussed in Section 5.

[50] See http://nerdpod.blogspot.com/2012/02/whats-c32ccd.html.

[51] See How Can Patient Choice Be Implemented in Electronic Health Information Exchange, available at: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

3.3 HIO Architectures and Electronic Consent Management

Electronic consent management is performed differently depending on the architecture model of an HIO. Generally, HIO architecture can influence how consent is collected, how it is updated, and where it is stored. This section introduces two HIO architecture models and explains how certain HIOs, with whom MITRE spoke, process consent.

The Health Information and Management Systems Society (HIMSS), a global, nonprofit organization that advances health engagement and care outcomes through IT,[52] provides a summary of common HIO technical architecture models. Our discussions referenced two of these models: centralized and federated.

As the name suggests, the centralized model uses a data repository to store health information in a single location—usually a "single large logical database that aggregates similar data from numerous sources . . . ."[53] The Central Data Repository (CDR) contains patient consent directives as well as an enterprise master patient index (EMPI). Requests for patient health information are routed through the CDR, and participating providers push patient information to the CDR on a daily basis. Figure 2 represents an example of a centralized model.

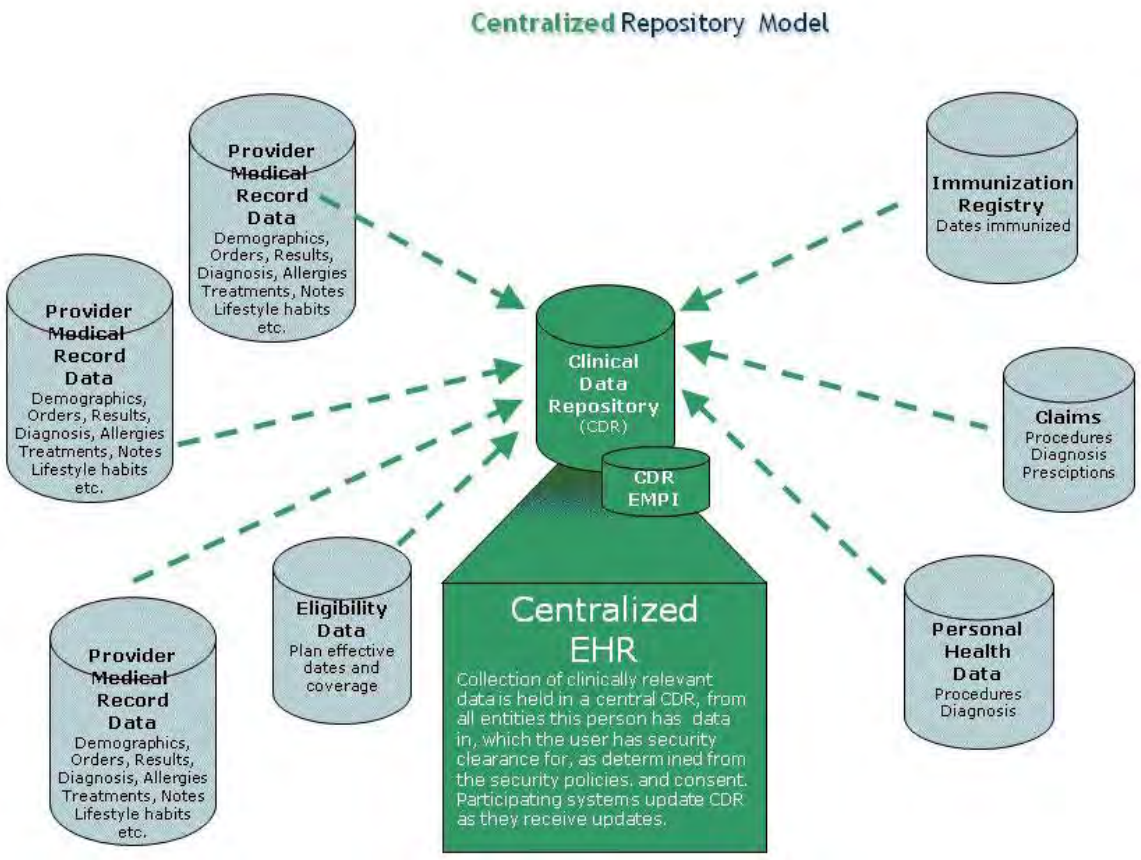

Figure 2. Centralized HIO Architecture[54]

[52] See HIMSS, available at: http://www.himss.org/AboutHIMSS/index.aspx.

[53] See Common HIE Technical Architecture Models, available at: https://himsshie.pbworks.com/w/page/4777793/HIEModels (hereinafter Common Architecture Models). The terms "decentralized" and "federated" are used synonymously in this report.

[54] See Common Architecture Models, available at: https://himsshie.pbworks.com/w/page/4777793/HIEModels.

A decentralized or federated model provides a framework for data sharing in which individual participants (e.g., providers, medical groups, labs, imaging services organizations, etc.) maintain "ownership and control" over their health information and these participants request access to updated health records only when needed.[55] Access to health information is usually routed by a record locator service (RLS). An RLS is a repository that contains limited patient demographic data and identifies where within a network a patient's data may reside.[56] Figure 3 represents an example of a federated model.

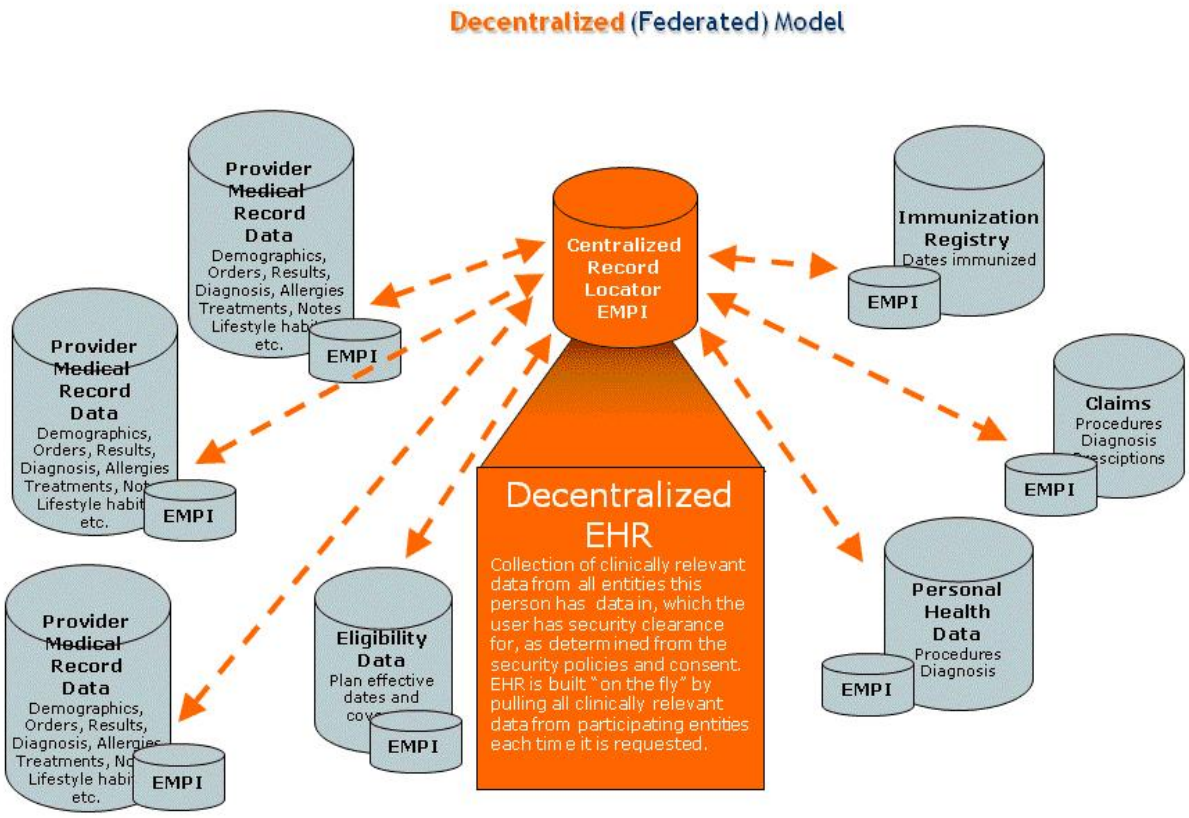

Figure 3. Decentralized HIO Architecture[57]

The New England Healthcare Exchange Network

The New England Healthcare Exchange Network[58] (NEHEN) is a Massachusetts-based HIO with a decentralized network architecture.[59] Each provider stores patient health information and consent forms locally, but NEHEN's architecture does not use an RLS. Instead, each participating provider obtains a list of all participating providers, and each provider can share health information on a peer-to-peer basis within the NEHEN network.

[55] See Common Architecture Models.

[56] See HIMSS HIE White Paper, p. 12.

[57] See Common Architecture Models.

[58] See http://www.nehen.org.

[59] See Common Architecture Models.

Providers sign participation agreements, which create a trust fabric. Providers use NEHEN's software (NEHEN*Clincal*) to "push" data through the HIO network using Direct messaging.[60] Providers can use standard messaging formats, such as Health Level Seven International (HL7) Clinical Document Architecture (CDA) documents, which includes the CCD. NEHEN also supports standards created by the Accredited Standards Committee (ASC) X12[61] and the National Council for Prescription Drug Programs (NCPDP).[62]

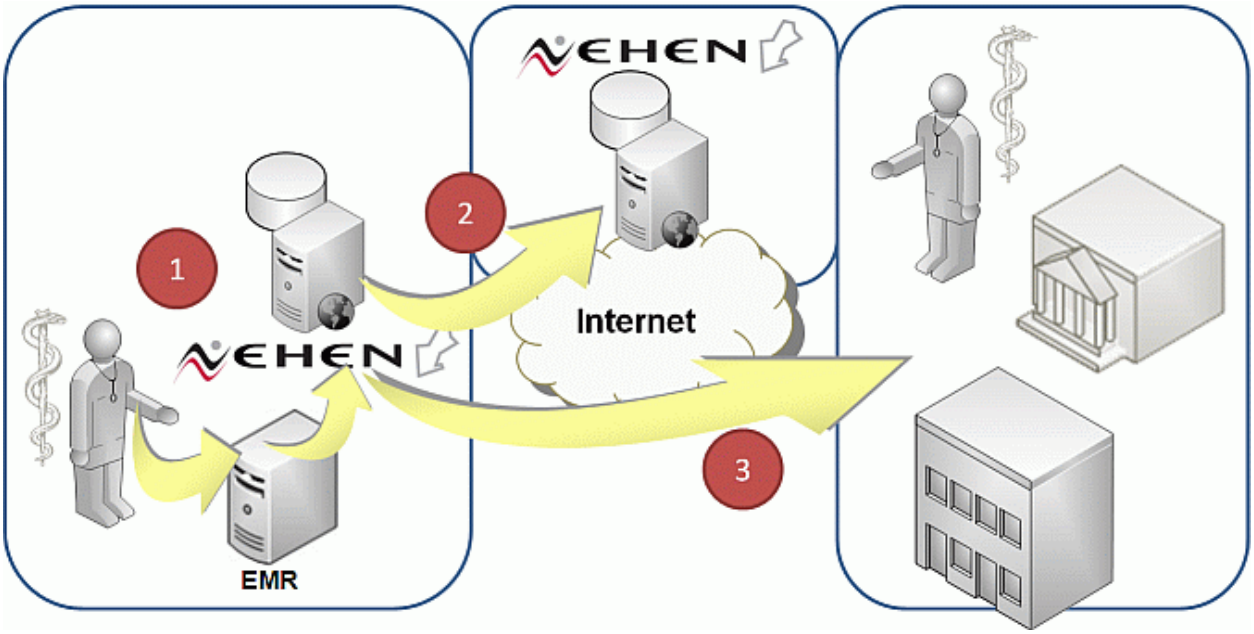

Figure 4. Decentralized NEHEN Architecture[63]

