This report was prepared by John R. Christiansen, J.D., in collaboration with Chris Apgar and Dennis Melamed for the National Governors Association Center for Best Practices.
State and Federal Consent Laws Affecting Interstate Health Information Exchange
2011

Contents

1. Executive Summary .................................................................................................................. 1
2. Introduction ............................................................................................................................ 1
3. Consent Background and Management .................................................................................. 7
   3.1. Consent Issues in Electronic Health Information Exchange ........................................ 10
   3.2. Types of Consent ............................................................................................................ 15
   3.3. HISPC Consent Recommendations .............................................................................. 17
4. The Case Studies .................................................................................................................... 20
   4.1. Case Study Methodology ............................................................................................... 20
   4.2. Review of Cases .............................................................................................................. 21
      4.2.1. eHealthConnecticut ................................................................................................ 21
      4.2.2. CareSpark .............................................................................................................. 25
      4.2.3. HealthBridge .......................................................................................................... 28
      4.2.4. Inland Northwest Health Services 1HealthRecord .............................................. 30
      4.2.5. Kaiser Permanente ................................................................................................ 32
      4.2.6. Mayo Clinic ............................................................................................................ 36
      4.2.7. Surescripts ............................................................................................................. 41
      4.2.8. Texas Health Services Mental Health Transformation Project .............................. 43
      4.2.9. WellPoint Individual Health Record ..................................................................... 48
5. Legal Standards and Issues Affecting Use of Consents ....................................................... 51
   5.1. Consents under HIPAA: The Federal Baseline ............................................................ 52
   5.2. Federalism and the Application of State Laws in Other States’ Territories ................ 57
   5.3. Alcohol and Drug Abuse Treatment Program Records .............................................. 60
   5.4. Family Educational Rights and Privacy Act .................................................................... 63
6. The Problem of Diverging Standards .................................................................................... 71
7. Discussion of Report Findings and Tools ............................................................................. 72

Tables

Table 1: Consent Typology ........................................................................................................ 17
Table 2: Summary of Case Studies........................................................................................................21
“Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.”¹

“Liability issues appear to be one of the biggest obstacles to agreeing upon any standard approach to consent.”²

1. **EXECUTIVE SUMMARY**

The electronic exchange of health information has been touted as a means to improve the efficiency and effectiveness of our health care system. Exchanging health information requires individuals to grant permission for their records to move from one provider to another. The process of and requirements for obtaining individual consent for sharing information places more or less control of information use and disclosure in the individual’s hands, and can vary by types of information, duration of consent, and other variables. Differences in federal and state consent laws are often challenging for states, HIOs and providers to reconcile, creating one of the major obstacles to smooth and regular electronic health information exchange (HIE).

Consent is defined as a process intended to determine the level of control of information disclosure and use in individuals. The process may include any of the following elements: Notice to the individual, documentation of individual intent, documentation of the scope and terms of permission, and mechanisms for communicating and enforcing any limits on the permission. Collectively these consent elements guide how health information can be collected, shared and accessed.

As states and state designated entities begin collecting and exchanging electronic health information across state lines, they need to develop consent policies that comply with federal polices and align across state laws to ensure the adequate protection of health information while ensuring the information is available to providers to utilize in delivering care. Sensitive health information, such as HIV/AIDS status, genetic information and behavioral health status are of particular concern and require heightened protections and consent policies.


This report provides substantial background information that can help states, HIOs and providers in developing patient consent strategy in electronic health information exchange; and identifies legal standards and issues that should be addressed when developing these policies. This report is a technical document that assumes some knowledge of privacy laws and consent issues. The related Consents Toolkit is intended to provide analytical tools and suggestions for the identification and reconciliation of overlapping laws concerning consents, and the implementation and management of consent processes.

Through a review of existing literature and a series of nine case studies of health information organizations and associations currently involved in HIE, this report can serve as a collection of best practices. The case studies in this report identify various consent options utilized by organizations with existing HIE. The case studies were selected because they present acts and conditions which provide useful lessons and information for organizations engaged in different types of HIE involving varying types of information.

The summary of case studies table at the end of the executive summary can be used to find organizations with similar governance and architecture structures. The table summarizes the findings from the case studies in terms of the governance architecture, consent source and consent type. A more detailed examination of the corresponding case study in this report will describe successful consent strategies that may be useful as states and state designated organizations design their consent policies for the electronic exchange of health information.

**Findings**

HIPAA articulates the national baseline standard for consent as “No Consent” required for treatment, payment and health care operations disclosures, and includes specific Opt-In or Opt-out processes for sensitive health information (i.e., particular conditions, treatments or diagnoses deemed to require additional protections). Some states have placed additional requirements on the disclosure of health information, thereby leaving organizations and providers confused about which laws apply when exchanging health information across state lines.

This report identifies several key findings:

- Many state laws vest greater control of health information in individuals than HIPAA does, especially with respect to sensitive health information. Individuals need to comply with both state and federal laws, which can be difficult to reconcile. The Consents Toolkit will help states and health information organizations (HIOs) identify applicable laws dealing with consent.
• Recipients of health information are only required to follow the consent laws of the place in which they are physically located, including applicable federal and state laws, when using and disclosing information received through HIE. HIOs that wish to require higher standards can incorporate them contractually.

• Reconciling differences in state laws can occur through contract, memorandum of understanding or alignment of state laws.

Recommendations for States, and HIOs, and Providers
There is no single model for HIE consent, and approaches in this area will continue to have to balance the values of administrative efficiency and clinical improvement against patient control and public trust. There are several recommendations for states and HIOs as they develop policies to protect and exchange health information:

• States should develop guidance and standards for intra- and interstate HIE to help organizations best meet the requirements under both federal and state law.

• Based on state analyses and guidance, HIOs should develop clear guidance for providers.

• If sensitive health information is included in HIE, consent processes should be implemented to enforce permission limitations when they are more stringent than HIPAA limitations and must take into consideration existing state and federal laws, such as 42 CFR Part 2. Interstate differences should be specifically discussed and consistent ways of addressing these differences should be established and articulated to all participating entities.

• If highly granular access controls are not available, it may be necessary to exclude transactions involving sensitive health information.

While a uniform nationwide HIE consent model may be adopted at some point, current variations in state and federal law indicate that some variation in consent approaches is probably inevitable and possibly desirable. In the absence of a national uniform solution, consent processes for HIE will have to adapt to variations in law and preferences of the states. Operational strategies based on a process that recognizes the variation in consent laws among states and different processes among HIE models will only help all stakeholders achieve interstate exchange of health information. This report provides a foundation of best practices on such strategies.
# Summary of Case Studies

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Page</th>
<th>Governance</th>
<th>Architecture</th>
<th>Consent Source</th>
<th>Consent Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealthCt.</td>
<td>21</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Opt-In (per encounter)</td>
</tr>
<tr>
<td>CareSpark</td>
<td>25</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Variable (per provider)</td>
</tr>
<tr>
<td>HealthBridge</td>
<td>28</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Variable (per provider)</td>
</tr>
<tr>
<td>1HealthRecord</td>
<td>30</td>
<td>Utility (PHR)</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Directive</td>
</tr>
<tr>
<td>Kaiser Permanente</td>
<td>32</td>
<td>Enterprise</td>
<td>Centralized</td>
<td>Enterprise</td>
<td>Opt-In</td>
</tr>
<tr>
<td>Mayo Clinic</td>
<td>36</td>
<td>Enterprise</td>
<td>Centralized</td>
<td>Enterprise</td>
<td>Opt-In</td>
</tr>
<tr>
<td>SureScripts</td>
<td>41</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider (records)</td>
<td>Plan (MPI) Unknown (per plan)</td>
</tr>
<tr>
<td>Texas Mental Hlth</td>
<td>43</td>
<td>Standard HIO</td>
<td>Centralized</td>
<td>Provider</td>
<td>Opt-In (per 42 CFR Part 2)</td>
</tr>
<tr>
<td>Wellpoint IHR</td>
<td>48</td>
<td>Standard HIO</td>
<td>Centralized</td>
<td>Provider</td>
<td>No Consent (EHR) Opt-In (PHR)</td>
</tr>
</tbody>
</table>
2. INTRODUCTION

The principal objective of this Report is to provide information to help HIE developers, operator and participants, and state agencies and other parties supporting them, to help resolve the issues involving the implementation and management of consents in the following circumstances:

- When HIE occurs between participants in different states that have different consent laws;
- Where HIE may involve information protected under federal alcohol and substance abuse records protection law (42 CFR Part 2), which impose stricter consent requirements; and
- Where HIE may involve information from educational institutions protected under FERPA, which require the application of its own specific consent requirements.

The information in this Report was developed through a set of nine Case Studies of organizations and associations involved in HIE, as well as a review of key previous studies and analyses.

In this Report we will use the term “consent” to mean any process by which an individual is considered by law to have been informed of and agreed to permit another person to use or disclose personal information about the individual. The definition includes a spectrum of processes which can be described in terms of the degree of control vested in individuals.3

For example, at one end of the spectrum an entity might implement a consent process which informs individuals of the ways it will disclose their information in the provisions of a notice of privacy practices, and individuals may only have the right to opt-out of having their information disclosed as described by declining to use the services of the entity publishing the notice.4

---

3 Compare Pritts and Connor, The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands (The Ability to Mask or Limit Access to Health Data) (February 16, 2007) at 1:

This paper uses the term “consent” policies and practices when referring to policies and practices that govern whether and how individuals have the right to control when and how their health information can be shared with others. The term "consent mechanism" is used to refer to the methods by which an individual can exercise such control.

4 This type of consent is sometimes called the “No Consent” rule; see Section 3, infra. It is in fact the legal minimum consent process for disclosures of Protected Health Information (“PHI”) for treatment, payment or health care operations under the HIPAA Privacy Rule. See 45 CFR §§ 164.502(a)(1)(ii) (authorizing use and disclosure for such purposes), .506 (use and disclosure for such purposes may be subject to consent at Covered
the middle of the spectrum would be opt-out or opt-in processes in which individuals have the right to specifically prohibit or permit disclosures by signed request documents, a consent process which is probably the mainstream concept of a “consent,” “authorization” or “release.”

At the maximum control end of the spectrum this definition also include “directives,” documents under which an individual not only permits but directs a person to make a disclosure or use of personal information, which may be used to enable access to information by the individual or other parties at the individual’s discretion. While there may be important differences among the specific processes and documents included under this term, depending on the discussion or the law which applies, for convenience all will be referred to as “consents” in this Report.

This Report is not intended to provide policy recommendations about when and how consents should be used in HIE, or to recommend new laws or regulations. Key legal issues will be discussed to ensure their requirements and application are clear, and some are discussed in depth in reports and white papers cited in the footnotes and in the Bibliography provided in Appendix A. Copies of some relevant documentation from the Case Studies are also included, in Appendix C, while the accompanying Consents Toolkit is intended to provide analytical tools and suggestions for the identification and reconciliation of overlapping laws concerning consents, and the implementation and management of consent processes.

Entity’s option, not otherwise required) and .520(b)(1)(ii)(A) (notice of privacy practices must describe and give examples of permitted uses for treatment, payment and health care operations).

5 The various terms are noted and discussed in Pritts, Lewis, Jacobson, Lucia and Kayne, Privacy and Security Solutions for Interoperable Health Information Exchange, Report on State Law Requirements for Patient Permission to Disclose Health Information (August 2009). Note also that in many discussions “consent” implies greater participation by the consumer in the decision-making process: “Consent implies an active, affirmative agreement of the individual to engage in the activity in question. It also implies that the individual have some understanding of the implications of what is being consented to.” Pricilla Regan, quoted in Connecting for Health Common Framework for Networked Personal Health Information, Consumer Consent to Collections, Uses, and Disclosures of Information (June 2008).

6 Directives in this sense must be distinguished from “consent directives” standard developed by the Health Information Technology Standards Panel, a standard which “describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient’s right to consent.” Health Information Technology Standards Panel, Manage Consent Directives Transaction Package, Version 1.3 (July 8, 2009) at 5.

7 This spectrum may also be characterized as combining individual choice and individual access, in terms of the principles articulated in the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (December 15, 2008).
3. **CONSENT BACKGROUND AND MANAGEMENT**

Individual consent to the use and disclosure is one of the “Fair Information Practices” principles which inform most privacy analyses and many privacy laws.\(^8\) This principle is usually articulated as the concept that “the collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.”\(^9\)

Implementation of this principle, however, requires policies, procedures and technical mechanisms which may vary considerably. For implementation purposes, then, consent may be considered as any type of process through which individuals are given some degree of control over another party’s use and disclosure of personal information about them, though this Report is really only concerned about disclosure.\(^10\) This might include control over content, medium, recipients, time and conditions predicate to disclosure. Consent processes necessarily impose some burden on the parties which have to administer them, and when required by law create potential penalty or damages exposures if not done correctly.

Consent requirements therefore create burdens and disincentives for HIE, which tend to increase in direct proportion to the degree of control vested in individuals. At the same time, consent is essential to ensuring individual choice, which is essential for individual and public trust as electronic HIE expands. Decisions about designing and implementing consent processes always involve reaching an appropriate and functional balance between the need to engender and maintain trust by providing individual control, and the need to maintain efficiency and manage costs by minimizing administration.

Consent requirements can therefore be categorized in terms of a spectrum of individual control rights. At the “low control” ("No Consent") end of this spectrum, individuals may only be given general notice that their information may be disclosed for a stated purpose or purposes, for example in a notice of privacy practices published by their hospital. The notice may or may not

---


\(^10\) HIPAA distinguishes information “use,” meaning “the sharing . . . of . . . information within an entity that maintains such information” from “disclosure,” meaning “the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.” 45 CFR § 160.103 (emphasis added). For purposes of this Report HIE is usually considered the exchange of information between entities, and therefore disclosure.
indicate that the disclosures will be through electronic HIE, and the only way an individual may be able to prevent such disclosure may be by choosing not to receive care there.\textsuperscript{11}

“No Consent” is the default consent standard for the disclosure of Protected Health Information (“PHI”) for the core purposes of treatment, payment and health care operation (“TPO”) under HIPAA.\textsuperscript{12} This standard was adopted after express consideration of consent process benefits and burdens.

The Department heard concerns about significant practical problems that resulted from the consent requirements in the Privacy Rule. Covered entities and others provided numerous examples of obstacles that the consent provisions would pose to timely access to health care. These examples extended to various types of providers and various settings. The most troubling, pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to their initial face-to-face contact with the patient, something which is routinely done today to provide patients with timely access to quality health care.

\ldots

As a result of the large number of treatment-related obstacles raised by various types of health care providers that would have been required to obtain consent, the Department became concerned that individual fixes would be too complex and could possibly overlook important problems. Instead, the Department proposed an approach designed to protect privacy interests by affording patients the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded . . .\textsuperscript{13}

As will be discussed, HIPAA gives individuals greater control over disclosures than “No Consent” for many purposes other than TPO. Individuals also have greater control over alcohol and drug treatment information maintained by alcohol and drug treatment programs (“Programs”). Before a Program can disclose information about one of its patients to anyone, through any medium, the patient must “Opt-In” by the patient’s written authorization, at the patient’s

\textsuperscript{11} Under HIPAA an individual may request additional restrictions on disclosure, but as noted below the hospital would not be required to accept it unless it concerned information about treatment the individual has paid for out-of-pocket.

\textsuperscript{12} The Health Insurance Portability and Accountability Act of 1996, Pub.L. 104-191(August 21, 1996) and its implementing Security Rule, 45 CFR Part 164 Subpart A and C, and Privacy Rule, 45 CFR Part 164, Subparts A and E. This is the HIPAA standard for use and disclosure for these three types of purpose. See 45 CFR §§ 164.502(a)(1)(ii), .506(a) and (c), and .520(b)(ii)(A).

\textsuperscript{13} U.S. Department of Health and Human Services, \textit{Standards for Privacy of Individually Identifiable Health Information; Final Rule}, 67 F.R. 53182 (August 14, 2002) at 53209.
discretion. Finally, at the “high control” end of the spectrum, individuals have the right to copies of the information about them maintained by Covered Entities, and so (for example) a patient may execute a “Directive” require a hospital to provide her with a copy of her medical records.\(^\text{14}\) Consent issues are complicated by the multiple overlapping laws which apply to HIE, especially interstate HIE. Baseline national legal requirements for consents are set by HIPAA, for PHI which includes essentially any information about an individual patient or member maintained by or for a health care provider or health plan.\(^\text{15}\) HIPAA provides a baseline because it preempts any federal or state law which provides less individual control over PHI.

At the same time, most if not all states have statutes, regulations and/or caselaw which create or condition consent rights for state residents for personal health information which overlap HIPAA, and also have laws which single out subcategories of particularly sensitive information – which varies state by state, but often includes HIV/AIDS, alcohol and drug treatment, mental health, genetic information, and the like (“Sensitive Health Information,” or “SHI”) – and provide additional rights and protections. Some states provide greater consent rights for state law-protected information which is PHI under HIPAA, while most (perhaps all) provide it only for specified categories of SHI. Federal law also provides additional consent requirements for alcohol and drug treatment program-related patient information under 42 CFR Part, and there is a parallel process for educational information under FERPA.

Covered Entities are the principal entities required to comply with HIPAA, along with their Business Associates.\(^\text{16}\) Covered Entities are responsible for ensuring that their own disclosures of PHI are permitted under HIPAA, and for obtaining contractual assurances from any Business Associates which obtain or disclose PHI on their behalf only do so as permitted by HIPAA and their Business Associate Contract.\(^\text{17}\) They are not required to implement contracts before disclosing PHI to other Covered Entities (unless the other Covered Entity is acting on behalf of the first, in which case it is a Business Associate\(^\text{18}\) ), but that Covered Entity in turn is responsible for ensuring that its own use and disclosure of the PHI is permitted under HIPAA.

---

\(^{14}\) Under regulations to be promulgated under § 13405(e) of the Health Information Technology for Clinical and Economic Health Act (“HITECH”), Title XIII of the American Recovery and Reinvestment Act, H.R. 1, Pub.L. 111-5 (February 17, 2009), individuals will be entitled to obtain such information in electronic form, and to have it transmitted to a third party of the individual’s choosing.

\(^{15}\) See 45 CFR § 160.103.

\(^{16}\) A “Covered Entity” is a health care provider, health plan (including health insurance companies and other payors) or health care clearinghouse, while a “Business Associate” is any person which obtains, uses or discloses PHI for a function or activity on behalf of a Covered Entity. See 45 CFR § 160.103.

\(^{17}\) See 45 CFR § 164.504(e)(2).

\(^{18}\) See 45 CFR § 160.103.
Alcohol and drug programs will always be health care providers and therefore Covered Entities, and most if not all entities required to comply with state consent laws will be Covered Entities. Some entities may be required to comply with both HIPAA and FERPA, but PHI under HIPAA is specifically defined to exclude information subject to FERPA. FERPA uses a consent scheme parallel to HIPAA, however, so this analysis generally applies to educational institutions under FERPA as if they were Covered Entities under HIPAA.

### 3.1. Consent Issues in Electronic Health Information Exchange

The issue of individuals’ control over the sharing of their information through HIE has been analyzed and debated in many publications, and this Report will not try to review or analyze these arguments. However, some background on electronic HIE models and operational arrangements is necessary to frame consent questions and analyses appropriately.

There are a number of strategies in use and development for electronic HIE within and among organizations, under a set of national public policy initiatives intended to develop a nationwide health information network (“NHIN”). The NHIN is currently envisioned as a “network of networks” allowing for the electronic sharing of health information when and where needed among health care organizations across the nation.

The NHIN is in development incrementally, developing through the implementation of proprietary enterprise and organization networks, and local, regional and state-wide networks for the sharing of health information, and the growing interconnectivity of these networks. These subsidiary networks are sometimes called “subnetwork organizations” (“SNOs”), health information organizations (“HIOs”) including regional HIos (“RHIOs”), or health information exchanges (“HIEs”) (not to be confused with health information exchange, or “HIE,” used to denote an activity as in this Report). For simplicity’s sake this Report will refer to all network organizations as “HIOS.”

---

19 See 45 CFR § 160.103.
22 Cf. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, 1 J. Health & Life Sci. Law 1 (January 2008) at 14:

> . . . the most useful approach may be to consider that HIE is an activity that takes place over electronic communications networks involving use of EHRs and related applications, organized by a state, private entity, or consortium of entities, including those entities necessary to make the HIE activity self-sustaining. The network may be operated by one or more entities, and may be called a RHIO, a RHIN, a SNO, an HIE initiative or organization, or something else; the parties may define their relationships by a “web of contracts.” At the least organized level HIE may simply take place among an informally organized coalition of entities using a public network such as the Internet. However the network is
HIOS may use a variety of governance models, across a spectrum from “closed” to “open” participation.23

- **Enterprise HIO.** An enterprise HIE is typically operated by and principally for a single organization (one or more legally associated entities). This is a relatively “closed” system, typically available only to the enterprise and some of its trading partners.

- **Standard HIO.** A “Standard HIO”24 is based on agreements among a group of entities in a given region or market which have identified business reasons for sharing information, typically because they serve common or overlapping populations. This is the “classic” RHIO model, though governance may be more or less formal. This is a more “open” model than the Enterprise HIO, and is often available on a limited geographic basis (e.g. local or regional), to a limited class of entities (e.g. providers but not plans).

- **Utility HIO.** Some HIEs may use services providers (which might be participating healthcare organizations acting as services providers) to various technical services allowing organizations to exchange information, including network services, but are generally “lighter” and less centralized than Standard HIOs. This is probably the model which has the most potential to be “open,” but is likely to be more or less limited depending on the services provider’s or participants’ preferences.

At another level, there are three basic network architectures for HIE, which may be analyzed on a spectrum from centralized to decentralized.25

---

23 This taxonomy is based on an analysis of the Case Studies in light of previous policy analyses. See esp. University of Massachusetts Medical School Center for Health Policy and Research, National Opinion Research Center (NORC) and National Governors Association Center for Best Practices, *Public Governance Models for a Sustainable Health Information Exchange Industry: A Report to the State Alliance for e-Health* (2009). Note that nomenclature in this area is not settled. See Christiansen, supra note 29, at 8 – 14.

24 This is a term of convenience, and should not be taken to indicate that there is a single structure or arrangement which is “standard” for HIOs. Rather, this is intended to refer to the range of HIOs usually called “RHIOs,” which may be membership-based, agreement-based or mixed. See Christiansen, supra note 29.

25 See Sittig, Shiffman, Leonard, Friedman, Rudolph, Hripcsak, Adams, Kleinman and Kausha, *A Draft Framework for Measuring Progress Towards the Development of a National Health Information Infrastructure*, 5 BMC Medical Informatics and Decision Making 14 (2005) and Rosati and Lamar, *The Quest for Interoperable Electronic Health Records: A Guide to Legal Issues in Establishing Health Information Networks* (July 2005). Another characterization be applicable in this analysis is whether a given architecture supports HIE “push” or “pull,” with “push” indicating a point-to-point electronic HIE more or less modeled on existing paper-based HIE, and “pull” indicating “a shared architecture and supporting services that enable a more sophisticated capacity to search for and extract - or “pull” - electronic data from one or more networked sources using a query system[.]” See Goldstein and Rein, *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis* (March 23, 2010) at 3.
• **Repository Architecture.** A “centralized repository” or “community health record system” is the most centralized architecture, in which data from the various participating organizations is aggregated into a single repository for access by authorized users.

• **Federated Architecture.** Sometimes called “hub-and-spoke,” “data warehouse-silo,” or “federated repository” system, in this architecture different participating organizations store health information on their own and/or others’ behalf in separate repositories each maintain, and make it available to other participants upon request.

• **Pointer Architecture.** A “pointer” or “point-to-point” system is the least centralized architecture, in which network HIE services (such as a master patient index (“MPI”) and/or record locator service (“RLS”)) allow authorized users to identify records stored by the various participants, so that they can directly request the information from the holder.26

There is no necessary correlation between HIO-level governance and HIE architecture, though it seems likely that a Utility HIO would correlate more with the provision of lighter services supporting Pointer Architecture, while an Enterprise HIO may find a Repository Architecture more consistent with the needs and goals of a centralized organization and be able to implement such an approach easier than a loose agreement-based HIO.

Each governance model and architecture may present different issues affecting consent strategies. In a provider-based Pointer Architecture, for example, there may be sufficient trust that the providers will be effective as consent “gatekeepers” who will not disclose information for improper purposes that a minimal consent process is acceptable. Conversely, some individuals might be concerned that a Repository Architecture would be more likely to be subject to legal but untrusted data mining, and HIO policy for such an architecture appropriately let individuals Opt-Out (or Opt-In). Consent questions therefore need to be answered in the context of actual operations and their implications for individual and public trust in electronic HIE.

It is not clear at this point how HIE networks implemented on different architectures and subject to different modes of governance will be able to mesh into a functional NHIN, but consent variations between them seem likely to be a significant barrier. All HIE models present

---

26 Because MPI and RLS information necessarily identifies individuals and associates their identification with health care, they maintain PHI. While this information should be limited to demographic and certain other relatively less sensitive information, its use and disclosure is nonetheless subject to HIPAA and applicable state law compliance. Some type of consent may therefore be desirable or may be necessary. See generally Connecting for Health, *Notification and Consent When Using a Record Locator Service* (2006). For HIE specifications in this area see U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology, *Nationwide Health Information Network (NHIN) Patient Discovery Web Service Interface Specification* V. 1.0 (January 29, 2010) and *Nationwide Health Information Network (NHIN) Query for Documents Web Service Interface Specification* V. 2.0 (January 29, 2010).
the problem of communicating information use and disclosure limitations which might have been established by the individual from the information source to downstream recipients, and binding recipients to those limitations. Inter-network HIE may present significant issues in this area, in the absence of common standards for communication of consent limitations and transfer of legal obligations.