The NEHEN website describes the exchange process in three steps (see Figure 4):

1. Provider staff enters consent and health information using their existing hospital or electronic medical record system, which generates a CCD; this is transmitted to the local NEHEN*Clinical* gateway.
2. The NEHEN*Clinical* gateway examines the transaction and determines the destination, then looks up where the recipient is located from a common participant directory.
3. The transaction is routed directly to the intended recipient over the Internet. The recipient receives the transaction and replies with an appropriate acknowledgment.[64]

Our discussions revealed that patient consent is not required to share non-sensitive health information in the NEHEN architecture (i.e., the *no consent* model). The law in Massachusetts requires an *opt-in* consent model only for state-run HIOs. Because NEHEN is a private, nonprofit organization, patient consent is not mandated. Additionally, NEHEN's architecture was equated to a traditional telephone network that operates as a blind conduit of information.

[60] See The Direct Project, available at: http://www.healthit.gov/policy-researchers-implementers/direct-project.

[61] See http://www.x12.org.

[62] See http://www.ncpdp.org.

[63] NEHEN Architecture available at: http://www.nehen.org/products/clinical.aspx.

[64] See http://www.nehen.org/products/clinical.aspx.

Members of the NEHEN network are comfortable sharing both sensitive and non-sensitive information because of the trust fabric established by detailed participation agreements. In addition, current NEHEN participants that share sensitive information have done so for many years; these relationships are already well established. Providers that share sensitive health information subject to federal and state laws collect patient consent in whatever manner they choose (either paper or electronic). Consent forms are stored and updated individually by each provider.

The Massachusetts Health Information Highway (Mass HIway)

The Massachusetts Health Information Highway[65] (Mass HIway) is an example of another HIO with a decentralized architecture, but Mass HIway employs a centrally managed RLS (see Figure 5). Mass HIway is a state-run HIO, which means providers must obtain patient consent to access and share patient health information electronically. The Mass HIway uses an *opt-in* consent model, so patients must actively express consent to participate in electronic exchange through the HIO.

Mass HIway offers both push and pull technologies. Providers can push health information to authorized recipients in a secure manner using Direct standards.[66] Additionally, Mass HIway's query and response service, new as of January 2014, enables providers to identify whether other providers possess records on the treated patient through an RLS and to request that those records be provided.

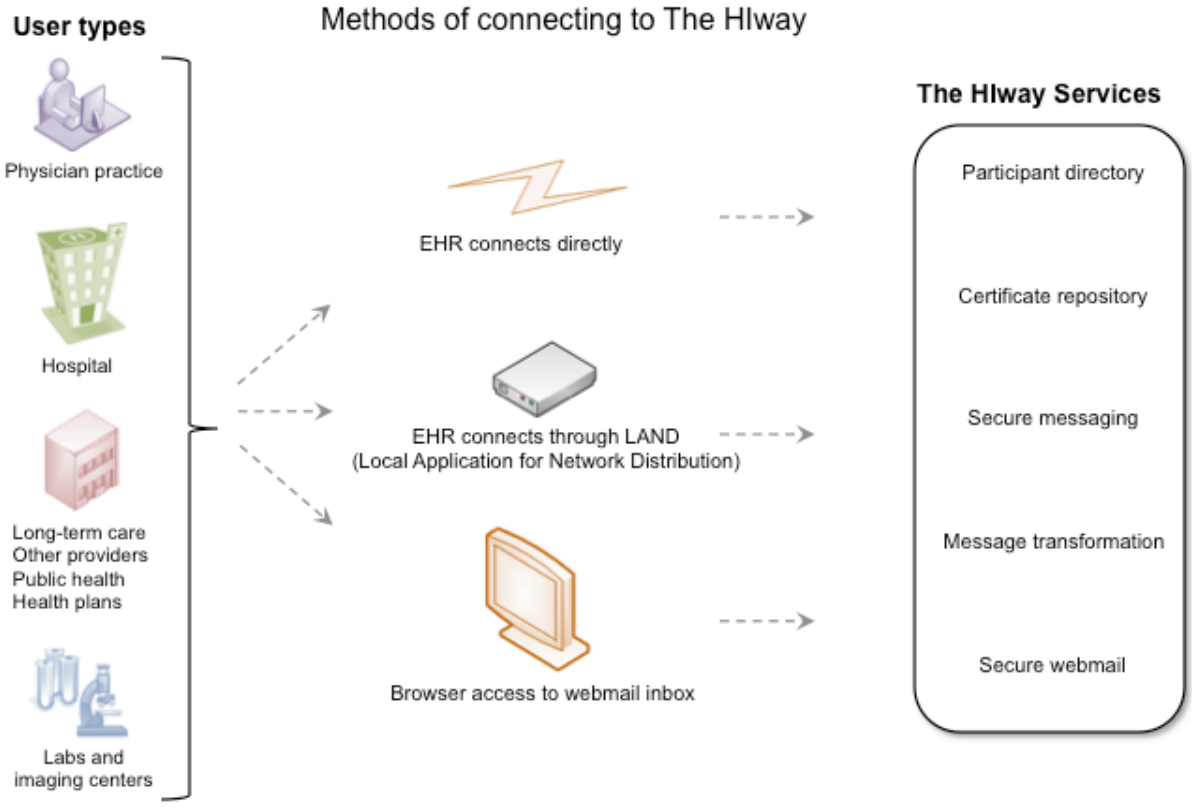

Figure 5. Mass HIway Methods of Connecting

[65] See www.mass.gov/hhs/masshiway.

[66] More information about the Direct Project is available at: http://wiki.directproject.org.

The Mass HIway does not store patient clinical information centrally, but it does capture and store patient demographic information and consent decisions in the RLS. Demographic information includes (1) the sender's organization ID, (2) the medical record number for the sending organization, (3) patient name, (4) patient gender, (5) patient date of birth, (6) patient address, (7) patient telephone number, and (8) patient email.[67] All demographic information is encrypted, and logs record all requests for access to health information by authorized users.

Patient consent is transmitted to the RLS in the form of an HL7 Admit, Discharge, and Transfer (ADT) message feed.[68] The "Z segment" of the ADT message contains a "Y" (Yes) or "N" (No) flag. If a new patient consents to participating in the Mass HIway, the ADT message is sent to the RLS, the RLS reads the "Y" flag, and demographic data is transmitted to the RLS. Health information can be pushed to and pulled from participating institutions and providers.

If a new patient does not consent to participate, the Mass HIway sees the "N" flag in the ADT message and the message is rejected and destroyed, leaving no trace at the HIway of the patient's relationship to the institution that sent the message.

If the patient previously consented but then changes his or her mind, the Mass HIway stores the transaction with the "N" flag to preserve an audit trail of the patient's consent decision having changed, but all previous information that was stored by the HIway is destroyed.

Rhode Island Quality Institute (RIQI) and CurrentCare

CurrentCare[69] is the health information exchange system used by the sole regional HIO in the state of Rhode Island, the Rhode Island Quality Institute (RIQI). CurrentCare's centralized network architecture maintains an *opt-in* consent model, so when a patient elects to participate, all health information is sent to a centralized server, as represented in Figure 2.

Consent is collected in two ways: patients either register online or at their provider's office.[70] Some providers still offer paper forms, which staff collect and use to enter data electronically via CurrentCare's portal. The ultimate goal is to achieve 100% electronic enrollment.

The CurrentCare enrollment form notifies patients that health information is protected under both federal and Rhode Island laws. Patients agree to allow disclosure of and access to all health information, "including information relating to alcohol and substance abuse, mental or behavioral health, HIV/AIDS, genetic diseases or tests, sickle cell anemia and sexually transmitted diseases."[71] Additionally, patients agree that if this type of sensitive information is requested, patients authorize its release to CurrentCare and to authorized providers and professionals listed on the reverse side of the form. Patients are presented with three options: (1) authorize access by all doctors, including emergency situations, (2) authorize access only in emergency situations, or (3) authorize only some doctors and emergency situations. Under the third option, patients list each provider or organization name, address, and phone number for each provider. Patients also acknowledge that they have had the opportunity to access the list of all participating provider organizations prior to providing consent.

---

[67] See http://www.masshiway.net/HPP/Services/ConnectionServices/index.htm

[68] See HL7 ADT-Admit Discharge Transfer, available at: http://www.corepointhealth.com/resource-center/hl7-resources/hl7-adt.

[69] See http://www.currentcareri.org.

[70] Current Care offers 24-hour-per-day online enrollment, or patients may enroll at their provider's location. See http://www.currentcareri.org/AboutCurrentCare/FAQs.aspx#47810-2-how-easy-is-it-to-enroll

[71] See CurrentCare Enrollment Form, available at: http://currentcareri.org/Portals/0/Uploads/Documents/CurrentCare-Enrollment-Form-05Dec13.pdf.

Patients may revoke their consent at any time by filling out and submitting a Cancellation of Enrollment form to RIQI.[72] However, the revocation does not affect previous disclosures while the consent was in effect, and it does not prevent the future redisclosure of health information that was validly disclosed before the revocation. Additionally, the patient's identity must be authenticated by a healthcare provider or facility that is an enrollment partner or RIQI employee. If the patient does not submit his or her cancellation at the provider's office or RIQI-affiliated facility, then the patient must have his or her cancellation form notarized. Enrollment and cancellation forms, both paper and electronic, are maintained by RIQI.

Only authorized providers and department of health personnel with unique log-in credentials can access patient records in CurrentCare (payers are excluded).[73] Providers use a web-based portal, the CurrentCare Viewer, to see the most up-to-date patient health information, which providers push daily to the participation gateway.[74] The participation gateway is an IT system that applies rules to decide whether health information may be uploaded to CurrentCare or whether health information is rejected, never reaching the CDR. The gateway accomplishes this by determining whether the information belongs to an enrolled patient participant. If the patient is enrolled, their data is updated; if the patient is not enrolled, the data is discarded.

CurrentCare enables providers to view sensitive health information, including Part 2 information. For a Part 2 provider to send Part 2 data to CurrentCare, the Part 2 provider must have a patient sign a separate consent form authorizing the provider to disclose the data to CurrentCare. This separate consent form is a standardized document used by all Part 2 providers in Rhode Island, and it was developed in cooperation with the state regulator.[75] A Part 2 patient must also sign the CurrentCare consent form to enroll in CurrentCare.