The former might be resolved by development of standards for “Consent Metadata,” i.e., information which accompanies HIE transactions which communicates any limitations on purposes for which the information may be used or disclosed, specifically permitted or prohibited recipients (or classes of recipients), expiration date if applicable, and so on. Standards for this sort of communication should be relatively straightforward to develop, and could be adopted voluntarily (or mandated by law if sufficiently supported).

However, in the absence of applicable law the receipt of Consent Metadata would not bind recipients to the limitations it included. Most states do not have such laws, and currently, only 42 CFR Part 2’s information redisclosure provisions (discussed below) provide for the communication of Consent Metadata and make it binding on recipients by law. In the absence of such a law, recipients of communications stating limitations on the use or disclosure of the information they contain are bound only if they agree to the limitations. Where information is transferred and there is no agreement the receiving party is bound only by whatever laws control its use and disclosure of information received, which may not be consistent with the consent limitations established by the disclosing party.

Some mechanism for agreement therefore needs to be in place to transfer the obligation to comply with limitations included in Consent Metadata for most HIE. The obligation to comply with consent limitations is always required under Business Associate Contracts for disclosures from Covered Entities to Business Associates under HIPAA, and under “qualified services organization agreements” (“QSOAs”) by Programs subject to 42 CFR Part 2 (see below). It can

27 Compare the HITSP Manage Consent Directives Transaction Package, supra note 13, which provides electronic transaction specifications for such information.

28 But see California Civil Code 56.13, restricting disclosure by parties receiving medical information disclosed by authorization or under other specified conditions. While this provision does not specify that the receiving party must receive notice of the limitations, as a practical and perhaps due process matter enforcement of such limitations would require some kind of notice.

29 This means, for example, that many of the standard statements about confidentiality included in email are not binding on most recipients.

30 A Covered Entity may, but is generally not required to accept an individual’s request for restrictions on use and disclosure of PHI which are in addition to those otherwise provided by HIPAA. See 45 CFR § 164.522. A Covered Entity which accepted such a restriction would be required to pass it along to any Business Associate by Business Associate Contract, but it is not clear if it would be binding upon another Covered Entity which received it without an agreement to be bound. It seems unlikely a Covered Entity would be held bound by a restriction if it had not notice of it, but it might be held bound by a restriction if it were notified.
also be done optionally under HIO agreements, or other forms of HIE agreement such as the NHIN Data Use and Reciprocal Support Agreement (“DURSA”).

Another alternative is electronic contracting, for example where a recipient is only given access to information if the recipient “clicks to accept” limitations in Consent Metadata. This can be done to bind participants to long-term HIE contracts, or could be done on a per-transaction basis when information is requested, binding the recipient only with respect to the information in the specific transaction. Either way, an electronic contracting strategy requires sound authentication processes to ensure that any party executing the agreement is who they claim to be.

Where no agreement is made, or as a limitation control in addition to an agreement, where feasible Consent Metadata limitations may be enforceable by technical mechanisms such as the segregation and masking of information, especially SHI. In this context, “masking” means “coding data in such a way that access to or transfer of the data is restricted.”

Masking solutions include access controls allowing access only to specified users or organizations, pre-set access period limitations, anonymization of information by substituting “shared secret” information for standard identifiers, and encryption with encryption keys subject to controlled distribution. Masking solutions may need to be implemented at the level

---

31 NHIN Cooperative DURSA Team, Data Use and Reciprocal Support Agreement (DURSA) for NHIN Limited Production Pilot Activities (October 21, 2009).

32 “Click to accept” or “clickwrap” contracts are established when one party offers to provide something of value to another in an online transaction in which the second party has to take some action (such as “clicking” a button on the screen) to accept the conditions under which it is offered. This is a well-established basis for electronic commerce based on the federal Electronic Signatures in Global and National Commerce Act (“E-SIGN”) and the Uniform Electronic Transactions Act (“UETA”) which has been adopted in almost all the states (see below). The courts consistently uphold clickwrap contracts as long as the party accepting them has reasonable notice and an opportunity to read the terms before executing the “click.” See Moringiello and Reynolds, Electronic Contracting Cases 2008–2009, 65 Bus. Law 317 (2009); Moringiello and Reynolds, Survey of the Law of Cyberspace: Electronic Contracting Cases 2007–2008, 64 Bus. Law 199 (2008); Moringiello and Reynolds, Survey of the Law of Cyberspace: Electronic Contracting Cases 2006–2007, 63 Bus. Law 219 (2007); Moringiello and Reynolds, Survey of the Law of Cyberspace: Electronic Contracting Cases 2005–2006, 62 Bus. Law 195 (2006); and Moringiello and Reynolds, Survey of the Law of Cyberspace: Internet Contracting Cases 2004–2005, 61 Bus. Law 433 (2005).

33 This was the strategy of the contract form developed by the HealthKey Collaborative, Template for a Comprehensive Health Care Information Protection Agreement Between Business Associates (September 2001), which allowed HIE participants to “opt-in” to a contractual relationship with other parties wishing to participate in HIE by electronic signature to an online contract.

34 See Section 3.3.2, below.


of the data source ("gatekeeper" in this Report), database (repository) or HIE service (MPI or RLS), depending on the HIE architecture.

Technical mechanisms for consent enforcement in the NHIN are in development, including national HIE transaction specifications for communicating consent information between HIE "nodes." In order to be effective, however, mechanisms of this type will need to be able to communicate Consent Metadata accurately and consistently both within HIOs whose participants may be in different states or otherwise subject to different consent requirements (e.g. under 42 CFR Part 2), and between HIOs which may have decided to implement different consent standards for given types of disclosure.

3.2. Types of Consent

There are a number of ways to categorize consents, depending on the purpose of the analysis. The most frequently used categories include:

- By the type of entity required to obtain a consent, such as a Covered Entity under HIPAA, or by regulated entity like the educational institutions subject to FERPA.
- By the type of information the consent applies to, such as the alcohol and drug abuse records subject to 42 CFR Part 2.
- By the type of use or disclosure of information permitted under the consent, such as a HIPAA authorization to use PHI for research purposes.
- By duration of the consent.
- By the degree of individual control the consent process actually vests in individuals.

In practice these categories almost always interact. Laws usually define both the information subject to consent requirements and the persons required to comply. They also often (but not always) define purposes for which protected information may be used, with or without consent, and may vest greater or lesser control in individuals. Some types of information,

37 Pritts and Connor, supra note 10, at 4.


39 See Goldstein and Rein, Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis (March 23, 2010), defining consent categories by “granularity” including data type, provider type, time range and purpose. Because HIE participation is not necessarily limited to health care providers – it may include payors, public health agencies, services providers and consumers where appropriate, in particular – we would suggest not limiting the regulated entity category to providers.

40 See Goldstein and Rein, supra note 46.
particularly personal information defined by law or otherwise considered relatively more sensitive, may be subject to a greater degree of individual control.

Concern about variability in the authority to disclose protected information from one HIE participant to another, and the authority of recipients to use it, has been consistently identified as an obstacle to HIE. Since this authority is based on (or limited or conditioned by) applicable law, the practical questions in any given HIE transaction are:

- Whether applicable law permits the disclosure and use of the protected information without a consent;
- If not (or if the HIE participants have agreed to a consent standard not required by law), whether a consent process meeting applicable requirements was followed with respect to the information involved.

The latter in turn is a function of compliance with any notice and documentation requirements, and any individual action required to make the consent effective. Categorization in terms of individual control often uses the following five consent models:41

- No Consent.
- Opt-out.
- Opt-out with exceptions.
- Opt-in.
- Opt-in with restrictions.

A recent nationwide survey of HIEs indicated that out of 199 respondents, 36 had implemented policies requiring Opt-In for sharing of information, 81 had implemented Opt-out, 27 were not sure of their policies and the balance did not answer.42

We also note that under HIPAA and many states’ laws individuals have the right to obtain copies of their personal information from at least some entities which possess it.43 New federal law under the Health Information for Economic and Clinical Health Act (“HITECH”)44 will also require healthcare organizations to make PHI available to individual data subjects in electronic form upon request, including direct transmission of a copy to any person designated by the

---

41 Id. See also Health Information Security and Privacy Collaboration (“HISPC”), Intrastate and Interstate Consent Policy Options Collaborative Final Report, supra note 2.
43 See e.g. HIPAA, 45 CFR § 164.524, Access of Individuals to Protected Health Information.
individual. In one case study, the 1HealthRecord personal health record (“PHR”), this kind of request is already being used by patients to authorize and direct their physicians to transfer electronic copies of their information to the patients PHRs. This kind of directive may play an important role in enabling consumer participation in HIE, and so we also suggest adding “Directives” as a form of consent. We note that there are also a very few categories in which no directive may apply.

The consent types are summarized in Table 1.

<table>
<thead>
<tr>
<th>Type of Consent</th>
<th>Comments and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Consent</td>
<td>Some notice to individual of disclosures</td>
</tr>
<tr>
<td></td>
<td>HIPAA Treatment, Payment, Health Care Operations (“TPO”)</td>
</tr>
<tr>
<td>Opt-Out</td>
<td>Notice to individual and opportunity to prohibit disclosure</td>
</tr>
<tr>
<td></td>
<td>HIPAA marketing</td>
</tr>
<tr>
<td>Opt-In</td>
<td>Notice to individual and authorization by individual</td>
</tr>
<tr>
<td></td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>42 CFR Part 2</td>
</tr>
<tr>
<td>Directive</td>
<td>Organization is required to disclose information as</td>
</tr>
<tr>
<td></td>
<td>directed by individual</td>
</tr>
<tr>
<td></td>
<td>HITECH electronic health records</td>
</tr>
<tr>
<td>No Directive Permitted</td>
<td>Individual may not direct organization to disclose</td>
</tr>
<tr>
<td></td>
<td>information under any conditions</td>
</tr>
<tr>
<td></td>
<td>HIPAA psychotherapy notes</td>
</tr>
</tbody>
</table>

### 3.3. HISPC Consent Recommendations

The Health Information Security and Privacy Collaboration (“HISPC”) was a four-year series of projects studying state laws, as well as legal interpretations, policies and practices which were

---

obstacles to HIE, and identifying possible solutions. Consent issues were identified early in the process as significant obstacles in most states. Possible solutions to this problem included development of uniform or model forms, “segmentation of data” so that information subject to special legal protections is presumptively not included in HIE, and implementation of technical mechanisms to “capture, share and implement patient consent.”

Phase III of the HISPC established collaboratives of representatives from various states working together to identify solutions in areas ranging from standards adoption to education to consents to legal issue evaluation. Several states were involved in two separate consent collaborative projects.

The mission of the first collaborative, the Intrastate and Interstate Consent Policy Options Collaborative (“Consent Options Collaborative”), was to examine the relative utility of select legal mechanisms that states may enact to facilitate interstate HIE and examine a variety of consent policy alternatives, to develop tools and resources that states and health care stakeholders could use to determine the degree of choice consumers should have about the electronic access to and use and disclosure of their health information. The Consent Requirements Collaborative therefore identified and evaluated various factors that affect the balance between consumer privacy interests and affordable provider access to reliable health information through HIE.

The second consent collaborative, the Interstate Disclosure and Patient Consent Requirements Collaborative (“Consent Requirements Collaborative”), had the mission of providing actionable findings to assist in removing legal barriers or assist in developing solutions to address legal environment differences to expand the use of interstate HIE, based upon detailed statutory and regulatory requirements related to patient consent/authorization. This included development of a model for identifying PHI disclosure and patient consent requirements across states and related analytical tools to use in comparing differing state legal environments.

The findings and analyses in the reports from these collaboratives provide valuable insights and tools for addressing consent issues in interstate and intrastate HIE.

Findings of the Consent Options Collaborative

---

46 See HISPC, Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions (July 2007) at 3-1, 3-20.

47 Id. at 5 - 5

48 Id. at 5 – 20.

49 Id. at 5 – 21.

50 See HISPC, Intrastate and Interstate Consent Policy Options Collaborative Final Report, supra note 2.

51 Id.
This collaborative involved several states but the two key states involved in the development of a consent model were North Carolina and California. As likely could have been expected, each state followed different approaches to develop a common consent model that it was considered could be used on an intra and interstate basis. This Collaborative worked with the five basic consent models described above, on a spectrum from No Consent to Opt In. For example, under the No Consent model PHI would be shared across an HIE and the individual would not be give the choice to opt in or out, while Opt In would require the individual to actively authorize the sharing through HIE.

The Collaborative evaluated several different scenarios ranging from the exchange of PHI that is not specially protected, PHI that is specially protected and PHI exchange in an emergent situation and related scenarios. Different consent models were generally associated with differing data exchanges, primarily as it related to non-emergent versus emergent care settings and whether or not specially protected health information was part of a patient’s medical record and would be shared. Ultimately, the Collaborative did not identify a single consent model that all participants considered acceptable across all scenarios.