The CurrentCare participation gateway segregates data that originates from Part 2 providers. After a patient enrolls, their Part 2 records are aggregated into a tab. Any healthcare provider can access the Part 2 tab if they affirmatively confirm that they have a treating relationship with the patient and they have a need to know the information to treat the patient. The treating provider clicks on the statutorily required language to acknowledge that they understand that the information cannot be redisclosed without patient consent or a court order.

Privacy and security officers at RIQI perform regular audits and send letters to providers when suspicious activity is identified. CurrentCare is also able to provide patients with a copy of their healthcare information and a disclosure report that details which providers have accessed their health information.

CurrentCare has been operating successfully for nearly one year. The HIO currently services more than 400,000 of the state's one million eligible patients, and enrollment is increasing at the rate of about 8,000 patients per month. In Rhode Island, 100 percent of labs, 98 percent of pharmacies, and all hospitals can use the system, even if they use different EHR platforms. The only technical participation requirement is the ability to push data to the participation gateway.

[72] See CurrentCare Enrollment Cancellation, available at: http://www.currentcareri.org/Portals/0/Uploads/Documents/MemberForms/CurrentCare%20Enrollment%20Cancellation%20ver.062.2014.pdf.

[73] See Who can see my health records in CurrentCare? available at: http://www.currentcareri.org/AboutCurrentCare/FAQs.aspx#47813-5-who-can-see-my-health-records-in-currentcare.

[74] See CurrentCare Services, available at: http://www.currentcareri.org/HealthcareProviders/CurrentCareServices.aspx.

[75] See Health Information Exchange Advisory Commission, available at: http://www.health.ri.gov/partners/advisorycommissions/healthinformationexchange/.

4 Gaps and Challenges

Continued reliance on the use of paper or PDF consent forms is not due to a gap in consent management technology. Instead, current consent management practices that rely on paper or PDF forms containing unstructured data are often the result of financial limitations or simply customary practice. Participants stated that current technologies and health IT standards are capable of performing electronic consent management. Pilot studies have shown that partial electronic consent management can be accomplished using current health IT standards, and several health IT developers are creating more sophisticated consent management solutions.

This section addresses gaps and challenges identified during our discussions, including technological challenges, compliance complexities, cost and sustainability challenges, cultural and educational challenges, and policy challenges.

4.1 Technological Gaps

MITRE's discussions revealed that the low rate of adoption and implementation of full electronic consent management is not due to a gap in technology, meaning electronic consent management is not hindered by the absence of a particular technology or technological standard. Instead, participants stated that electronic consent management is possible using existing technologies and standards, but there is not yet an industry-wide best practice or accepted framework for collecting consent and sharing consent decisions. Nevertheless, even if the technology exists, participants noted two technology-related challenges that must be overcome for electronic consent management to become common practice: (1) the lack of structured data in patient consent forms and (2) interoperability between health IT systems.

Lack of Structured Data

Contributors noted that electronic consent management would not become common practice until patient consent is represented as structured data. Data segmentation relies on the existence of structured data, and so long as patient consent forms are captured and processed as unstructured files (e.g., a PDF image), it will be challenging for any developer or HIO to manage patient consent directives in a sophisticated, automated way.

Additionally, contributors stated that health IT systems do not uniformly or consistently tag metadata the same way, making it more difficult to identify data that should be restricted. There must be a well-understood relationship or mapping between the consent metadata and the structure of the patient health information for consent management to be feasible in an automated consent management system. For example, if consent is not provided for a sensitive set of diagnoses, the system must have enough information to identify those diagnoses in the patient data in order to filter those diagnoses or restrict access to that data. This problem is complicated when information is being transferred between multiple health IT systems. When multiple systems are involved, the consent metadata must be standardized to allow additional systems to appropriately interpret the consent information for application to those systems' patient data. Similarly, developers identified challenges associated with coding numerous different consent forms that use different terms to describe the same information.

Interoperability Challenges

Contributors also identified interoperability challenges. For this report, interoperability means the ability of multiple systems to easily communicate and share information.[76] Providers noted that a single hospital system with multiple EHR systems is unable to easily share health information about the same patient. This further complicates the hospital's ability to collect and manage a patient's consent. Additionally, regional HIOs (RHIOs) in New York State are currently unable to seamlessly share patient data with each other; one reason identified is the difficulty in verifying patient identities across RHIOs. This has led to an effort to create a new umbrella infrastructure that will interconnect the RHIOs and leverage a master patient index (MPI) to help facilitate health information exchange.

Our conversations also identified a related challenge associated with patients being able to uniquely identify a healthcare provider with whom they would like to share their health information. This challenge is acute when providers change practices or practices are absorbed into other organizations via mergers and acquisitions, which is increasingly common.

In addition, contributors cited difficulties normalizing vocabularies under various semantic standards. Semantic vocabularies are important for describing unique data values in a way that most health IT organizations can interpret and use. Examples of these semantic vocabularies include the Logical Observation Identifiers Names and Codes (LOINC)[77] and Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT).[78] Contributors noted that data from different IT systems will use different standards and vocabularies, and it can be difficult to successfully normalize these so that data can be shared effectively.[79]

This difficulty in normalizing semantic vocabularies makes consent management across these systems challenging. These semantic vocabularies are used to identify the exact diagnosis, medication, encounter, etc., contained within the patient's health information. Consent metadata will likely also need to reference semantic vocabularies to specifically identify sets of diagnoses, medication, encounters, etc., for which consent is either provided or restricted based on sensitivity. Without a common set of vocabularies or normalized mappings between vocabularies, it will not be possible to reconcile consent information referencing codes from one vocabulary with patient information managed using a different vocabulary.

4.2 Compliance Complexity

Contributors cited compliance with multiple privacy and confidentiality laws, regulations, and policies as a barrier to adopting full electronic consent management. These laws, regulations, and policies address both patient consent rights and categories of information that are considered sensitive, and they may apply at various levels, including federal, state, regional, and organizational. Such compliance requirements can be complex, and depending on where a patient and a provider are located, rules may conflict. This combination makes it more difficult to offer patients consent options and to enforce consent decisions. But at the same time, it is unlikely that this complexity will diminish in the future, which means that technical solutions will need to be applied.

[76] See Health IT Terms, available at: http://www.healthit.gov/patients-families/health-it-terms.

[77] See http://loinc.org.

[78] See http://www.ihtsdo.org/snomed-ct/.

[79] See HIMSS HIE White Paper, p. 30, available at: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf.

Federal Laws

First, federal laws require heightened privacy protections for certain types of health information. As discussed in Section 1, 42 C.F.R. Part 2 (Part 2) covers information generated by federally funded substance abuse treatment facilities. Other federal laws also provide special protections for sensitive health information, such as the Genetic Information Nondiscrimination Act (GINA),[80] which makes it illegal to discriminate against employees or applicants because of genetic information. Additionally, under 38 U.S.C. §7332, the Department of Veterans Affairs (VA) must obtain "special written consent" to disclose "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient . . . relating to drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia . . . ."[81]

Healthcare providers or HIOs may offer broad consent (e.g., under a full "*opt-in*" or "*opt-out*" consent model) or more granular patient choice (e.g., the "*opt-in with restrictions*" or "*opt-out with exceptions*" models). Our discussions indicated that most providers currently offer *opt-in* or *opt-out* consent models, but developers noted growing demand for more granular patient choice options, especially in the behavioral health space. As a result, health IT systems must be able to share health information in accordance with more complex patient consent decisions.

State Laws

States have varying approaches for requiring patient consent and for defining sensitive information. Developers noted that it is challenging to build an IT system that can account for at least 50 potentially different rules. This is further complicated when HIOs and provider organizations apply additional rules since those may affect networks that extend across states. Contributors noted that this compliance challenge is not likely to abate. A developer stated that, as a result, software companies must be committed to designing flexible and interoperable systems.

For example, the system could manage the rules as software configuration rather than directly coding the rules into the business logic of their system software. This would allow the rules to be configured for various states and updated as the rules change without having to rebuild the underlying code for their software. Additionally, shared service deployments can also help to limit the impact of changes to rules. Shared services do not require making updates to numerous installations of the deployed software when rules change.

Massachusetts and New York laws provide good examples of legal complexity surrounding consent and sensitive information. Section 1 referenced a Massachusetts law that requires special written consent for HIV test information.[82] Several other Massachusetts laws also provide consent restrictions for special categories of health information, including:

- Genetic information and reports protected as private information
- Records pertaining to venereal disease
- Alcohol treatment records
- Records regarding drug rehabilitation treatment[83]

[80] See U.S. Equal Employment Opportunity Commission, available at: http://eeoc.gov/laws/types/genetic.cfm.

[81] See 38 U.S.C. § 7332(a)(1), available at: http://www.law.cornell.edu/uscode/text/38/7332.

[82] See M.G.L. ch.111 § 70F, available at: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXVI/Chapter111/Section70f.

[83] See M.G.L. ch.111 § 70G, ch.111 § 119, ch.111B § 11, and ch.111E § 18.

New York requires patient consent before a provider can disclose a patient's health information to another treating physician,[84] which is more restrictive than the rules under HIPAA.[85] New York also provides examples of unique consent requirements for certain health information that is considered sensitive, including:

- Birth defects
- Cancer
- HIV
- Sexually transmissible infections
- Substance abuse[86]

With regard to consent, the lack of uniform definitions for sensitive information causes challenges. For example, consent-driven restrictions on accessing and sharing HIV information in one state may include diagnosis and lab test results, while restrictions for HIV information in another state may also include prescription information for the treatment of HIV. As such, differences in what states consider protected HIV information creates challenges for IT systems to share consent about such information across jurisdictions. Participants suggested the federal government should support efforts to achieve greater consensus on definitions for sensitive information in the health IT community.

In sum, the lack of legal uniformity for consent is viewed by some as one of "the most complex challenges" for implementing electronic health information exchange.[87]

HIO Complexity

HIO architecture can pose a challenge to consent management depending on where the most current patient consent is maintained. In a centralized architecture, consent may be managed in a single database, but in a decentralized architecture, each participating provider maintains its own consent. Also, in a decentralized architecture, rules must be developed to resolve discrepancies between separate consent statements for a given patient. Discussion participants cited challenges with identifying the most up-to-date patient consent, especially when the most current consent must be referenced to share health information with a provider that uses a different HIO or a different health IT system.

Additionally, HIOs may adopt different consent models, which can lead to challenges. Generally, HIOs perform the following functions: authenticate the identities of patients in the system, apply the appropriate patient consent directive, monitor and audit use of consent to validate appropriate management, and facilitate provider access consistent with consent directives.[88] These tasks become more technically complex and resource-hungry depending on the type of consent model in place, with the more granular patient choice models being more difficult to implement.[89]

Most HIOs adopt an *opt-in* or *opt-out* consent model that accepts all health information or no health information, which is easier to manage than consent models that permit greater consent granularity. Consequently, many organizations that share sensitive health information, including

[84] See New York Public Health Law § 18(6), available at: http://codes.lp.findlaw.com/nycode/PBH/I/2/18.