Regarding interstate exchange of PHI, the Collaborative developed tools that could be used by states to evaluate acceptable consent practices related specifically to both individual state privacy laws and federal privacy laws other than HIPAA. The tool set created was comprehensive and relatively easy to use. No common approach to interstate PHI exchange or method (interstate compact, uniform law, etc.) was clearly identified by the group. Rather, the group evaluated the pros and cons to each approach.

**Findings of the Consent Requirements Collaborative**

One of the significant but not surprising findings of this Collaborative was the variability across states regarding when consent is and is not required. States considered ranged from Indiana, where consent is rarely if ever required pursuant to state law, to New York where consent is generally required for all health care treatment pursuant to state law. The Collaborative also documented significant variability within states in different legal interpretations and different professional practices, and confusion about what privacy requirements are.

These conditions apply whether the information exchange is paper based, point-to-point, or via a centrally managed network. However, the use of a centrally managed network appeared to increase confusion due to issues around control of HIE, as opposed to point-to-point HIE where there is little or no central authority over the exchange.

The Collaborative also found considerable variability regarding what were required elements that needed to be included as part of a consent or authorization form (paper or electronic). Some states were very specific regarding requirements, while others did not define documentation requirements. The Collaborative did discover, though, that many of the elements that were required, even pursuant to more stringent state statutes, were similar.
The Collaborative also found that what constitutes specially protected health information was relatively consistent across state lines. For example, common types of specially protected health information included mental health information and HIV/AIDS information. State laws varied in specific definitions, conditions to data exchange and other details, but just as the elements needed to be included as part of a consent form were broadly similar, most of the categories of specially protected health information were broadly the same from state to state.

4. THE CASE STUDIES

The following case studies are intended to describe the consent practices actually being used by a set of nine organizations. This is not intended to be a representative or comprehensive sample, but as a review of key factors and description of real-world processes used to manage consents. The case studies were selected principally because they present facts and conditions which appeared likely to provide useful lessons and information, from organizations engaged in different types of HIE involving different types of information and transactions.

4.1. Case Study Methodology

The case studies are based on interviews with one or more key individuals from the organizations which are the subject of the study, and additional materials where available and relevant. Interviews were conducted using the questionnaire based on the ONC-funded white paper Consumer Consent Options For Electronic Health Information Exchange: Policy Considerations and Analysis,52 as well as open-ended questions and discussion. The questionnaire provided a valuable starting point, but future analyses might benefit from additional questions about broader issues affecting consent, such as the effects of the HIE model (repository vs. point-to-point, etc.) and HIO governance mechanisms.

This Report does not purport to provide a rigorous analysis of the advantages and disadvantages of the consent strategies used in the case studies. The sample selected is not large enough for rigorous analysis, but we believe it is large enough to provide useful information and insights which may be applied to other HIE situations. Since no two HIE arrangements are alike and the field is rapidly evolving it is not clear an attempt at highly rigorous analysis would be either possible or useful. Rather, we have tried to provide the kind of descriptive and legal context information which will support different users in the development of consent strategies for many different types of HIE.

While more detailed information is provided in the narrative discussion of each case, Table 3 summarizes the findings in terms of each case’s governance, architecture, consent source and consent type.

52 See Goldstein and Rein, supra note 30. A copy of the questionnaire is provided in Appendix B.
### Table 2: Summary of Case Studies

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Governance</th>
<th>Architecture</th>
<th>Consent Source</th>
<th>Consent Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealthCt.</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Opt-In (per encounter)</td>
</tr>
<tr>
<td>CareSpark</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Variable (per provider)</td>
</tr>
<tr>
<td>HealthBridge</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Variable (per provider)</td>
</tr>
<tr>
<td>1HealthRecord</td>
<td>Utility (PHR)</td>
<td>Point-to-Point</td>
<td>Provider</td>
<td>Directive</td>
</tr>
<tr>
<td>Kaiser Permanente</td>
<td>Enterprise</td>
<td>Centralized</td>
<td>Enterprise</td>
<td>Opt-In</td>
</tr>
<tr>
<td>Mayo Clinic</td>
<td>Enterprise</td>
<td>Centralized</td>
<td>Enterprise</td>
<td>Opt-In</td>
</tr>
<tr>
<td>SureScripts</td>
<td>Utility</td>
<td>Point-to-Point</td>
<td>Provider (records)</td>
<td>Variable (per provider)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Plan (MPI)</td>
<td>Unknown (per plan)</td>
</tr>
<tr>
<td>Texas Mental Hlth</td>
<td>Standard HIO</td>
<td>Centralized</td>
<td>Provider</td>
<td>Opt-In (per 42 CFR Part 2)</td>
</tr>
<tr>
<td>Wellpoint IHR</td>
<td>Standard HIO</td>
<td>Centralized</td>
<td>Provider</td>
<td>No Consent (EHR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Opt-In (PHR)</td>
</tr>
</tbody>
</table>

### 4.2. Review of Cases

#### 4.2.1. eHealthConnecticut

**Governance:** Utility (Regional)  
**Architecture:** Point-to-Point  
**Consent Source:** Provider
Consent Type: Opt-In (per encounter)

eHealth Connecticut was established several years ago but until recently was not active and not a significant participant in Connecticut HIE planning activities. The non-profit is now partnering with the state Medicaid agency to assist in developing a Medicaid HIE for the state which is funded through a Medicaid transformation grant. The most significant barrier eHealth Connecticut has encountered is not the lack of tools or HIT but finding willing participants in the healthcare community and the lack of broader based funding to expand HIE efforts across the state.

The non-profit intends to address interstate HIE but, at this point in time, efforts are still concentrated on the expanded use of HIE on an intrastate basis. eHealth Connecticut is an entity not dissimilar to others across the US. There is a need build a solid intrastate HIE infrastructure before any real attention is focused on interstate HIE.

An ad hoc group headed up by Hartford Medical Center contracted with Micsys to develop an open source solution for the state. This ad hoc group will likely be a significant player as the Transforming Healthcare for Connecticut project moves forward. The group has partnered with eHealth Connecticut but governance problems still persist. The state and eHealth Connecticut has agreed to move forward with the Micsys solution nonetheless. At this time Hartford Medical Center is rolling out Micsys solution and a subset for the Connecticut Department of Human Services (Medicaid only).

Much of the current activity is being driven by the HIT regional extension center project. The state designated eHealth Connecticut as the state’s HIT regional extension center. Funding for the center was initially allocated to the Connecticut Department of Public Health and will be transferred to eHealth Connecticut, the newly designated HIT regional extension center lead. The state legislative assembly approved the allocation of HIE dollars and the governance structure with eHealth Connecticut as the HIT lead entity also.

Several healthcare organizations assisted the legislature in crafting the final HIT/HIE legislation. The oversight body is now designated as a quasi-public entity. Currently HIT/HIE project management is transitioning from the state public health agency to the newly formed entity. Full transition will not be complete until December 31, 2010.

It is unknown at this time if the HIT/HIE quasi-public entity will have a specifically designated technical workgroup or sub-organization. eHealth Connecticut is moving forward with the intent of being viewed as the HIT technical lead for Connecticut. As stated earlier, there are still problematic governance issues. Also, there remain multiple players vying for position as state HIE/HIT leaders. Two HIEs have been established within the state but neither exchange data across state lines. Middlesex was awarded a Beacon Grant to assist with expanded community level HIE/HIT and will likely contribute to the state HIE/HIT strategic plan and implementation efforts.

22
At this time most data exchanges are point-to-point with expanded HIT/HIE still in the planning phases. It is safe to say that the state is experiencing some of what amount to the initial growing pains of planning for and implementing this state-wide initiative. Again, little thought has been given to interstate HIE at this point in time.

**Geographic Coverage for Sharing PHI**
Currently HIE efforts are primarily in more urban areas. Specifically Hartford, Danbury and Middletown are actively involved in HIE efforts.

**Breadth and Scope for Sharing PHI**
The scope and breadth of health data sharing is narrow. The key areas being served at this time are predominately urban and are served by primarily private entities. The State of Connecticut has yet to enter into the HIE space in any significant way.

**Nature of Consent Process**
At this time all patients are asked to consent to the sharing of their health information, whether it is classified as specially protected health information or not. Also, consent occurs at each encounter versus a single request for patient consent for data sharing by any given provider. Individual providers request consent at each encounter which eHealth Connecticut believes to be administratively burdensome and is not necessarily conducive to the expansion of HIE in the state.

**Duration of Consent**
Consents are given to patients to sign at each encounter. At this point, this continues to be a barrier to meaningful HIE. If the state can move away from requiring consent at every encounter, the duration of the consent will likely be one year.

**Form of Agreement**
Currently there is no standard form of agreement. The state is pursuing the use of the Data DURSA that was developed as part of the HITSP project. Also, other agreements primarily follow the predominantly point-to-point model – the use of trading partner agreements and business associate contracts.

**Educational Efforts**
Currently most provider education regarding HIE comes through provider associations. Payer education has primarily been a part of the payer oversight/regulatory process. Current patient educational efforts have been primarily one-on-one and limited. Public health educational efforts have been primarily as part of the legislative process and through stakeholder meetings.

**Administrative Burdens/Stakeholder Challenges**
Given the lack of any meaningful HIE activity outside a few urban areas, most HIE continues to be point-to-point. The data is not available to generally share and this will likely continue to be
the case until governance issues have been addressed, the transition of the HIT/HIE project is completed and “meaningful use,” now that the rule is final, is more broadly adopted and instances of interoperable EHRs are more prevalent.

Provider trust continues to be an issue. This was found to be a multi-state or national issue during the Health Information Security and Privacy Collaborative (HISPC) project, Phase I. Providers have trust issues with other providers unless it is an emergent situation. To clarify, in Connecticut the primary trust issues exist at the individual provider and specialist level.

At this time consumer/patient involvement has not been very broad and it also represents a barrier to HIE. As is the case in a number of states, consumer advocates are visible and vocal but there is minimal involvement from consumers in general. Also, there has been minimal public education of consumers regarding HIE and the implications.

Quality of Care Challenges

Until such time as data is more widely shared in the form of what amounts to network versus point-to-point sharing, continuity of care will continue to be an issue. It is difficult currently for multiple providers of health care for a single patient to collaborate and provide what would qualify as higher quality and lower cost health care. Also, the national issue of how to treat patients who find themselves in emergency rooms without endangering the patient because of unknown conditions or prescribed substances will continue.

The state’s HIE project is in its infancy and quality of care will not be improved absent both technical and cultural changes. The expanded use of standardized methods of data exchange and use of standardized applications along with addressing provider trust issues will be key to increasing the quality of care in Connecticut. Also, given the state’s close proximity to New York City as well as other states, interstate HIE exchange will prove to be a significant barrier to an exchange resulting in quality of care and it will likely not be addressed in the short run.

Changes to Workflows

At this point in time there are no significant changes to workflows. That will likely not occur until the state HIE project has further matured and outstanding governance issues addressed.

Financial Incentives

Currently the primary financial incentives are HIT/HIE state stimulus dollars, the Medicaid HIE Medicaid transformation grant, HIE extension center funding and the limited private funding from such entities as Hartford Medical.

Currently there are a number of participants or stakeholders ranging from health care delivery systems to health plans to vendors to the state but there has been a lack of financial commitment on the part of most participants. This is a barrier to sustainable HIE following the expenditure of federal stimulus dollars.

Summary
eHealth Connecticut is the lead entity for Connecticut’s HIE extension center and involved in the state approved HIT/HIE project. At this time the issue of interstate HIE has not been addressed and will likely not be addressed until HIT/HIE is more mature within the state. Initially the primary organizations involved in Connecticut’s HIE efforts were private. State involvement is recent. At this point governance issues and a transition of HIT/HIE efforts from a state agency to a legislatively created quasi-public entity have delayed any HIE expansion within the state. eHealth Connecticut represents an example of an intrastate entity that is actively involved in state-level HIT/HIE efforts that are still in their infancy.

4.2.2. CareSpark

**Governance:** Utility (Regional)

**Architecture:** Point-to-Point

**Consent Source:** Provider

**Consent Type:** Variable – No Consent to Opt-In at Provider Election

CareSpark is a nonprofit Regional Health Information Organization (RHIO) established in 2005 to improve healthcare services in northeast Tennessee and southwest Virginia. Its primary focus is on healthcare providers serving a largely rural patient population. Its establishment followed two years of research and planning to explore ways to share health information securely, efficiently and cost-effectively.

The initiative grew out of the Community Health Improvement Partnership (CHIP), which had been working together for more than a decade through the local non-profit citizen organization Kingsport Tomorrow. This organization was one of nine communities awarded a grant for seed funding by the Foundation for eHealth Initiatives, which was financed by Health Resources and Services Administration (“HRSA”) within the U.S. Department of Health and Human Services. A $100,000 grant awarded in July 2004 was matched by about $500,000 from local organizations and their partners, allowing the group to conduct a thorough feasibility and planning process from August 2004 - April 2005.