[85] See 45 C.F.R. Part 160 and Subparts A and E of Part 164.

[86] See New York Public Health Law §§ 2733, 2402, 2781, and 2402.

[87] Consumer Consent Options, p. 48.

[88] Consumer Consent Options, p. 36.

[89] *Id.*

substance abuse treatment facilities covered by Part 2, find themselves excluded from many HIOs. Contributors also noted that many Part 2 providers are small organizations with limited resources to spend on health IT systems, and that Part 2 providers cannot obtain federal assistance under the EHR Incentive program. As a result, traditional paper-only consent management practices are still common for organizations that share sensitive information when the HIO maintains an *opt-in* or *opt-out* model.

4.3 Identity and Access Management (IDAM)

When patients consent to sharing their health information or make specific decisions about sensitive information, it is important to ensure that their identity is appropriately authenticated. Additionally, if patients update consent preferences remotely, such as through a web portal, it is important to have appropriate access controls.

MITRE's discussions revealed concerns regarding patient identity and access management, particularly with regard to remote access to health information and the use of web portals. Portals are becoming more common, especially given Meaningful Use Stage 2 requirements that providers (i.e., eligible professionals) must offer "patients the ability to view online, download, and transmit their health information within four business days of the information being available" to the provider.[90]

One participant noted that currently there is neither a consistent nor a truly secure way to identify a patient online; in-person verification of identity credentials at the provider's office remains the most secure method for verifying a patient's identity.

4.4 Costs and Sustainability

When asked about barriers to achieving full electronic consent management, contributors mentioned high costs to implement, update, and maintain health IT systems. Contributors noted that large urban or regional health networks may possess the financial and manpower resources to field and operate health IT systems with sophisticated consent management tools, including patient portals, but rural providers lack the ability to initially fund and maintain similar technologies. One contributor said that smaller practices do not have dedicated IT professionals on staff, and after a health IT system is initially purchased, smaller providers have difficulty keeping the system updated with the latest patches and software releases. This poses a sustainability challenge, both for keeping health IT systems current and for accepting future upgrades that will likely include more sophisticated consent management capabilities.

4.5 Workflow, Trust, and Education

MITRE's discussions uncovered workflow, trust, and education challenges related to the adoption of more sophisticated consent management.

Workflow and Trust

Providers stated that altering workflow from a paper process to an electronic process is a major change management concern. A developer echoed this, relating its experience with several providers that remain reluctant to move away from traditional workflows that use paper consent

[90] See Final Rule for Meaningful Use Stage 2, available at: http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf.

forms. Mainly, these providers are often not very tech-savvy, and the developer felt challenged to make the provider feel more comfortable about the new technology environment.

MITRE's discussions also touched on providers' reluctance to relinquish direct control of patient information. Providers acknowledged the value of more patient control over sensitive portions of their health information, but also expressed uncertainty about repercussions if restricted data is inadvertently shared contrary to a patient's consent decision. Specifically, these consequences include private legal action and regulatory enforcement penalties.

Finally, discussions revealed skepticism about both the ability of developers to achieve granular segmentation of patient health information in a consistent and accurate manner, and the utility of embracing more complex technologies. While some contributors believed that granular electronic consent management is not only in patients best interests, but also inevitable, other participants stated that complex automated consent management may never be achieved and may not have a positive impact on delivering coordinated healthcare. These contributors suggested that masking or redacting certain information from one provider may negatively impact improved care coordination as well as trust in health IT.[91]

Education

Participants identified the need for more education about consent management technologies and how sensitive information can be processed in a manner that complies with federal and state rules. Both patients and providers could benefit from this education.

Contributors also mentioned that many providers view confidentiality laws as being more restrictive than they actually are. The Substance Abuse and Mental Health Services Administration (SAMHSA) has tried to clarify Part 2 rules by publishing frequently asked questions (FAQ), but uncertainty regarding the regulation persists.[92]

4.6 Policy Challenges

Although the focus of this report is to survey a portion of the landscape of consent management technologies, many discussions touched on policy challenges. Policy and technology are closely coupled in the health IT space. Policy often drives innovation, as evidenced in the EHR Incentive Program.[93] But contributors noted that policy also may be hindering important objectives, such as participation in health information exchange and improved care coordination.[94] Contributors explained that this is a challenge faced by Part 2 providers.

42 C.F.R. Part 2

ONC openly recognizes that "privacy and confidentiality concerns are currently limiting the inclusion of behavioral health data in electronic health information exchange efforts."[95] Several participants that MITRE interviewed stated that the consent requirements in Part 2 are a partial cause.

---

[91] More information about improved care coordination is available at: http://www.healthit.gov/providers-professionals/improved-care-coordination.

[92] See Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE), available at: http://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf.

[93] More information about the EHR Incentive Program is available at: http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.

[94] See Benefits of EHRs, Improved Care Coordination, available at: http://www.healthit.gov/providers-professionals/improved-care-coordination.

[95] Consent Management, available at: http://www.healthit.gov/policy-researchers-implementers/consent-management.

Part 2 provides patient consent rules for the collection, use, and redisclosure of information processed by federally assisted substance abuse programs (state laws and other regulations may require Part 2 compliance from private programs as well).[96] As stated earlier, these rules require a special consent form that identifies the specific health information, the purpose for sharing, the expiration of the consent, and the receiving party. Part 2 records must also be accompanied by a standard narrative about the prohibition of redisclosure without additional patient consent. According to contributors, these unique consent requirements make it difficult for Part 2 providers to participate in most HIO networks.

SAMHSA held a public listening session in June 2014 to field public comments regarding potential changes to Part 2. SAMHSA acknowledged that "[a] number of organizations across the country are excluding substance abuse treatment data due to the difficulty and expense of implementing the functionality and workflow changes necessary to comply with current regulations," and that "patients are prevented from fully participating in integrated care efforts even if they are willing to provide consent."[97]

[96] See 42 C.F.R. Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records, available at: http://www.law.cornell.edu/cfr/text/42/part-2.

[97] Department of Health and Human Services, Notice of Public Listening Session, available at: https://www.federalregister.gov/articles/2014/05/12/2014-10913/confidentiality-of-alcohol-and-drug-abuse-patient-records.

5 Consent Management Technology

The Landscape Assessment (Section 3) discussed the Phase I and Phase II levels of maturity of consent management. This section focuses on Phase III, which addresses future capabilities that leverage technology to manage patient consent electronically. This phase is driven by the ability to capture and process structured data in an electronic consent form. Although Phase III is labeled a future state in this report, MITRE's discussions revealed that several technologies currently exist that can make full electronic consent management a reality.

More specifically, contributors indicated that electronic consent management can be accomplished using current health IT standards for transport, messaging and language, and vocabulary.[98] Although basic standards exist to support basic consent management capabilities, more mature standards will be needed to support the more complex implementations of electronic consent management.

This section provides a brief discussion of consent directives and a conceptual architecture, lists various standards, summarizes two pilot studies that demonstrated progress in advancing electronic consent management, and ends with a brief description of existing developer solutions addressed during our discussions.

5.1 Consent Directives

As discussed in Section 1, a consent directive can be expressed either in paper form or electronically as a technically implementable specification that enables patients to grant or withhold authorization to collect, access, use, or disclose their health information. Such permissions depend on the consent directive, the policies of the requesting organization, and the governing laws and regulations.[99]

An electronic consent directive may be implemented in various ways, including ADT messages or the HL7 CDA. For example, HL7 released a consent-specific Consent Directives Implementation Guide (IG) for CDA that is "intended to provide multiple representations for expressing privacy preferences and for exchanging privacy policies that can be enforced by consuming systems."[100] The IG addresses metadata tagging and the electronic exchange of patient privacy preferences and policies, and also provides instruction on how to send non-computable, scanned versions of a signed patient consent in the unstructured body of a CDA document. In sum, this IG enables providers to process CDA documents in a way that complies with patient consent decisions.

5.2 Conceptual HIO Architecture

In its 2009 white paper on health information exchange, the Healthcare Information and Management Systems Society (HIMSS) discusses a conceptual HIO architecture.[101] This conceptual architecture is important because it identifies the following business layer services and data layer elements that support electronic consent management:

---

[98] See also, 45 C.F.R. Part 170, Subpart B - Standards Implementation Specifications for Health Information Technology, available at: http://www.law.cornell.edu/cfr/text/45/part-170/subpart-B.

[99] See Implementation Guide for CDA Release 2.0, Privacy Consent Directive, Second Ballot, May 2010, p. 8.

[100] See HL7 Implementation Guide for CDA, Release 2: Consent Directives, Release 1, available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=280.

[101] See HIMSS HIE White Paper.

- Business Layer
    - Privacy Services, including patient consent
    - Security Services, including identity management and authentication
    - General Services, including auditing and logging
    - Workflow Services
    - Enterprise Master Patient Index (MPI) Services
    - Record Locator Services (RLS)
    - Vocabulary Services
    - Longitudinal Record Services
    - Reporting Services, including decision support for HIPAA
- Data Layer
    - Audit Logs
    - Vocabulary
    - Security Policy
    - Patient Consent Rules
    - Secured Health Messages
    - Record Locator Information
    - Business Rules and Patient Demographics and Registry
    - Patient Clinical Health Records
    - Clinical Information and Registry
    - Clinical Protocols and Guidelines

Figure 6 illustrates this conceptual HIO architecture.

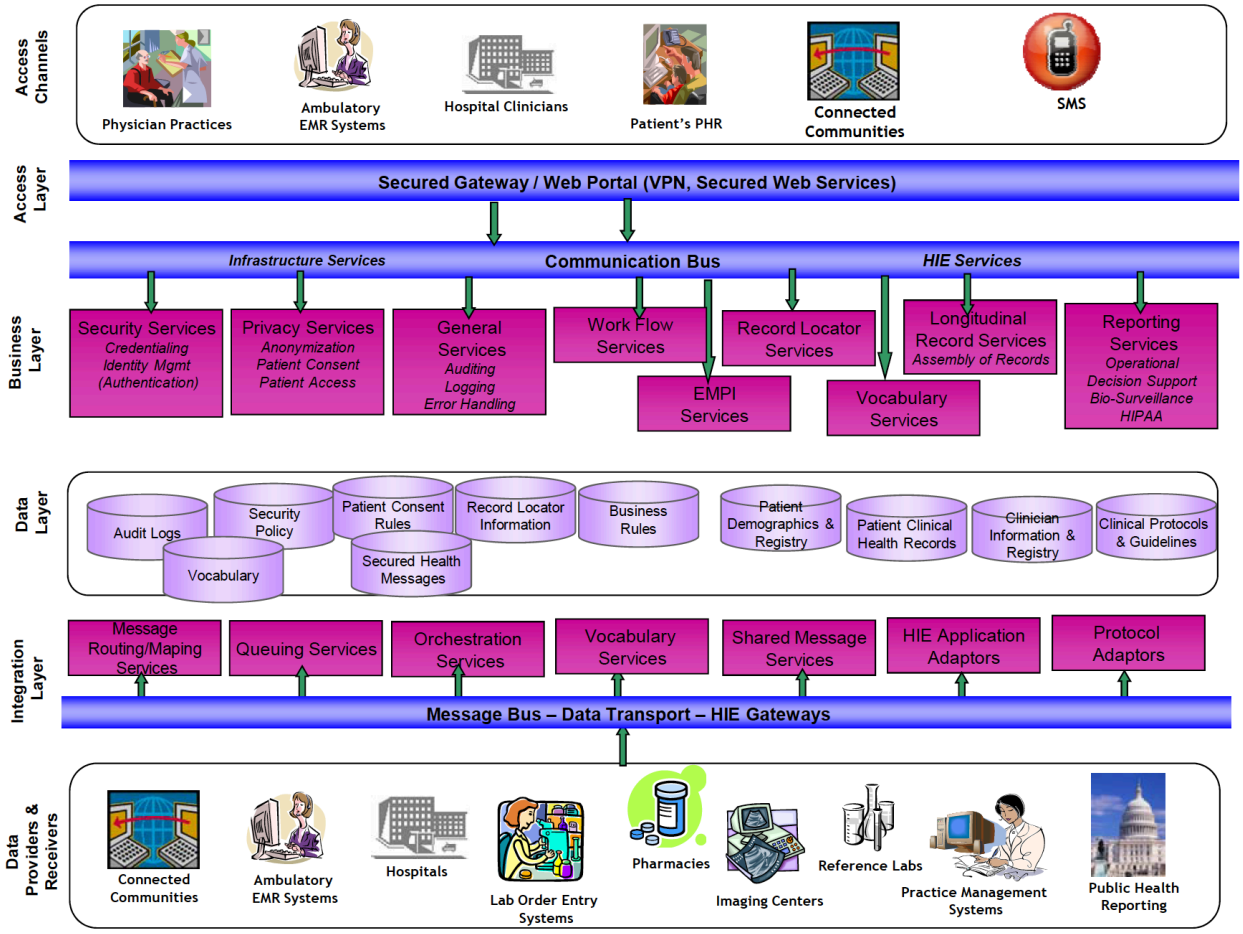

Figure 6. HIE Implementation Architectural View[102]

The pilot initiatives and developer systems discussed in this section leverage aspects of the services and elements identified in this conceptual architecture.

5.3 Common Technology Standards

The common health IT standards described in Table 4 were mentioned during our discussions. The table does not include every technology standard that may support patient consent; instead, it lists the standards referenced most frequently.

[102] See HIMSS HIE White Paper, p. 9.

Table 4. Common Technology Standards

Standard	Description
Transport Standards	
XDR	Cross-Enterprise Document Reliable Interchange (XDR) provides document interchange using a reliable messaging system. This permits direct document interchange between EHRs, PHRs, and other healthcare IT systems in the absence of a document-sharing infrastructure such as XDS Registry and Repositories.[103]
XDM	Cross-Enterprise Document Media Interchange (XDM) provides document interchange using a common file and directory structure over several standard media. This permits the patient to use physical media to carry medical documents. This also permits the use of person-to-person email to convey medical documents.[104]
XDS.b	Cross-Enterprise Document Sharing (XDS) facilitates the registration, distribution, and access across health enterprises of patient electronic health records. XDS.b followed XDS.a. XDS "is focused on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility and personal health record systems. This is managed through federated document repositories and a document registry to create a longitudinal record of information about a patient within a given clinical affinity domain."[105]
Messaging and Language Standards	
XML	Extensible Markup Language (XML) defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a free, open standard.
Health Level Seven International Version 2 / Version 3	Health Level Seven (HL7) version 2 is the most widely used healthcare messaging standard to exchange information. Its popular applications include admit, discharge, transfer (ADT) feeds, order messages (ORM) to order labs, and observation results (ORU) to communicate lab results. The hierarchical message structure includes segments, fields, data types, and vocabularies.
HL7 CDA	HL7's Clinical Document Architecture (CDA) is a document markup standard that specifies a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents. A CDA document is a defined and complete information object that can include text, images, sounds, and other multimedia content. CDAs have several important characteristics, including persistence, potential for authentication, context, and human readability. The CDA has several design principles, including compatibility with XML and the HL7 reference implementation model (RIM). CDA documents must be human-readable using generic CDA style sheets, and the architecture should impose minimal constraints on the document structure and content while accommodating fine-grained markup such as highly structured text and coded data. CDA documents have a common structure that includes a header and body.[106]

[103] See Cross-enterprise Document Reliable Interchange, available at: http://wiki.ihe.net/index.php?title=Cross-enterprise_Document_Reliable_Interchange.

[104] See Cross-Enterprise Document Media Interchange, available at: http://wiki.ihe.net/index.php?title=XDM.

[105] Cross-Enterprise Document Sharing, available at: http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing.

[106] See What is the CDA? available at: https://www.hl7.org/documentcenter/public_temp_72FAE36F-1C23-BA17-0C8BAFC56B09CBB2/calendarofevents/himss/2012/CDA%20and%20CCD%20for%20Patient%20Summaries.pdf.

Standard	Description
HL7 C-CDA	The Consolidated CDA (C-CDA) specifies libraries of templates and prescribes their use for a set of CDA document types. These implementation guides incorporate and harmonize previous work by HL7, Integrating the Healthcare Enterprise (IHE), and the Health Information Technology Standards Panel (HITSP). There are nine C-CDA document types, one of which is the CCD.[107]
HL7 CCD	The HL7 Continuity of Care Document (CCD) is an XML-based, US-specific markup standard used for patient summary clinical document exchange. The CCD contains patient demographic information and clinical facts. Each CCD contains a mandatory textual part for human interpretation and an optional structured part for software processing. CCDs enable providers to aggregate pertinent data about a patient and share it with another provider.[108]
C32	C32 is a standard CCD messaging format established by HITSP. C32 documents serve a variety of purposes, including enabling clinical access to patient data in an emergency scenario, quality reporting, biosurveillance, patient access to PHRs, and medication/allergy reconciliation.[109]
XACML	The Extensible Access Control Markup Language (XACML) defines access control policy language and is able to process how to evaluate access requests according to rules defined in a policy. XACML promotes common terminology and interoperability between access control implementations by multiple vendors. XACML is primarily an attribute-based access control system (ABAC), where attributes (bits of data) associated with a user, action, or resource are inputs into the decision of whether a given user may access a given resource in a particular way. Role-based access control (RBAC) can also be implemented in XACML as a specialization of ABAC.
SAML	The Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between parties (an identity provider and a service provider). SAML is able to address single sign-on (SSO) in a web browser by specifying assertions between a service provider, an identity provider, and a principal (the user).[110]
Vocabulary Standards	
LOINC	Logical Observation Identifiers Names and Codes (LOINC) is a database of terms used for the exchange and pooling of results for clinical care, outcomes management, and research. These include both laboratory and clinical observations.[111]
SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT) is a comprehensive clinical terminology originally created by the College of American Pathologists.[112] SNOMED CT is a computer-readable collection of medical terms that cover anatomy, disease, findings, and other categories. It facilitates the indexing, storage, and retrieval of medical data.

[107] See Consolidated CDA Overview, available at: http://www.healthit.gov/policy-researchers-implementers/consolidated-cda-overview.

[108] See HL7 IG for CDA R2 – Continuity of Care Document (CCD) Release 1, available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6.

[109] See C32/CCD Clinical Summary, available at: http://www.ihs.gov/RPMS/PackageDocs/BJMD/bjmd010u.pdf.

[110] See Security Assertion Markup Language, available at: http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language.

[111] See LOINC, available at: http://loinc.org/background.

[112] See SNOMED Clinical Terms, available at: http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html.

Standard	Description
RxNorm	RxNorm "provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software."[113]
ICD-9 / ICD-10	The International Classification of Diseases (ICD) is the standard diagnostic tool for epidemiology, health management, and clinical purposes. ICD codes are used to classify diseases and other health problems recorded on many types of health and vital records.[114]

5.4 Pilot Programs

Contributors discussed pilot programs that have demonstrated that electronic patient consent management is possible with existing technologies. This subsection discusses two such programs: Data Segmentation for Privacy (DS4P) and Consent2Share (C2S).[115]

Data Segmentation for Privacy (DS4P)

In September 2011, ONC's Office of the Chief Privacy Officer (OCPO) and Office of Science and Technology (OST) partnered to fund the Data Segmentation for Privacy (DS4P) initiative. DS4P brought together experts including software developers, healthcare providers, patient advocates, and health informaticists, to assess health IT data standards and their practicality.[116]

Data segmentation technology is used to alert providers if information they want to share is subject to certain restrictions, such as "do not redisclose without the patient's consent." Data segmentation technology can also potentially give patients more detailed choice regarding which parts of their health information are shared by providers.[117] This technology was developed with Part 2 in mind; specifically, the need to electronically share sensitive information and limit redisclosure.

By 2014, DS4P test cases ("pilots") demonstrated the ability to exchange sensitive electronic health information with the proper, standardized privacy metadata. This enabled receiving organizations to properly handle health information and control its further access and redisclosure.

Pilots demonstrated that DS4P technology was able to tag Consolidated Clinical Document Architecture (CCDA) documents with appropriate and machine-readable disclosure restrictions. Using these data classification labels, a provider who electronically receives patient substance abuse records can implement a prohibition on redisclosure notice.[118]

Upon reviewing DS4P's progress, the Privacy and Security Tiger Team (Tiger Team) supporting the HITPC recommended two glide paths for the exchange of Part 2 data, one for senders and the other for receivers, as outlined in Tables 5 and 6.

[113] RxNorm, available at: http://www.nlm.nih.gov/research/umls/rxnorm/.

[114] See International Classification of Diseases (ICD), available at: http://www.who.int/classifications/icd/en/.

[115] The Software and Technology Vendors' Association (SATVA) also successfully demonstrated electronic consent management of Part 2 data. A demonstration video is available at: http://www.satva.org.

[116] See What is the History of Data Segmentation Efforts, available at: http://www.healthit.gov/providers-professionals/data-segmentation-overview (hereinafter DS4P Overview)

[117] DS4P Overview (Why Does Data Segmentation Matter?)

[118] DS4P Overview (How Does Data Segmentation Typically Work?)

Table 5. Glide Path for Senders of Part 2-Protected Data[119]

Level	Status	Description
0	Current State	Sender cannot send patient information electronically without some technical capability to indicate information is subject to restrictions on redisclosure consistent with Part 2. Sender also has to have confidence that receiver can properly handle electronically sent Part 2-protected data.
1	Document-level Sequester	With authorization from the patient, sender EHR can send Consolidated Clinical Document Architecture (CCDA) tagged as restricted and subject to Part 2 restrictions on redisclosure.