Consulting partners assisted the 80 volunteers who were actively engaged throughout the planning process. The partners included: HealthAlliant, Inc. (fundraising and strategic business planning); Manatt, Phelps and Phillips (legal and regulatory guidance); CareScience / QuoVadx (technical inventory and technology planning); and n tara (branding and marketing). The CareSpark planning process has been recognized nationally as a model for its broad-based coalition, multi-state region, long-range and comprehensive scope, and development of a sustainable financial model.

CareSpark’s mission was defined based on the local healthcare market, taking into account referral patterns in tertiary care facilities, such as trauma and specialty care facilities, and integrated delivery networks. CareSpark’s model is based heavily on provider support and
involvement in crafting the system. According to CareSpark executives this has been successful, in part, because patients in the service area have relatively high levels of trust in their physicians.

The providers drive decisions on the types of PHI that will be shared. The core document for information sharing is a continuity of care ("CCR") document that contains data on medication, allergies, diagnoses, radiology results and lab results. The disclosing provider decides what information to include on the CCR document.

Providers may access CareSpark’s system directly. If they do not have compatible software, they may access the system through a web portal. CareSpark’s custom system, which offers this kind of granularity, was expensive. It estimated that it cost $100,000 to develop. Off-the-shelf (OTS) software was not an option. CareSpark also expressed doubts that its software system could easily be adopted by other HIEs due to custom-nature of the product.

42 CFR Part 2 and FERPA are not addressed. However, behavioral health data may be shared incidentally due to the inclusion of prescription data in records from primary care providers.

Patients provide consent for sharing their PHI through their providers. Different providers may use different consent strategies. Depending on the provider, patients may passively consent based on notice and an election not to opt-out, or actively provide consent by opting-in. Patients generally may opt out or place other restrictions after consulting with their providers. Patients may also restrict the sharing of information among providers. The only exception to the sharing of information is that the CareSpark cannot discriminate among providers within a single practice group.

Participation by providers and patients is free. The costs are paid by state and federal grants, contributions and contracts with insurers and government agencies. Support for the organization include public health agencies, employers, payers, hospitals, physician practices, universities, community nonprofits, patient advocacy groups, and technology companies.

The RHIO has received approximately $5 million through June 2009 from the federal government to participate in the National Health Information Network (NHIN).

CareSpark attributed its success to staff people who were very familiar with health information management ("HIM") issues, procedures and mechanism. The substantial participation of relevant staff in the American Health Information Management Association ("AHIMA") was credited for providing such education and identifying trends and gray areas.

CareSpark also noted that technology-savvy legal advisors and good technical support professionals were very helpful. It noted a general need for ensuring that legal professionals were well-versed in electronic exchange issues.

**Geographic Coverage**

CareSpark serves northeast Tennessee and southwest Virginia, including 25 counties. Approximately 49 provider organizations of various sizes are participating.
Breadth of Purpose for Sharing PHI

CareSpark’s HIE mission is to support the regional medical market based on referral patterns in tertiary care facility and integrated delivery networks.

Its core document is a CCR document which can include data on medication, allergies, diagnoses, radiology results and lab results. Under this HIO’s model, the disclosing provider decides what information to include in the CCR document.

CareSpark explained it can share other types of PHI electronically if the providers wish to share it. The program does not yet include behavioral health information except for incidental inclusion of prescription data that may indicate issues in that area. The prescription data is typically included at the option of primary care physicians.

A few behavior health organizations have expressed interest in participating, but there is no program in place yet. One behavior health provider is provider is providing the name of the treatment provider and demographic information to help identify patients.

Because the system focuses on the provider, CareSpark reported few issues in reaching agreement on the range of PHI to be shared. The RHIO noted, however, that there have been some provider concerns over sharing lab results because of the laws and regulation that may apply to that information.

Another area of concern among providers was the use of the last four digits of a patient’s Social Security number.

Patient Population

The patient population is largely rural. The program reported little reluctance to participate from patients. CareSpark observed that patients typically view providers as trusted professionals. The RHIO also noted that patients tended to have long-term relationships with providers in the area.

Nature of Consent Process

CareSpark has adopted a flexible, provider-based approach to consent.

A survey in 2006 by the RHIO found that patients overwhelmingly wanted to conduct any consent transaction in their doctors’ offices. This was consistent with expressed provider desires to be responsible for obtaining consent.

Some providers felt it was necessary to have patients to sign a form granting permission for sharing data electronically. Other providers were comfortable with placing a notice in their HIPAA Notice of Privacy Practices. CareSpark therefore adopted a system that would accommodate these different approaches, including the following:

- Active enrollment by a consent which can be either opt-in or opt-out
State and Federal Consent Laws Affecting
Interstate Health Information Exchange
2011

- Passive enrollment, with no consent process but notice given in the provider’s Notice of Privacy Practices.
- Disenrollment at the patient’s option, whichever process for enrollment was used.

Providers have two ways for checking or managing a patient’s consent preferences.
- If the provider’s information system is compatible with CareSpark, it can access the information from CareSpark’s dedication network.
- If the provider’s information system is not compatible, it can log-in from an online portal to manage a patient’s consent options.

Patients can limit which providers may receive their information. However, the consent management system is not sufficiently granular to allow one provider access and reject another if both are in the same provider organization.

Consent is obtained once for use in CareSpark’s network. The duration of consent depends on the provider and how often he or she wants to ask. Patients also may limit the duration of consent. The typical period is one year.

The use of the information is primarily for treatment. CareSpark does allow other uses. The organization said it allows the following uses and disclosures:
- Patient: view content of records, view access log
- Provider: payment, treatment, operations
- Public health: required reporting and authorized queries
- Payers: de-identified aggregate data
- Research: IRB-approved studies

4.2.3. HealthBridge

Governance: Utility (Regional)
Architecture: Point-to-Point
Consent Source: Provider
Consent Type: Variable – No Consent to Opt-In at Provider Election

HealthBridge is a HIE organization based in Cincinnati, Ohio which serves a tri-state area including portions of Ohio, Indiana and Kentucky. It also provides links to the SureScripts network and to other HIEs in its three-state area, and other connections are in development. It is financially self-sustaining, but does receive grant funding from federal and some other sources on a project basis. HealthBridge is a regional extension center (“REC”) under HITECH.
HealthBridge was established in 1997, making it one of the oldest HIEs in operation. It is a nonprofit corporation, and serves some 32 hospitals, and over 800 physician practices including over 5,600 physicians. The patient population served is approximately 2.5 million, in Greater Cincinnati and surrounding rural areas.

HealthBridge does not serve payers, though some are involved in governance. It only serves public health agencies on a limited basis, including a contract to provide antiviral prescription monitoring for H1N1 based on pharmacy consent. HealthBridge maintains only very limited storage of PHI, but principally enables point-to-point transactions.

Some participating organizations do maintain repositories which may be information sources. HealthBridge estimates that 97% of transactions concern patient care. The balance are for public health and some research activities.

Behavioral health providers do not currently participate, so 42 CFR Part 2-protected information is not intentionally included in HIE. Some information relevant to behavioral health may be included incidentally in prescription transactions.

For consent (and most other privacy compliance purposes) HealthBridge is able to “operate in a HIPAA bubble.” The state laws of Ohio, Indiana and Kentucky do not preempt or interfere with HIE under HIPAA requirements, except that Ohio does have a problematic e-prescribing law.

Consent processes are delegated to the participating providers. HealthBridge treats the provider-patient relationship as “sacrosanct,” and will not interact with patients unless required by law, though it is able to provide electronic PHI to patients to support providers’ compliance with HITECH. HealthBridge does not provide an opt-out mechanism for patients.

Providers determine what information they will send in HIE, so they are also the data “filter.” HealthBridge HIE includes most types of clinical documentation which can be made available in electronic form, though a CCD and some e-prescribing transactions are still in a pilot phase.

The consent burden does not generally appear to be very great for providers or patients, except for the considerable burden on providers to change workflow to accommodate HIE in general. Burdens are somewhat greater for public health agencies.

HealthBridge engages in considerable outreach in various media and through various channels. In particular it maintains a specialized communications network for participating providers, and participants are represented on its board.

**Geographic Coverage**

Greater Cincinnati region, including metropolitan and rural areas in Ohio, Indiana and Kentucky.

**Breadth of Purpose for Sharing PHI**

Treatment, as determined by provider sending information.

**Patient Population**
General population.

**Nature of Consent Process**
Provider-administered.

### 4.2.4. Inland Northwest Health Services 1HealthRecord

<table>
<thead>
<tr>
<th>Governance</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>Consent Source</td>
<td>Provider</td>
</tr>
<tr>
<td>Consent Type</td>
<td>Directive</td>
</tr>
</tbody>
</table>

Inland Northwest Health Services ("INHS") is a health care services provider based in Spokane, Washington. Its Information Resources Management (IRM) division provides network and application services, including electronic medical records, to hospitals and physician practices throughout the Western United States. INHS is the lead organization in the Beacon Community of the Inland Northwest (BCIN), a project intended to increase health information exchange and use of information technology in eastern Washington and northern Idaho which is expected to involve twenty-five hospitals, eighteen federally-qualified health centers and more than 3,200 physicians, as well as pharmacies and long term care agencies across the region.

INHS is also one of three pilot sites in Washington State Health Care Authority’s health record bank project, under the oversight of the AccesMyHealth.org Board which includes consumers, physicians, Health Care Authority staff and other community members. A health record bank (HRB) is intended to be a consumer-managed information repository ("account") into which a consumer’s health information can be deposited and withdrawn as needed, under consumer control.

The INHS project, 1HealthRecord, uses the online GoogleHealth personal health record (PHR) as the account repository. Pilot providers including Heart Clinics Northwest, Physicians Clinic of Spokane and Rockwood Clinic have agreed to transfer patient information from their electronic health records (EHR) systems to patient accounts as and when directed by the patient. INHS provides the transfer service and processes the information so it will be accessible to the patient in his or her GoogleHealth account.

The pilot currently serves the Spokane metropolitan area, and will be expanded in response to provider and patient demand in the eastern Washington/northern Idaho region. The currently participating providers are physician practices ranging from about ten to about 200 physicians. There are about 320 patients participating for whom information is actually flowing, in the general patient population.
Because the HRB is intended to be consumer-controlled, once information has been transferred to the HRB the patient can do whatever he or she wants with it. So far, the only data available is medication and allergy lists, but there are current plans to add problem lists and simplified lab results such as cholesterol and blood pressure.

Providers are responsible for obtaining consents from patients, and use a form which includes directive information and is based on the typical form used for patient medical record requests. Patients and providers find it somewhat burdensome, but no more than usual medical record request processes. The larger provider found implementation the most burdensome, mostly because it had multiple offices and had to get information out to more personnel.

At this stage, where new data types are expected to be brought on line consents are effective per data type, so that additional consents will be needed as new data becomes available. This may change over time to make it easier, as it is not necessary and adds to the burden; a patient subscription model with a one-time consent might make more sense. Consents are effective until the patient revokes them.

INHS has Business Associate Agreements in place with participating providers to permit it to process information on their behalf. This agreement and some ancillary policies are the basis for the consent process and other compliance. There is no contract with GoogleHealth, since it is receiving information as directed by the patient.

Health information exchange via 1HealthRecord may be expanded to add payers, possibly via the BCIN, but that would require some additional development to deal with administrative data and there is no clear value in participation for payers at this point. 1HealthRecord may be able to interface with other health information exchanges, particularly BCIN and other networks operated by INHS. Likewise, 1HealthRecord could connect to public health resources, and connection to the public health Child Profile immunization repository in particular is under consideration.

INHS has conducted a variety of outreach and educational initiatives to reach patients and providers, including media campaigns, presentations at associations and meetings, and mailings. Both providers and patients tend to question why they would need the system, and some patients do not believe it is something they should have to do.

This is a Washington State-supported project, and its financial and other assistance has been important. Local government and provider professional associations, especially at the county level, have also been important supporters, as have some social services agencies and nonprofits. Outreach to patients has been facilitated by supportive associations such as the American Association of Retired Persons (AARP).

**Geographic Coverage**

Spokane, Washington metropolitan area; anticipated expansion to greater eastern Washington/northern Idaho region.
Breadth of Purpose for Sharing PHI
As determined by consumer.

Patient Population
General population, self-selected participation.

Nature of Consent Process
Physician-practice administered, form based on medical records disclosure request.

4.2.5. Kaiser Permanente

Governance: Enterprise
Architecture: Centralized
Consent Source: Enterprise
Consent Type: Opt-In

Kaiser Permanente ("Kaiser") is a nonprofit healthcare enterprise including hospitals, clinics and other provider facilities as well as health plans and services divisions. Kaiser has a significant presence in 10 states as well as a smaller presence in surrounding states. Kaiser has established regions in which the company operates, some are specific states such as California and others cross state lines. Kaiser represents a significant presence in the provider and payer market in the US and regularly transmits patient data across state lines, primarily within the company rather than with or between other providers or health plans.

The operating model Kaiser has adopted for determining which state laws apply to HIE within the Kaiser enterprise across state lines and with external entities applies the most stringent state and federal privacy laws to all HIE, rather than determining allowable exchanges based on individual exchanges between states. This creates, at least for internal HIE across state lines, a simple consent process. Interstate HIE does not, however, occur frequently within Kaiser or between Kaiser and other entities. Kaiser indicated that interstate HIE can be a challenge even in an integrated system.

Any patient seeking care within the Kaiser system is asked to sign a consent/authorization to exchange their entire PHI if care is provided in a state other than the patient’s home state. This is mandated for all exchanges that transfer of PHI across state line. In essence, Kaiser requires an authorization for transmission of PHI, no matter the purpose of the exchange or the data that will be exchanged.

Even though this is a simpler solution than assessing each state’s laws prior to data exchange, challenges still exist. As an example, the requirements related to the exchange of 42 CFR Part
2-protected alcohol and chemical dependency data requires monitoring because re-disclosure is prohibited with additional authorization from the patient.

Kaiser has deployed the Epic electronic health record ("EHR") system across all Kaiser regions. This supports improved ability to exchange PHI between regions and states. Nonetheless, except in emergency situations, traveling patients are still asked to sign a consent or authorization before any PHI is transmitted from Kaiser region to another. Kaiser is its own gatekeeper as it relates to the exchange of PHI within the Kaiser system.

Kaiser does have established HIE with external entities related to treatment. When data is shared with external entities, the same process as for internal HIE is followed – Kaiser obtains patient authorization/consent prior to releasing any PHI to a third party. At this time, these exchanges are point-to-point.

Kaiser’s current health information technology ("HIT") infrastructure and the EHR it has adopted allow the segregation of data. This supports Kaiser’s efforts to comply with more stringent state and federal law by allowing the exclusion of specified, specially PHI in HIE unless specifically authorized by the patient. Despite the general requirement to obtain consent/authorization, the patient will not always authorize the sharing of all PHI, and this may require Kaiser to restrict the sharing of data to non-specially PHI.

Kaiser is not directly engaged with any RHIOs or HIOs but is involved with state HIE initiatives in states Kaiser operates. Kaiser is not moving forward with any local HIE initiative given the technical and policy issues and related expense of adopting to different local HIE standards. Kaiser’s intent is to work with states to develop a common set of understanding across states where Kaiser is involved in state level HIE initiatives.

**Geographic Coverage for Sharing PHI**

Kaiser shares PHI nationally but primarily within the Kaiser system. The sharing of PHI with external entities for treatment purposes is limited. Most data is shared across the 10 states within which Kaiser operates. Kaiser does not currently participate in any RHIO or HIO locally or state level.

**Breadth and Scope for Sharing PHI**

The scope and breadth is wide but limited in the sense that large volumes of PHI may be transmitted between Kaiser facilities within a specific region but data sharing across state lines is generally limited (internal and external). Again, data sharing only involves point-to-point HIE at this time. There is an interest in sharing PHI more broadly across HIEs as barriers at the state level are addressed. Kaiser does not have any plans at this time to connect to any local HIEs.

**Nature of Consent Process**

Kaiser has generally adopted an opt-in with restrictions consent model. If the PHI exchange is across state lines or, in the case of Kaiser, between regions, patients are always asked for consent/authorization to exchange PHI except in an emergency. The same is true for any PHI
disclosures by Kaiser to an external entity. Kaiser’s technical infrastructure supports segregation of data (generally specially protected health information) to accommodate a patient’s limited consent/authorization to exchange the patient’s PHI.

This is also the same consent model that has been adopted by Kaiser and the Veterans Administration ("VA") to support the current partnership project between Kaiser and the VA. It is not known if the VA’s technical environment supports the ability to appropriately segregate data when restrictions to exchange apply.

Duration of Consent

Consent for general PHI exchange is a one-time use only and is per encounter. This is true for Kaiser patients and when patients are acting in the capacity of health plan members. Specific consent or authorization relating to specially protected health information is durable – they do not expire until revoked by the patient or the authorization expires (time or event driven expiration pursuant to the HIPAA Privacy Rule).

Form of Agreement

Kaiser uses a common consent form within Kaiser. Kaiser currently has not entered into any HIE related agreements with other states or any RHIOs or HIOs. Kaiser is interested in a standardized approach that fits with national efforts and the NHIN framework. Development of any common form of agreement that accommodates interstate exchange of PHI is not likely close to drafting or adoption given a number of the states Kaiser is working with have not addressed interstate HIE yet.

Educational Efforts

Provider education occurs through provider associations, mailings and Web based educational medium. Payer education utilizes the same methods as provider education. Patient education occurs through media, mailings and Web. Kaiser is not currently involved in public health educational efforts but is interested in effective methods of expanding the use of HIE between public health entities and between public health entities and payers/providers.

Standards Adoption Barriers

Kaiser’s goal is to work with states to adopt nationally accepted HIE standards and to adopt standards that accommodate interfacing with the national health information network ("NHIN"). Kaiser is concerned more about adoption of common national standards (especially technical) than the patchwork of state and federal privacy laws, especially given Kaiser’s current practices related to interstate HIE.

Kaiser is fully aware that different states will adopt different HIE models such as record locator systems, databases, etc. One of the most significant issues Kaiser sees as a barrier to HIE between states is that there is a high potential that states’ HIE efforts will not meet NHIN standards.
Several states are considering forming their own accreditation bodies for HIEs with what will likely be differing sets of standards depending on the state. Kaiser believes this should be more of a national activity similar to certification of EHRs. The more accreditation bodies formed state by state, the higher the risk that the NHIN technical standards and other related standards will not be consistently included as requirements in the accreditation process.

**Privacy Barriers**

Kaiser has adopted a conservative approach to consumer/patient privacy. One of the significant reasons Kaiser has adopted its current internal consent model is Kaiser strongly believes the patient should be in control of how and when that patient’s data is shared. It is more than just an issue of what laws are more stringent when it comes to the privacy of PHI.

Kaiser is currently involved in a joint project with the VA and has adopted a consent model of opt in with restrictions. Patients are asked if they want their data to be exchanged between Kaiser and the VA versus an opt out model that allows exchange of PHI unless the patient Kaiser strongly believes the decision regarding what to exchange rests with the patient and the gatekeeper who indicates what data can and will be shared is the health care provider. This is reflective of other discussions that point to the provider as the gatekeeper and the individual or entity that is required to determine what data should be transmitted point-to-point or made available to multiple providers participating in an HIE.

A concern was also raised regarding the secondary use of data by the RHIO or HIO and others with access to data that may be stored in a central repository or even data that is captured as it is transmitted through an HIE. Kaiser is concerned that entities such as RHIOs and HIOs will profit from the secondary use of data and use it without necessarily the consent of the patient. Also, Kaiser is concerned about what may amount to significant fees charged by RHIOs and HIOs for using their services and accessing what amounts to PHI needed for improved quality of care and as authorized by the patient.

**Financial Concerns**

As indicated above, Kaiser is concerned that the exchange of PHI will become a revenue-generating activity rather than a way to improve health care quality and improve efficiency. It is understood that HIEs need to be self-sustaining but there is a concern that the cost associated with the HIE will exceed what would be considered necessary to sustain the HIE in the long term.

As the health care provider, Kaiser believes Kaiser should be in control of the patient data and how it is used. This would include primary and secondary use of the data. Kaiser is interested in supporting a system that treats patient data appropriately, allows appropriate consumer/patient involvement/decision making when the patient’s data will be used for purposes other than treatment and HIEs established do not add extra cost to the provision of health care. Kaiser strongly believes in a consumer/patient centric model.

**Administrative Burdens**
Kaiser believes the adoption of HIE will result in significant burdens to providers, patients and to some extent patients. This is related to engagement, establishing exchanges and the actual burden of interacting with other providers through an HIE.

There will be a need to change workflows across the industry. Kaiser is a very patient-centric organization and sees a need to actively engage patients in the process of moving toward greater exchange of PHI across HIEs. Workflow changes will also be required at the provider and payer level. Kaiser’s goal is to see the adoption of NIST related standards and other nationally adopted technical and policy standards. This will require a change in how providers and payers operate resulting in workflow changes and retooling on the part of the workforce.

4.2.6. Mayo Clinic

**Governance:** Enterprise

**Architecture:** Centralized

**Consent Source:** Enterprise

**Consent Type:** Opt-In

The Mayo Clinic operates three clinics in three states (Minnesota, Arizona and Florida) and the Mayo Healthcare system operates in five states (the above states plus Iowa and Wisconsin). Mayo provides direct care in 75 communities, primarily in the Mid-West. Mayo also provides a significant volume of care for patients who reside across the U.S. with a small but significant number of patients residing outside the U.S.

Mayo maintains a data exchange serving Mayo facilities in all five states in which it operates, which is internal to Mayo. Mayo has implemented an internal master patient index (MPI) to assist in accurately identifying patients and uses three major EHR platforms to manage patient data. The EHR deployed is generally related to a specific area in which Mayo operates. Mayo has developed its own “translator” between the three EHRs and has adopted common standards across all platforms.

Mayo has developed an integrated clinical repository using standardized data that includes PHI from across all five states in which the Mayo Healthcare Delivery system operates. Complete access to the repository and common data exchange is limited in the Southern states. The data exchange is limited and a web browser approach is used to access data in this area.

Mayo understands the challenge of differing legal requirements and addresses it through what amounts to an Opt-In with restrictions model (except for research within the State of Minnesota) through which differing state and federal privacy laws can be accommodated. Mayo see the more significant challenge to be inconsistent standards, rules and practices adopted by states that act as a barrier to electronic exchange of data.
Mayo organized a multi-state HIE summit during Fall 2009. Public sector invitees include the five states Mayo operates in. A second summit is planned for Fall 2010. The purpose of the summits is to work towards common adoption of standards that meet NHIN requirements. Kaiser is also a partner with Mayo in this effort.

Mayo does share PHI with external entities for purposes related to treatment. When data is shared with external entities, Mayo acts as the gatekeeper and obtains the patient’s consent/authorization to disclose PHI to a third party. If the consent/authorization does not include permission to exchange certain types of health data such as specially protected health information, the data is excluded from the data set that is exchanges. Mayo primarily exchanges PHI with external entities using point-to-point HIE rather than a networked HIE. At this time Mayo does not participate in any RHIOs or HIOs, local or state. Most hospitals in Minnesota participate in the Minnesota HIE but Mayo does not at this time.

**Geographic Coverage for Sharing PHI**

A fair amount of PHI shared by Mayo is shared within the Mayo system and across five states. Mayo does exchange a large amount of patient data with external entities since Mayo provides care for patients across the US and internationally. If data is shared with an external entity the same or a similar process is followed – patient consent/authorization is obtained and Mayo acts as the gatekeeper, only sharing the data as authorized by the patient with the external third party.

**Breadth and Scope for Sharing PHI**

The scope and breadth is wide. A large volume of PHI is transmitted between Mayo facilities within the states in which Mayo operates. Also, a large amount of data is exchanged outside the Mayo operating area given the scope and breadth of care provided by Mayo. Mayo also needs to take into account international privacy law which, as an example, in Europe is more stringent than in the US.

Data sharing only involves point-to-point HIE at this time. There is an interest in sharing PHI more broadly across HIEs as barriers at the state level are addressed. Mayo does not have any plans at this time to connect to any local HIEs.

**Nature of Consent Process**

Mayo has adopted an opt-in with restrictions consent model. This is true for data exchanged within the Mayo system and between Mayo and external entities for the purpose of treatment. The exception is the collection and use of PHI for research purposes in the state of Minnesota. In the case of research in Minnesota, an Opt-Out consent is used. Mayo does not view either form of consent model as a significant issue with patients or for the exchange of PHI.

Consent is obtained by providers in all cases. It is obtained at the place of treatment at the time treatment is scheduled or as part of a pre-registration process.

**Duration of Consent**
Consent obtained from the patient expires following an episode of treatment. If the patient returns for treatment and it is considered part of the same episode of treatment, an additional consent is not requested. If it is considered another episode of treatment or encounter, consent is obtained again. Research-related consent is one time only and is offered to the patient at each encounter.

**Form of Agreement**

Where an opt-in with restrictions consent is used, Mayo uses, for the most part, a common consent form. The same is true for the opt-out consent (related to research). Agreements with third parties to protect the patients’ PHI and to enforce adherence to the patients’ wishes as documented in the consent form are primarily business associate contracts and trading partner agreements.

Internally, Mayo enforces the appropriate segregation of specially protected health information through policy. All providers who attempt to access a patient’s record must read a warning regarding inappropriate patient record access and the fact that provider access is logged and reviewed and click to verify the provider is the patient’s provider and authorized to view the patient’s PHI. This method of enforcement has proven effective for Mayo and is effective across state lines.