Table 6. Glide Path for Recipients of Part 2-Protected Data[120]

Level	Status	Description
0	Current State	Part 2-protected data is not provided electronically to general healthcare providers. The status quo remains to share Part 2-protected data via paper, fax, etc.
1	Document-level Sequester	Recipient EHR can receive and automatically recognize documents from Part 2 providers, but the document is sequestered from other EHR data. A recipient provider using DS4P would have the capability to view the restricted CCDA (or data element), but the CCDA or data cannot be automatically parsed/consumed/inter-digitated into the EHR. Document-level tagging can help prevent redisclosure.
2	Local Use Only Solution	Recipient EHR can parse and extract data from structured documents from Part 2 providers for use in local Clinical Decision Support (CDS) and quality reporting engines, but data elements must be tagged and/or restricted to help prevent redisclosure to other legal entities through manual or automated reporting or interfaces. This would allow the data to be used locally for CDS but would not require complicated redisclosure logic for the EHR vendor (i.e., processes related to redisclosure are not well-defined).
3	EHRs for General Use and Sharing Advanced Metadata and Redisclosure	Recipient EHR can consume patient authorization for redisclosure from Part 2 provider and act on such authorizations at a data level. At a minimum, the recipient EHR would need to make the user aware of whether additional Part 2 consent is required before redisclosing any particular data element to another legal entity and allow recording of patient authorization for redisclosure at the data level. Processes for redisclosure are well-defined.

The Tiger Team recommended that Level 1 send and receive functionality be included in the voluntary certification program for behavioral health providers under Meaningful Use Stage 3. The Tiger Team also recommended including Level 1 receiver functionality as a voluntary certification criterion for Certified EHR Technology (CEHRT).

[119] HIT Policy Committee Transmittal Letter, July 15, 2014, p. 2, available at: http://www.healthit.gov/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf (hereinafter July 15 Transmittal Letter).

[120] July 15 Transmittal Letter, p. 3.

Consent2Share

The Consent2Share initiative is a pilot project sponsored by SAMHSA that builds from the work pioneered by DS4P. Consent2Share is an open-source tool for consent management and data segmentation that is designed to integrate with existing EHR and HIO systems. The Consent2Share architecture contains two components: a patient-facing system called Patient Consent Management (PCM) and a backend system called Access Control Services (ACS). The PCM enables patients to capture, electronically sign, and revoke their consent directives. The ACS provides a Policy Enforcement Point (PEP), a Policy Decision Point (PDP), and a Data Segmentation Engine to enforce consent directives and apply privacy metadata to clinical documents. This technical approach includes the ability to redact data based on patient preferences and to apply metadata tags to clinical documents—for example, confidentiality, applicable privacy law, refrain policy (such as redisclosure warnings under Part 2), and obligation policy tags.[121] Figure 7 shows the Consent2Share system and its objectives.

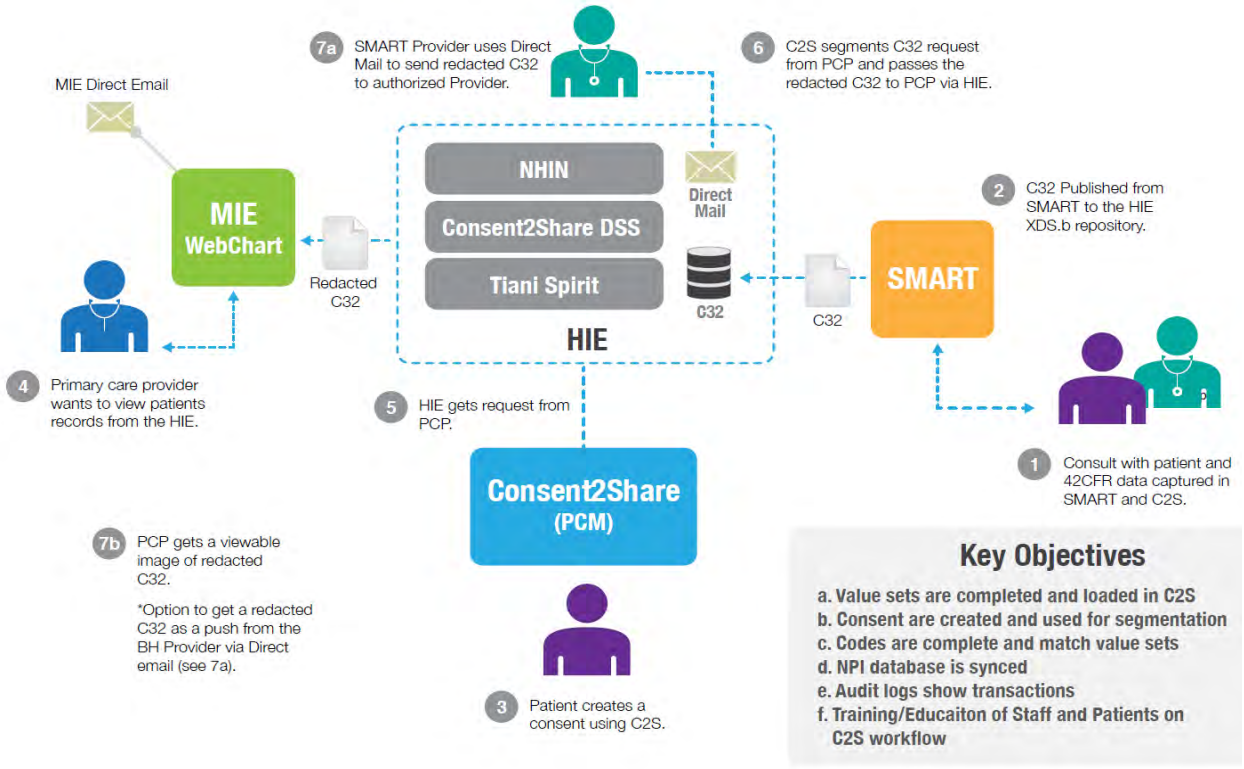

Figure 7. Consent2Share Ecosystem Diagram

5.5 Federal Efforts

Electronic consent management is also being addressed by federal agencies collaborating under the Federal Health Architecture (FHA). FHA seeks to improve health information exchange and interoperability among federal agencies, including their trading partners. These federal partners include the Department of Defense (DoD), Indian Health Services (IHS), the Social Security

[121] See http://wiki.siframework.org/SAMHSA+Consent2Share+Project.

Administration (SSA) and the Department of Veterans Affairs (VA); each have established methods for managing patient consent and authorization issues. The DoD, IHS and VA have at least 40% of their patients receiving treatment from private practice; therefore the challenges that they face are not just internally focused but external as well.

Department of Defense

The DoD serves over 1.2 million active duty soldiers and their families in over 65 hospitals and 412 clinics. The challenge for the DoD is to effectively manage the patient consent and authorization for soldiers that must deploy around the world and still have access to their information. Additionally, the DoD also supports the family members and dependents, and the patient consents and authorizations are generally treated with a higher level of protection. This information is managed within the military EHR represented by AHLTA.

Currently, DoD has a proposal for a new EHR with the anticipation of an award in the near future. This new system is mentioned because it may alter the way that patient consents and authorizations are managed in the future.

DoD has more than one means of sharing information between organizations whether federal or commercial. Currently, it is effective for DoD to manage the patient consents and authorizations on paper and scan it later so it can be processed as an electronic consent. Some administrators have expressed concern that it is possible that automation may initially slow down the process of managing these consents and authorizations.

Another issue experienced at DoD, and in most healthcare organizations, is that the current system is not able to handle the information at a very granular level. For example, if the patient or entity marks one piece of information as sensitive, the whole record is rendered not viewable.

In addition to consideration of all of the typical laws, policies and regulations that govern US consents and authorizations, the DoD must occasionally work with international organizations for treatment of patients. This international component increases the level of complexity for the DoD but is generally handled as a manual process that relies on the knowledge of local experts.

DoD is governed by the following Privacy Laws and Statutes

- Privacy Act, as amended, Title 5 United States Code (USC) 552a, implemented by Title 5 Code of Federal Regulations (CFR) Part 5b, provides for the confidentiality of individually identifiable and retrievable information about living individuals that is maintained in a Privacy Act system of records.
- Health Insurance Portability and Accountability Act (HIPAA), Public Law (Pub. L.) 104-191, implemented by 45 CFR Parts 160 and 164, establishes standards and requirements for the electronic transmission, privacy, and security of PHI/PII.
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, governs how organizations will address the access, use, and disclosure of PHI, including receiving an electronic copy of the patient's file. It also establishes a national breach notification requirement when information is accessed in an unauthorized or inappropriate manner.

- 38 U.S.C. 7332 - Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records
- 38 U.S.C. 5705 - Confidentiality of Healthcare Quality Assurance Review Records

Indian Health Services

IHS serves members of 566 federally recognized Tribes. The challenge for IHS is that they must manage federal, state, local and tribal considerations as well as protect sensitive patient information. IHS also has a large minor population that presents some unique challenges in managing consents and authorizations, particularly when patients receive treatment in multiple states.

IHS generally uses the Resource and Patient Management System (RPMS). RPMS is a decentralized, integrated public health information system and is in use at approximately 400 facilities nationwide, including all federal IHS facilities and most tribal programs. The use or disclosure of health information in IHS is managed by Facility Health Information Management (HIM) Department.

The HIM staff validates requests before disclosing health information. They must continue to manage consent within new HIE-related services as well. The consent default is out of exchange and a patient is given the opportunity to opt–in. The IHS-810 Form or Written Request provides a description of information to release and indicates a date or range of dates. Both the hard copy and soft copy are maintained. There is no granularity of information as it is just recognized as a scanned document. Authorization is good for 5 years.

Due to the large population of minors, IHS consent management can become complicated. The policy for access and disclosure of Personal Health Information for un-emancipated minors was revised to include Personal Health Record (PHR) (Privacy Act more stringent) access. The parent may access information about treatment for which they (the parent) provided the consent. A minor is treated like an adult when they consent to treatment. The parent agrees to confidentiality of treatment, or submits a court order for services. If the parent requests to create or access the minor's PHR, they must submit an electronic request for a PHR Account and provide verification of identity. A written request (IHS-810) must be approved by a health professional. The PHR Account is created/must agree to PHR Terms & Conditions. Filtered information is not shared with the parent (e.g., birth control, STDs, Substance Abuse treatment, services for which the minor may consent, etc.).

Some of these challenges can be overcome with:

- Consistent alignment of laws, policies and regulations
- Revised laws, policy frameworks and regulations to leverage the capabilities of current and future IT
- Constrained consent/authorization standards in order to improve interoperable exchange
- Effective implementation of a computable patient consent management system

IHS is governed by the following Privacy Laws and Statutes

- Privacy Act, as amended, Title 5 United States Code (USC) 552a, implemented by Title 5 Code of Federal Regulations (CFR) Part 5b, provides for the confidentiality of

individually identifiable and retrievable information about living individuals that is maintained in a Privacy Act system of records.

- Health Insurance Portability and Accountability Act (HIPAA), Public Law (Pub. L.) 104-191, implemented by 45 CFR Parts 160 and 164, establishes standards and requirements for the electronic transmission, privacy, and security of PHI/PII.
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, governs how organizations will address the access, use, and disclosure of PHI, including receiving an electronic copy of the patient's file. It also establishes a national breach notification requirement when information is accessed in an unauthorized or inappropriate manner.
- Indian Heath Care Improvement Act, 25 USC, Section 1662.