**Educational Efforts**

Mayo has and will continue to use HIE summits involving states Mayo operates in as a tool to educate states regarding the use of common technical and policy standards that have been adopted nationally and accommodate interfacing with NHIN. At this point in time Mayo is involved in internal education of providers but is not involved in any more expansive educational efforts. Mayo does belong to a coalition of other large healthcare delivery systems such as Inter-Mountain, Sutter and Kaiser and is engaged with the coalition in addressing standard adoption of technical requirements and related policies versus what would be considered “on the ground” educational efforts with individual payers or patients.

**Standards Adoption Barriers**

Mayo’s goal is to work the previously mentioned collaborative and the states in which Mayo operates to adopt nationally accepted HIE standards and to adopt standards that accommodate interfacing with NHIN. Mayo is concerned more about adoption of common national standards (especially technical) than the patchwork of state and federal privacy laws.

One of the more significant issues Mayo has encountered when working with the five states where Mayo has a presence is the adoption of state specific rules as it relates to how HIEs will exchange data rather than adopting nationally identified standards. Mayo believes this is a significant barrier and, more than issues related to disparate privacy laws, will impede the flow of PHI between states and nationally.
Several states are considering forming their own accreditation bodies for HIEs with what will likely be differing sets of standards depending on the state. Kaiser believes this should be more of a national activity similar to certification of EHRs. The more accreditation bodies formed state by state, the higher the risk that the NHIN technical standards and other related standards will not be consistently included as requirements in the accreditation process.

Privacy Barriers
The accurate identification of patients through an HIE is seen by Mayo as both a standards and a privacy barrier. Mayo has adopted its own internal MPI but there is not a nationally accepted MPI nor are there national patient identifiers. There is a concern that the wrong patient will be identified which impacts the privacy of the patient’s PHI, may impact the quality of care provided and potentially lead to adverse outcomes. Mayo understands that the implementation of a national patient identifier is not likely to occur but Mayo believes a national MPI model should be adopted that is updated regularly to reasonably ensure the patient’s data that is exchanged through an HIE actually is the data of the patient that will be diagnosed or treated.

A concern was also raised regarding the secondary use of data by the RHIO or HIO and others with access to data that may be stored in a central repository or even data that is captured as it is transmitted through an HIE. Kaiser is concerned that entities such as RHIOs and HIOs will profit from the secondary use of data and use it without necessarily the consent of the patient. Also, Kaiser is concerned about what may amount to significant fees charged by RHIOs and HIOs for using their services and accessing what amounts to PHI needed for improved quality of care and as authorized by the patient.

Financial Concerns
Mayo indicated there will likely be a fairly significant cost associated with technically connecting states as part of interstate HIE and a connection to NHIN. There are differing levels of sophistication, maturity and standardization between state HIE programs and potential participants within each state. Funding may be available to assist at this time to address interconnection but it will not necessarily be available for a sufficient period of time to assist in developing a lasting connection between states and nationally.

Another challenge Mayo sees facing the industry from a financial perspective is the adoption of EHRs that meet meaningful use standards. One of the contributors to the exchange of quality, complete and usable data is the expanded adoption of EHRs that accommodate meaningful use which includes interoperability. Small and rural providers may be slow to adopt new technology because of the cost. The incentives associated with adoption of an EHR a provider can utilize requires the provider pay for the cost of implementation/upgrade, training, conversion, etc. up front prior to receiving payment to cover the cost of the implementation or upgrade. The lack of broad based adoption will likely reduce the amount of meaningful data available through an HIE.
Administrative Burdens

Mayo does not see payers facing a significant administrative burden as it relates to interstate HIE. Mayo does see there will likely be a significant burden to providers (EHR implementation/upgrade, HIE connection and data management, deployment of personal health records (PHR) for patient use). Mayo also expects there will be a significant burden placed on patients who will feel the pressure from states and others to utilize their own PHR.

Mayo believes in the long run broad adoption of meaningful use standards and NHIN related standards will assist in improving the quality of healthcare while decreasing the cost of providing healthcare. In the short run, though, Mayo believes the administrative burden and associated cost to the industry will not be insignificant.

Quality of Care Challenges

Until such time as data is more widely shared in the form of what amounts to network versus point-to-point sharing, continuity of care will continue to be an issue. It is difficult currently for multiple providers of health care for a single patient to collaborate and provide what would qualify as higher quality and lower cost health care. Mayo is also concerned that patient care will be adversely impacted without a standardized MPI. If, as an example, a patient prescribed medication that highly interacts with other medications and substances is seen even in a general care setting and the provider accesses the wrong patient’s record, the presenting patient may be prescribed medication or a treatment regime that will adversely interact with current medication.

Technical Challenges

Mayo considers the technical environment created by individual states will represent a significant barrier to PHI exchange beyond the state’s boundaries. If common technical standards are not adopted, Mayo is not confident that interstate HIE will become a reality other than the current point-to-point method let alone the expansion of a viable national network used to share PHI.

A significant challenge Mayo articulated is the disparity in the maturity of state HIE/HIT programs. States are seen by Mayo as reluctant to share individual state resources if the resources are not used in the best interest of the state. In other words, states are reluctant to spend what really are limited HIE dollars to assist a neighboring state still in its HIT/HIE infancy mature its internal HIT/HIE infrastructure. Given current state budget crises, all states are taking a very close look at how funding is spend, no matter the source.

Financial Incentives

Mayo believes federal financial incentives made available to states would have been more effective if the same dollars were allocated to each state that agreed to enter into a collaborative tougher rather than receiving less funding because of perceived efficiencies. In this case, states who were much further along in expanding their HIE/HIT infrastructure were
reluctant to receive less dollars and be required to use those dollars assisting another state reach the same level of maturity.

At this time Mayo looks at the primary financial incentives as related to federal stimulus dollars versus, at least initially, dollars from states or private entities. Mayo and other members of the collaborative Mayo participates in are assisting in providing technical expertise and guidance which amounts to a financial incentive based on staff support rather than, say, issuing grants. Kaiser

Mayo does believe the incentive dollars associated with meaningful use will benefit Mayo and others in expanding the use of HIT and the expansion of the amount of data available through an HIE. At this point, though, Mayo is reviewing organizational options and looking for a national strategy to emerge.

Summary

Mayo is a consumer/patient centric healthcare delivery system with major clinics in three states and a delivery system covering a total of five states. Mayo is unique in that Mayo provides health care services to residents of all 50 states and to international residents. While there is a definite catchment area for the Mayo Healthcare Delivery System, Mayo is a significant national and international provider of care. This places Mayo in the unique position of disclosing PHI across all state lines and outside the US. Given that, Mayo has developed its own system based on internally developed standards to share data relatively easily across Mayo and also between states.

Mayo’s primary concern is related to the common adoption of technical and policy standards across all states that are consistent with NHIN. Mayo sees this as a more significant barrier to interstate and ultimately national IHE than the hodgepodge of state and federal privacy laws. Mayo participates in a collaborative consisting primarily of large healthcare delivery systems and works with the five states Mayo has business operations in. The goal is to adopt national standards across states and also adopt a standardized MPI that provides greater accuracy in patient identification. Mayo is not currently directly involved with any RHIO or HIO. All or most HIE is point-to-point.

4.2.7. Surescripts

<table>
<thead>
<tr>
<th>Governance</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>Consent Source</td>
<td>Provider (Transactions)</td>
</tr>
<tr>
<td></td>
<td>Plan (MPI)</td>
</tr>
<tr>
<td>Consent Type</td>
<td>Variable at Provider/Plan Election</td>
</tr>
</tbody>
</table>
Surescripts operates a nationwide e-prescribing network. The current network was formed through the 2008 merger of SureScripts, which was established to provide e-prescribing services by the National Association of Chain of Drug Stores and the National Community of Pharmacists Association, with RxHub, which was established for complementary purposes by pharmacy benefits managers (“PBM”) including CVS Caremark, Medco Health Solutions, and Express Scripts. The company is owned by the PBM and pharmacy associations which established the original companies.

Surescripts principally provides network services to pharmacies, hospitals and physician practices, and health plans and PBMs. It currently serves an estimated 190,000 physicians and 50,000 pharmacies. Surescripts does not contract directly with providers, but instead contracts with their electronic medical records (“EMR”) vendors, whose systems must support a connection to Surescripts. Surescripts is provided to prescribers at no cost, and obtains its revenues from payers and pharmacies.

Surescripts transmits prescribing-related transactions using industry standards. It does not serve as a repository for information, and does not claim ownership of transaction information. It does maintain a master patient index (“MPI”) including demographic information on an estimated 250 million individuals, provided by some twenty or so payors which use the network. Consents may be implicated in both these functions. Surescripts does not obtain or administer consents, but relies on its participants to do so where appropriate.

RxHub had developed transaction consent forms, but these proved unnecessary under the EMR vendor contracting business model. At this point Surescript manages compliance issues of this kind by contract. In particular, in its technology partner (EMR vendor) contracts Surescripts requires the vendor to in turn require their customers (prescribers and pharmacies) to comply with all applicable laws. Language in the contracts between the vendor and its customers then passes the compliance obligation to the customer.

Surescripts does not verify or require the verification of the existence of an applicable consent for transactions, except for medication history requests. Those transactions require the consent “flag” to be present, indicating that patient consent has been obtained or applicable law has otherwise been complied with. Surescripts relies on the payers which provide MPI information to obtain any consent which might be required for that kind of use.

Surescripts (and RxHub prior to the merger) has participated actively in standards bodies and related activities to help develop the standards needed to enable e-prescribing. Its representatives speak at relevant conferences and other events, and it has engaged in some media campaigns.

**Geographic Coverage**

National.

**Breadth of Purpose for Sharing PHI**
Limited to prescription fulfillment and payment.

**Patient Population**

General.

**Nature of Consent Process**

Transaction consent delegated to individual providers.

Use of information for MPI purposes delegated to patients’ health plans.

4.2.8. *Texas Health Services Mental Health Transformation Project*

**Governance:** Standard HIO  
**Architecture:** Centralized  
**Consent Source:** Provider (Program)  
**Consent Type:** Opt-In

The Clinical Management for Behavioral Health Services System (“CMBHS”) was created by the Texas Department of State Health Services as part of a statewide initiative to improve the delivery and management of behavioral health services. The statewide program is aligned with The President’s New Freedom Commission on Mental Health recommendations issued July 22, 2003.

The CMBHS is focused on 42 CFR Part 2-related issues and works through state-licensed substance abuse treatment facilities. The two primary patient populations served by the system are Medicaid and state-subsidized individuals.

The CMBHS is intended to be an integrated clinical management system for behavioral health services with the following features:

- An EHR
- An integrated billing functionality
- One system to house DSHS behavioral health data in
- Interoperability with other systems

The CMBHS is an intra-state system for sharing behavioral health information among state-funded providers. At the time of this report, the substance abuse components of the system have been released, connecting about 250 organizations and approximately 4,600 end users.
Connectivity to contracted mental health providers (Local Mental Health Authorities/NorthSTAR\textsuperscript{53}) will be improved during the fall of 2010 and advanced information exchange with mental health providers is proposed for development during the next 24 months, CMBHS officials said.

The consent management system in CMBHS is part of an intra-state information exchange that has only come online in December 2009. At the time of this report, the substance abuse components of the system have been released, connecting about 250 organizations and approximately 4,600 end users. Certain components of data sharing, consistent with applicable law, such as interconnectivity to the state’s criminal justice and courts systems have been implemented. Connectivity to contracted mental health providers (Local Mental Health Authorities/NorthSTAR) will be improved during the fall of 2010 and advanced information exchange with mental health providers is proposed for development during the next 24 months. CMBHS managers adopted a phased-in approach to implementing the system and have taken steps to deeply involve providers. This was possible in large part because the providers are contractors for the state.

42 CFR Part 2 and mental health consent requirements are considered obstacles to electronic HIE. In this project, the issues appear to have been resolved because patients are giving consents for sharing information for mental health and substance abuse records first, which then allows the sharing of information with other providers.

Patient permission is obtained once by a state-licensed treatment center from the patient. The consent is inclusive of all information related to substance abuse and other aspects of the patient’s medical record in support of providing assessments and treatment planning. Patients may restrict or revoke their consents to share data with providers through the healthcare provider.

The CMBHS managers noted that there has been no interaction with FERPA and related educational records privacy laws and rules. The CMBHS system serves contracted providers. No contracted providers are school-based health providers, although some contractors may receive referrals from education-based health care providers such as school-based health centers. Students and parents must seek treatment voluntarily.

Generating support for the system was straightforward as providers were state-licensed substance abuse treatment centers. They were aimed at providers through professional associations and through training programs operated by DSHS. Program managers also emphasized that providers were involved in the development of the CMBHS to ensure that it met their operational needs. CMBHS officials crafted use cases, tested prototypes of the system, and then solicited feedback from the providers.

\textsuperscript{53} NorthSTAR is a behavioral health service system, through which mental health and substance abuse services are provided to eligible consumers, serves seven counties. NorthSTAR is composed of the Dallas Area NorthSTAR Authority (DANSA) and a Behavioral Health Managed Care Organizations (BHO). DANSA provides local authority functions and the BHO manages a provider network, including several community mental health centers.
This took some effort by both CMBHS managers and the provider community.