Department of Veterans Affairs

The VA has over 1,269 hospitals, centers or clinics that support more than 8.9 million enrolled Veterans. The challenge for the VA is to receive and manage records from other federal organizations and interact with private organizations in the treatment of veterans.

The VA uses VistA as its EHR. All patients are considered to be out of exchange by default unless they opt-in, thereby changing that status. The VA provides veterans with the option to complete an authorization form in-person at their VA Medical Center, on the eBenefits Web portal or with signature pads.

To electronically manage consents, the VA uses iMedConsent. This software package supports electronic access, completion, electronically captured signature, and storage of documents such as informed consent forms and advance directives.

VA's current universal approach of having everyone out of exchange as the default state has historically been driven by requirements of 38 USC 7332 which requires special protection for certain categories of protected health information (PHI). Currently, all Veterans must actively choose (opt-in) to allow their health information to be exchanged. This means that each and every Veteran must specifically choose to share their PHI by signing an authorization regardless of whether or not they actually have a 38 USC 7332 protected condition.

While effective in meeting 38 USC 7332 requirements, universal out of exchange as the default state has placed an unnecessary burden on millions of Veterans who would otherwise have been willing to share their PHI with Covered Entities for the purpose of treatment, payment, and healthcare operations, as already permitted by HIPAA. This universal requirement for actively opting-in to an exchange may be responsible for the current low rate of Veteran participation in health information exchange.

The VA has worked diligently within the federal community to encourage electronic patient consent. For example, the VA played a key role in advancing HL7 standards. The VA's future efforts will include consent tools based on the HL7 Fast Healthcare Interoperability Resource (FHIR) in a hypertext transfer protocol (HTTP)-based Representational State Transfer (RESTful) architecture.[122] FHIR enables interoperability so that patient "resources," which are instances of

[122] See Fast Healthcare Interoperability Resource (FHIR), available at: http://wiki.hl7.org/index.php?title=FHIR.

data that are stored or exchanged,[123] can be represented in multiple languages (XML, JSON, HTML), and each resource has a predictable uniform resource locator (URL).

VA is governed by the following Privacy Laws and Statutes[124]

- The Privacy Act [5 U.S.C.552a]
- The Health Insurance Portability and Accountability Act (HIPAA) [45 CFR Parts 160 and 164]
- 38 U.S.C. 5701 - VA Claims Confidentiality Statute
- 38 U.S.C. 7332 - Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records
- 38 U.S.C. 5705 - Confidentiality of Healthcare Quality Assurance Review Records

Social Security Administration

SSA requests medical documentation from a healthcare provider with the patient's authorization in order to determine disability claims. The primary challenge for SSA is to effectively manage the patient authorizations so that they can efficiently receive information to substantiate claims; consequently, there is a need to receive and manage patient authorizations in an effective manner.

Generally, patients that have engaged SSA are interested in substantiating their claims. By the very nature of the request, they must provide authorization so SSA can receive correct supporting information. SSA developed an authorization form, Form SSA–827 (Patient Authorization) which is now universally accepted by all providers across the country. This standardization of the form, and the processes incorporated with it, dramatically improved the effectiveness of their data management practices. Previously, most of the documentation was handled through a manual process. Now, the SSA leverages the eHealth Exchange to allow a provider to retrieve the stored patient authorization and ultimately provide SSA with a summary of care document in support of the patient's claim. The process allows claimants the option to sign and submit Form SSA–827 electronically rather than completing a paper form with a pen and ink signature. The attestation process for applications is taken in person and over the telephone. The exchange uses an Authorization Decision Statement to allow an entity to assert that the requester be permitted to execute the transaction based on a specific security policy. The Access Consent Policy and Authorization Framework specifications define the format of the policy.

SSA is governed by the following Privacy Laws and Statutes

- Privacy Act, as amended, Title 5 United States Code (USC) 552a, implemented by Title 5 Code of Federal Regulations (CFR) Part 5b, provides for the confidentiality of

[123] See Definitions, available at: http://www.hl7.org/implement/standards/fhir/resources.html.

[124] Information available at: http://www.gpo.gov/fdsys/browse/collectionUScode.action?collectionCode=USCODE&bread=true

iMedConsent at http://www1.va.gov/VHAPUBLICATIONS/ViewPublication.asp?pub_ID=3064

individually identifiable and retrievable information about living individuals that is maintained in a Privacy Act system of records.

- Health Insurance Portability and Accountability Act (HIPAA), Public Law (Pub. L.) 104-191, implemented by 45 CFR Parts 160 and 164, establishes standards and requirements for the electronic transmission, privacy, and security of PHI/PII.
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, governs how organizations will address the access, use, and disclosure of PHI, including receiving an electronic copy of the patient's file. It also establishes a national breach notification requirement when information is accessed in an unauthorized or inappropriate manner.
- Sections 205(a), 233(d)(5)(A), 1614(a)(3)(H)(i), 1631(d)(l) and 1631(e)(l)(A) of the Social Security Act as amended, [42 U.S.C. 405(a), 433(d)(5)(A), 1382c(a)(3)(H)(i), 1383(d)(l) and 1383(e)(l)(A)]
- P.L. 104-191 ("HIPAA")
- 42 U.S. Code section 290dd-2
- 42 CFR part 2; 38 U.S. Code section 7332
- 38 CFR 1.475
- 20 U.S. Code section 1232g ("FERPA")
- 34 CFR parts 99 and 300
- State law

5.6 Developer Solutions

Developers discussed the capabilities of their software and products (solutions) with regard to consent management. Health IT solutions vary considerably in the way they capture, process, and store consent. Nevertheless, these solutions consistently leverage common transport, messaging, and vocabulary standards. The following paragraphs discuss a few of these solutions without identifying the particular developer.

One developer offers a web-based solution that enables service organizations to help patients share sensitive information, including mental health, substance abuse, HIV/AIDS, and developmental disabilities information. The workflow requires a patient to be present in order to register to share information electronically. Either the patient can complete a digital consent form at the provider's office and sign a signature pad or click a confirmation box, or the patient can obtain a personal identification number (PIN) upon verifying his or her identity with the provider's staff, then use the pin to log in and register consent from a computer at home.

The patient's consent decision is recorded as a standardized data element in an HL7 ADT A08 message transaction. This data element is recorded as a "Y" granting permission to share, "N" denying permission, or "U" to "unset." (This feature resets the consent process and purges all prior information so that it appears that the patient had never before granted the HIO authorization to share information.)

If the patient has not previously registered, then patient demographic information in the ADT message is matched with demographic information in the HIO's master patient index. (The developer supports an organization that uses a centralized architecture). The developer retains a copy of the ADT message in its own database.

The developer does not yet support health information exchange among Part 2 providers, but the developer noted that its technology could be modified to provide granular patient consent in the future. This would be done by filtering content in CDA documents based on a mapping to the patient's consent directive.

A second developer discussed its solution, which customers use as a stand-alone HIO. Consent is initially collected in either paper form, which is transcribed into electronic form by the provider's clerical staff, or electronically via the provider's web portal computer. Consent is transmitted to the developer's centralized database either as an ADT message or an XACML document. Clients that use ADT messages are usually operating in opt-in or opt-out models; all that is required is a "Yes," "No," or "Withdraw" consent decision.

The developer also uses XACML documents to manage patient consent. The XACML consent document is transmitted via the XDS.b profile. XACML offers greater flexibility to identify structured data elements that a patient decides may or may not be accessed and shared. The developer mentioned that this capability is not widely used, but it expects that XACML format for sharing consent will become more popular as demand for more granular consent grows.

A third developer deployed its solution to customers in the behavior health community. The solution uses common standards established by standards developing organizations (SDOs) such as HL7, Basic Patient Privacy Controls (BPPC), and Integrating the Healthcare Enterprise (IHE). Providers can establish and configure their own consent policies, and the developer maintains a secondary consent policy that explicitly defines which participants can share sensitive information. The solution maintains a robust audit mechanism that flags each time a consent document changes. The audit capability also identifies each time a provider accesses health information and which specific health information is accessed. This solution also uses XACML and BPPC standards to electronically manage patient consent at the document level. The developer stated that it is possible to track data at the data element level but that this type of segmentation is not yet used.

6 Suggestions

When asked what the federal government could do to facilitate the adoption of electronic consent management, contributors offered several suggestions. These suggestions may be considered for further research and consideration, but they are not formal recommendations.

6.1 Federal Electronic Consent Management Framework

During our discussions, several participants suggested that the federal government take the lead in developing a model framework to address electronic consent management. They noted that a commonly used model for sharing consent information does not yet exist. A federal framework could include guidance for how consent is collected, what data elements must be captured, what vocabularies are used, what messaging standards are used, how data provenance should be tracked, and what identity and access management controls should be applied. Participants stated their belief that electronic patient consent will not become mainstream until the federal government openly supports such a consent framework.

Although it was not clear how the government might advance a model framework, one contributor suggested a system of adoption similar to the ballot process that standards developing organizations (SDOs) use to review and approve new standards. Generally, this process involves registration; receiving the ballot document, comment spreadsheet, and supplemental materials; reviewing the implementation guide; submitting comments; providing a vote; reconciling the ballot; and a final vote.[125] The participant also stressed that ONC, CMS, and SAMHSA should engage together to ensure broad participation from the healthcare community.

6.2 Standard Sensitive Information Consent Form

MITRE's discussions identified a desire to have a common standardized consent form that would satisfy the requirements set forth in various confidentiality laws. According to developers, electronic consent forms vary from state to state, HIO to HIO, and EHR to EHR. Some developers have invested significant money and time to code electronic consent forms that comply with the rules of each jurisdiction in which they operate.

The Legal Action Center (LAC), a nonprofit law and policy organization that fights discrimination against people with histories of addiction,[126] provides several sample consent forms, including a form for Part 2 consent.[127] LAC has experience in dealing with Part 2, as it prepared the most recent edition of the SAMHSA FAQ.

6.3 Centralized Services

Some participants suggested that a nationwide enterprise master patient index (MPI) would be useful for ensuring proper identification of and access to patient health information. Others suggested this was not possible given that it would require a universal patient identification number, which would be met by privacy concerns.

Nevertheless, participants suggested that it would be beneficial to have a nationwide index of healthcare providers to support consent decisions when patients select providers who may have

[125] See CET Ballot Reconciliation, available at: http://wiki.siframework.org/CET+-+Ballot+Reconciliation.

[126] See LAC's Mission, available at: http://lac.org/index.php/lac/category/about_us.

[127] See Sample Forms, available at: http://lac.org/resources/substance-use-resources/confidentiality-resources/sample-forms-confidentiality/.

access to their health information. A nationwide registry of providers already exists in the form of the National Plan & Provider Enumeration System National Provider Identifier (NPI),[128] but the NPI is not adapted to support patient consent. Contributors suggested leveraging NPI for patient consent, but this has not been explored.

Finally, one participant suggested that the federal government help create a centralized consent inventory. This inventory would contain the most current patient consent information, and every HIO and health IT system could reference the central consent inventory as part of the health information exchange process.

6.4 Education

Our discussions emphasized the need for more education about the rules for sharing sensitive health information and electronic patient consent. Previous studies have stated that education for HIPAA implementation was costly and time-consuming.[129] Participants asserted that providers are often saddled with the burden of educating patients about their consent options because providers have direct contact with patients at the point of intake when the consent decision is made.

As a result, participants suggested that ONC partner with other federal agencies to create concise and informative videos or other media to educate both patients and providers about the value of electronic patient consent and the rules for sharing sensitive health information.

6.5 Identity and Access Management (IDAM) Solutions

To address IDAM concerns related to unauthorized access to and use of patient-facing portals, participants suggested a number of options:

- Use multi-factor authentication[130] to ensure stronger security, especially for web portal access. This method could involve sending a real-time text message code to a patient's cell phone and requiring a patient to enter that code to log in to their portal page.
- Require patients to initially appear in person before obtaining access to a portal; provide patients with a PIN or a one-time password once their identity is confirmed.
- Employ more sophisticated (possibly more expensive) authentication solutions that require patients to answer questions only they would know the answers to, such as the amount they pay on their mortgage, or the sum of the first and last digits of their social security number.

6.6 More Financial Incentives

Additional financial incentives could be an effective way to encourage more providers to embrace sophisticated electronic consent management technologies. Participants stated that clinical counselors and treatment facilities are not eligible for the Medicare and Medicaid EHR Incentive Programs. Expanding the pool of eligible participants may increase the adoption of electronic consent management technologies.

---

[128] See National Plan & Provider Enumeration System, NPI Registry, available at: https://nppes.cms.hhs.gov/NPPES/NPIRegistryHome.do.

[129] See Consumer Consent Options, p. 35.

[130] Two-factor authentication requires a user to submit multiple types of identity proofs, which usually includes something known and something possessed. See Two-Factor Authentication, available at: http://technet.microsoft.com/en-us/library/jj916649.aspx.

6.7 42 C.F.R. Part 2 (Part 2) Reform

Finally, participants stated that reforms to Part 2 could simplify electronic consent management, making it more attractive and implementable. First, the requirement to identify specifically who can receive information could be relaxed. Currently, Part 2 patients cannot consent to sharing their health information with future Part 2 providers that are not named.

Second, participants suggested that electronic consent management would be more widely adopted if sharing under Part 2 were made consistent with HIPAA rules. To offset the relaxed rules for sharing, enforcement could be strengthened to prevent the misuse of sensitive information.[131] Under these revisions, participants believed, electronic consent management might gain more traction.

[131] Current penalties for violating Part 2 begin at $500 and are capped at $5,000 for subsequent offences. See 42 C.F.R. § 2.4, available at: http://www.law.cornell.edu/cfr/text/42/2.4.

Glossary

Term	Definition
Clinical Document Architecture (CDA)	HL7's document markup standard that specifies a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents. A CDA document is a defined and complete information object that can include text, images, sounds, and other multimedia content. CDAs have several important characteristics, including persistence, potential for authentication, context, and human readability. The CDA has several design principles, including compatibility with XML (an open source language standard) and the HL7 reference implementation model, that CDA documents must be human-readable using generic CDA style sheets, and that the architecture should impose minimal constraints on the document structure and content while accommodating fine-grained markup such as highly structured text and coded data. CDA documents have a common structure that includes a header and body. See CDA Release 2, available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7.
Consolidated Clinical Document Architecture (C-CDA)	Implementation guides that specify libraries of templates and prescribe their use for a set of CDA document types. The guides incorporate and harmonize previous work by HL7, Integrating the Healthcare Enterprise (IHE), and the Health Information Technology Standards Panel (HITSP). There are nine C-CDA document types, one of which is the CCD. Source: http://www.healthit.gov/policy-researchers-implementers/consolidated-cda-overview.
Continuity of Care Document (CCD)	The HL7 XML-based, US-specific markup standard used for patient summary clinical document exchange. The CCD contains patient demographic information and clinical facts. Each CCD contains a mandatory textual part for human interpretation and an optional structured part for software processing. CCDs enable providers to aggregate pertinent data about a patient and share it with another provider. Source: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6.
Electronic Health Record (EHR)	Digital version of a patient's paper chart maintained by a healthcare provider. Source: http://www.healthit.gov/patients-families/health-it-terms.

Term	Definition
Health Information	Any information, whether oral or recorded in any form or medium, that (1) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual. See 45 C.F.R. § 160.103. Source: http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf
Health Information Exchange (HIE)	The electronic movement of health-related information among organizations according to nationally recognized standards. HIE allows healthcare providers and patients to appropriately access and securely share a patient's vital medical information electronically. Source: http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie.
Health Information Organization (HIO)	Entity that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards. In practice, the term HIE is often used synonymously with HIO. Source: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf.
Health Information Technology	Hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by healthcare entities or patients of the electronic creation, maintenance, access, or exchange of health information. Pub. L. No. 11-5 § 3000(5), available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf
Health Level Seven International (HL7)	A not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery, and evaluation of health services. Adapted from: http://www.hl7.org/about/index.cfm?ref=nav.

Term	Definition
HL7 Reference Information Model (RIM)	Cornerstone of the HL7 Version 3 development process and an essential part of the HL7 V3 development methodology. RIM expresses the data content needed in a specific clinical or administrative context and provides an explicit representation of the semantic and logical connections that exist between the information carried in the fields of HL7 messages. The RIM is essential to increasing precision and reducing implementation costs. Source: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf.
HL7 v2.x	The most widely implemented standard for health information in the world. V2 defines a series of electronic messages to support administrative, logistical, financial, and clinical processes. Source: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf.
HL7 v3.0	Uses an object-oriented development methodology and Reference Information Model (RIM) to create messages. The messages are also based on an XML encoding syntax. The V3 standard was developed around 1995, resulting in an initial standard publication in 2005. Source: http://www.himss.org/files/HIMSSorg/Content/files/HIE/HIE_GuideWhitePaper.pdf.
Individually Identifiable Health Information (IIHI)	Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual; and – (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. See 45 C.F.R. § 160.103. Source: http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf
Integrating the Healthcare Enterprise (IHE)	Standards organization comprising healthcare professionals and industry. IHE's objective is to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as Digital Imaging and Communications in Medicine (DICOM) and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE are expected to communicate better with one another, make implementation easier, and enable care providers to use information more effectively. Adapted from: http://www.ihe.net/About_IHE/

Term	Definition
Protected Health Information (PHI)	Protected health information means IIHI that is (i) transmitted by electronic media, (ii) maintained in electronic media, or (iii) transmitted or maintained in any other form or medium. PHI is not IIHI in (i) education records covered by the Family Educational Rights and Privacy Act (FERPA), (ii) certain student health records under 20 U.S.C. §1232g(a)(4)(B)(iv), or (iii) employment records held by a covered entity in its role as employer. See 45 C.F.R. 160.103. Source: http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf
Security Assertion Markup Language (SAML)	An XML-based open standard data format for exchanging authentication and authorization data between parties (an identity provider and a service provider). SAML is able to address single sign-on (SSO) in a web browser by specifying assertions between a service provider, an identity provider, and a principal (the user). See SAML, available at: http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language.
XACML	Extensible Access Control Markup Language in an access control policy language that describes how to evaluate access requests according to rules defined in policies. XACML promotes common terminology and interoperability between access control implementations by multiple developers. XACML is primarily an attribute-based access control system (ABAC), where attributes (bits of data) associated with a user, action, or resource are inputs into the decision of whether a given user may access a given resource in a particular way. Role-based access control (RBAC) can also be implemented in XACML as a specialization of ABAC. See XACML, available at http://en.wikipedia.org/wiki/XACML.
XML	Extensible Markup Language (XML) defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a free, open standard. See XML, available at: http://en.wikipedia.org/wiki/XML.

Contributors

Contributor	Type	Website
Chesapeake Regional Information System for our Patients	HIO	http://crisphealth.org/
Delaware Health Information Network	HIO	http://www.dhin.org/
Indiana Health Information Exchange	HIO	http://www.ihie.org/
Michigan Health Connect	HIO	http://michiganhealthconnect.org/
Rochester Regional Health Information Organization	HIO	http://www.grrhio.org/
American Medical Association	Provider	http://www.ama-assn.org/ama
College of Healthcare Information Management Executives	Provider	http://www.cio-chime.org/
National Rural Health Association	Provider	http://www.ruralhealthweb.org/
New England Healthcare Exchange Network	Provider	http://www.nehen.org/
Cerner Corporation	Developer	http://www.cerner.com/
Core Solutions	Developer	http://www.coresolutions.com/
Epic Systems	Developer	http://www.epic.com/
Foothold Technologies	Developer	http://footholdtechnology.com/
GE Healthcare	Developer	http://www3.gehealthcare.com/en/global_gateway
Netsmart	Developer	http://www.ntst.com/
Sandlot Solutions	Developer	http://www.sandlotsolutions.com/
Martin, Blanck and Associates	SME	http://www.martin-blanck.com/
National Council for Behavioral Health	SME	http://www.thenationalcouncil.org/
Nixon Peabody LLP	SME	http://www.nixonpeabody.com/
Patient Privacy Rights	SME	http://patientprivacyrights.org
Popovits and Robinson Health Law	SME	http://www.popovitslaw.com/

Acronyms

Term	Definition
ACS	Access Control Services
ADT	Admit Discharge Transfer
AIDS	Acquired Immunodeficiency Syndrome
ANSI	American National Standards Institute
BPPC	Basic Patient Privacy Controls
BRMS	Business Rule Management System
CCD	Continuity of Care Document
CDA	Clinical Document Architecture
CDR	Clinical Data Repository
CMS	Centers for Medicare & Medicaid Services
CPeH	Consumer Partnership for eHealth
DS4P	Data Segmentation for Privacy
EHR	Electronic Health Record
FAQ	Frequently Asked Questions
FHIR	Fast Healthcare Interoperability Resource
HIE	Health Information Exchange
HIMSS	Healthcare Information and Management Systems Society
HIO	Health Information Organization
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
HITPC	Health Information Technology Policy Committee
HIV	Human Immunodeficiency Virus
HL7	Health Level Seven International
HTML	Hypertext Markup Language
ICD	International Statistical Classification of Diseases and Related Health Problems
IDAM	Identity and Access Management
IG	Consent Directives Implementation Guide
IHE	Integrating the Healthcare Enterprise

Term	Definition
IIHI	Individually Identifiable Health Information
IT	Information Technology
JSON	JavaScript Object Notation
LAC	Legal Action Center
LOINC	Logical Observation Identifiers Names and Codes
MU	Meaningful Use
NEHEN	New England Healthcare Exchange Network
NPI	National Provider Identifier
ONC	Office of the National Coordinator for Health Information Technology
PCM	Patient Consent Management
PDF	Portable Document Format
PHI	Protected Health Information
PHR	Personal Health Record
PIN	Personal Identification Number
RFC	Request for Comments
RHIO	Regional Health Information Organization
RIQI	Rhode Island Quality Institute
RLS	Record Locator Service
SAMHSA	Substance Abuse and Mental Health Services Administration
SAML	Security Assertion Markup Language
SME	Subject Matter Expert
SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms
VA	Department of Veterans Affairs
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language