In piloting the project, CMBHS create the following framework:

Over 350 fields in assessment

- Not all fields must be completed

- Participating sites represent
  - Urban areas
  - Rural areas
  - Mental health provider
  - Substance abuse treatment providers
  - Geographic diversity within Texas

Program managers reported that the financial burden on providers was not an issue. Overall, the system could be viewed as an incentive because the state licensed treatment facilities avoided system maintenance responsibilities. They also noted that when the state rolled out the BHIPs system, the state helped finance provider equipment to run the system.

The state did not have a substantial burden because the program funded largely through a SAMSHA grant.

The Consent Process

Patients opt in to the CMBHS. The consent covers most PHI as it allow the use and disclosure of information as it relates to the patient’s substance abuse issues, including assessments and treatment planning. That meant that substance abuse treatment professionals had access to a large portion of a patient’s PHI. This, in fact, was one purpose of the system, as the state wanted to move toward treating the “whole person,” who had substance abuse issues.

Consent is a one-time event that allows providers across the system to access patient records as deemed justified and appropriate for treatment purposes.

Privacy and Security Controls

The program used contracts because the healthcare providers were state-licensed substance abuse treatment facilities. The contract language was incorporated into the treatment facility’s performance contracts. There is no separate agreement for using CMBHS.

Program managers reported that the inclusion of these contract provisions was not a challenge because CMBHS grew out of its Behavioral Health Integrated Provider System (BHIP), an existing state IT/IS initiative that was crafted to meet legal requirements.

Memoranda of understanding were executed between DSHS with the Office of Court Administration and with the Department of Public Safety as part of state legislative mandates to better manage behavior health issues in the criminal justice and judicial systems.
State and Federal Consent Laws Affecting
Interstate Health Information Exchange
2011

Patient Rights
Patients have the right to opt-out of the system but must do so through the provider. A patient may restrict the flow of information to certain providers. These rights are consistent with Part 2 requirements generally.

CMBHS managers reported minimal problems stemming from the nature of the patient population. They did note, however, that was some concern in some rural communities. These concerns were based on the fact that residents were well-acquainted with one another. However, these concerns were expressed as a general caution and not as an objection related specifically to obtaining consent or electronic medical records.

Geographical Coverage
CMBHS is part of a Texas intrastate information exchange that has only come online in December 2009. As of the date of this review, the systems covers approximately 250 licensed substance abuse treatment facilities that have contracts with the state to provide services.

Breadth of Purpose for Sharing PHI
Program officials state that the consent covers most PHI as it allow the use and disclosure of information as it relates to the patient’s substance abuse issues, including assessments and treatment planning.

Because the program was focused on substance abuse issues and involved state-licensed entities, determining the amount of PHI covered by consent was not a significant issue.

Patient Population
Patients are generally individuals who received publicly-subsidized services including Medicaid and state general revenue-funded services.

CMBHS manager reported minimal problems stemming from the nature of the patient population. They did note, however, that was some concern in some rural communities. These concerns were based on the fact that residents were well-acquainted with one another. However, these concerns were expressed as a general caution and not as an objection related specifically to obtaining consent or electronic medical records.

Nature of Consent Process
CMBHS relies on an opt-in consent process in which the patient determines who will have access to his or her medical records.

Consent is a one-time event that allows providers across the system to access patient records as deemed justified and appropriate for treatment purposes. There are no specific time periods for the duration of the consents. The duration is up to the provider, but program managers state that one year appears to be the default time frame.

A patient is allowed to change the nature of the consent through the provider.
Program managers have not detected any significant problems or issues from providers or patients thus far.

**Form of Agreement Among Stakeholders**

The program used contracts because the healthcare providers were state-licensed substance abuse treatment facilities. The contract language was incorporated into the treatment facility’s performance contracts. There is no separate agreement for using CMBHS.

Program managers reported that the inclusion of these contract provisions were not a challenge because CMBHS grew out of its Behavioral Health Integrated Provider System, an existing state initiative that was designed to meet legal requirements.

Memoranda of understanding have been established between the Texas Department of Social and Health Services, Office of Court Administration and Department of Public Safety as part of state legislative mandates to better manage behavior health issues in the criminal justice and judicial systems.

**Existing Relationships**

CMBHS managers report that its provider base represents “a small slice” of the broad healthcare provider community. In addition, many of the facilities have been contractors to the state for long periods of time.

**Educational Efforts**

Because providers were state-licensed substance abuse treatment centers, educational efforts were straightforward. They were aimed at providers through professional associations and through training programs operated by DSHS.

Patients are educated by providers.

Program managers also emphasized that providers were involved in the development of the CMBHS to ensure that it met their operational needs. CMBHS officials crafted use cases and tested prototypes of the system and then solicited feedback from the providers. This took some effort by both CMBHS managers and the provider community.

**Administrative Burden and Need to Change Workflows**

Migration to a new system involved some changes administratively for providers. However, because they were involved in the development of the process, this burden was considered moderate.

**Financial Burden**

Program managers reported that the financial burden on providers was limited. Overall, the system could be viewed as an incentive because the state licensed treatment facilities avoided system maintenance responsibilities. The state did not have a substantial burden as the program funded largely through a SAMSHA grant.
4.2.9. WellPoint Individual Health Record

<table>
<thead>
<tr>
<th>Governance:</th>
<th>Standard HIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture:</td>
<td>Centralized</td>
</tr>
<tr>
<td>Consent Source:</td>
<td>Provider</td>
</tr>
<tr>
<td>Consent Type:</td>
<td>EHR: No Consent</td>
</tr>
<tr>
<td></td>
<td>PHR: Opt-In</td>
</tr>
</tbody>
</table>

A collaboration among Anthem Blue Cross Blue Shield/WellPoint, Kettering Health System and CentriHealth is implementing an “individual health record” (“IHR”) system centered in a 10-county region surrounding Dayton, Ohio. The IHR combines and aggregates data from multiple sources, for treatment purposes only. The system generates both an electronic medical record and a personal health record for 10-county region surrounding Dayton, Ohio. Approximately 500,000 patients and 1,000 healthcare providers participate.

Participation in the system spans the entire healthcare provider community and includes payers and employers as well. WellPoint has consistently made a business case for participation, noting savings from reduced duplication of tests and other healthcare services. An equally important factor, according to the company, is that the system improves healthcare quality.

The system manages both EHRs and PHRs through an integrated system, which both populates the EHR and enables patient access and provides patient controls of how the data is shared. The EHR and PHR functionality can be used independently of one another.

Patient permission to use and disclose health information is at the discretion of the patient. There is no definite duration, but the system requires patients to change their passwords to the system on a routine basis.

From a permission perspective, healthcare providers decide to participate in the EHR typically without consulting the patient. WellPoint explained that providers provide notice of their use of EHRs in their HIPAA Notice of Privacy Practices.

 Patients, however, have substantial control in the area. Patients who participate in the personal health record system may impose restrictions on which healthcare providers have access to their data. As a result, healthcare providers only see information that patients authorize.

WellPoint, which was one main backers of the initiative in 2006, pays for the operation and maintenance of the system. However, the system is operated by a vendor under contract to WellPoint. Consequently, the payer is not involved in the day-to-day activities.

The system does not share electronic health records across state lines. However, WellPoint observed that PHRs do cross state boundaries because some dependents leave outside of Ohio.
The IHR does not include educational records covered under FERPA or 42 CFR Part 2 records. WellPoint is piloting a Member Medical History system in emergency rooms in Missouri, California and Kentucky.

The insurer also offers free e-prescribing system to all its network physicians through the National E-prescribing Patient Safety Initiative.

While the IHR has an e—prescribing component, WellPoint said it was too early to tell whether meaningful use incentives provided in the HITECH has had much effect on participation.

The key features of the IHR are:

- The ability of the IHR to incorporate comprehensive clinical and claims data into a single electronic understanding of the patient.
- The ability to provide physicians a professional view of the IHR as an EHR containing organized history and problem lists, alerts and evidence-based medicine reminders.
- The ability for members to use the layman’s view of the IHR as a PHR including patient generated notes, patient-oriented wellness and preventive reminders, and patient access to full medical information.
- Electronic prescribing offering safety alerts, dosage information, and cost guidance; and
- Integrated and automated collection of clinical and claim data with central access to medical information from all providers involved in the patient’s care including medical claims.

In February 2009, WellPoint reported high rates of use with about 70% of employees exposed to the tool making use of it. More than 40% of patients made use of the tool six times or more. Patients with chronic conditions seem to be the heaviest users of the PHR system.

**Geographic Coverage for Sharing PHI**

The IHR is used as an EHR by providers in a 10-county region surrounding Dayton, Ohio. WellPoint estimates that the PHRs are used in Ohio and 12 other states where dependents reside.

**Breadth and Scope for Sharing PHI**

The IHR is used for treatment and disease management purposes and involves all PHI with the exception of 42 CFR Part 2 data. Educational records are not included either.

**Nature of Consent Process: IHR as EHR**

Healthcare providers do not typically discuss patient permission to use health data electronically, according to WellPoint. Instead, the providers include a reference to this practice in their Notice of Privacy Practices.
Providers are limited to viewing records only for their own patients or patients that have been referred to them by another provider.

**Nature of Consent Process: IHR as PHR**

Patients voluntarily register to participate in this program. In some instances, patients will notify their providers that they are participating in the PHR program, thus encouraging provider participation.

Patients control which physicians may view the records through the IHR system. The IHR system then imposes those restrictions on the EHR used by the treating provider.

**Duration of Consent**

Consents are given once and have no formal expiration dates. Patients may revoke consents through their PHR management system.

**Form of Agreement**

WellPoint said that the system used a combination of contracts and unified policies and procedures.

**Challenges for Recruitment/Education Efforts**

WellPoint explained that it had “lots of sit downs” with many different stakeholders to outline the program. Sponsors of the IHR spent considerable resources in making the business case for its system to providers, employers and payers. Individual physician practices presented some of the biggest challenges as they viewed this system as “one more thing to learn.” However, WellPoint said they were generally convinced to participate after being educated on how treatment would be improved.

The providers had varying degrees of experience with IT. Major concerns over participating in the program did not solely focus on privacy and security. The key issues were how such a system would improve quality as providers stated that they worked in an environment with limited data. The insurer noted that providers were more difficult to recruit than patients.

Patient concerns focuses on who would receive the data and who would receive it. There have been no formal studies of patient reaction, but WellPoint anecdotally reported only one instance of a patient expressing a concern in the 2.5 years of operation. WellPoint reported that patients also expressed some reluctance at having “to learn one more thing.”

Payers were brought on board as the system demonstrated that treatment would be improved and the number of unnecessary or duplicated tests and procedures would be significantly reduced.

Reaching large employers also helped generate large numbers of patients who could be targeted for educational materials encouraging participation.
Outreach was based on some Internet demonstrations that allowed providers and patients to see how the system would work.

The collaborative also worked with the state medical society and other organizations. WellPoint noted that its size and name recognition helped provide a level of trust among the participants.

**Administrative Burdens/Changes to Workflows**

WellPoint reported that there were few burdens on providers or patients. Providers accessed the system through a web portal. Some providers faced some burden in coordinating their access to an IHR with the systems they used at other healthcare facilities where they had privileges.

**Financial Incentives**

WellPoint is paying for the operation and maintenance of the IHR system. It subcontracts the operation to a vendor. The insurer said it was not involved in the day-to-day operation of the system except to the extent that it added its data feeds to the system.

**Effect of Meaningful Use Incentives**

WellPoint said that it had a sense that the meaningful use incentives provided in the HITECH Act may have had some influence on provider participation. It did not view these incentives as particularly compelling. Moreover, the incentive system has yet to take effect so there is no evidence to base any conclusions.

### 5. Legal Standards and Issues Affecting Use of Consents

Potential liabilities related to variations in legal requirements for consents have consistently been identified as an obstacle to interstate HIE. It is true that there is significant variation in consent requirements among the states, between state and federal laws, and between the three principal federal laws in this area (HIPAA, FERPA and 42 CFR Part 2). However, while it is clear that these variations have created considerable confusion, it is not clear that these variations in fact create liability exposures that are not subject to reasonable management except in a few specialized use cases.

The principal healthcare law concerning consents is the federal Health Insurance Portability and Accountability Act of 1996 (“HIPAA“) and its implementing privacy regulations (42 CFR Part 164, Subpart E, the “Privacy Rule”). FERPA and 42 CFR Part 2 concern consents in specialized educational and alcohol and substance abuse treatment contexts respectively, and most (probably all) states have one or more laws requiring or otherwise concerning the use of consents for at least some healthcare organizations, actions or records.
HIPAA provides a useful baseline and “floor” for interstate HIE consents, which provides a basic framework of consent requirements for most use cases. Where state law is more stringent than HIPAA (i.e., provides more limitations against use or disclosure of information, or grants patients greater rights), state law applies; where state law is less stringent, HIPAA applies.

Since state laws apply only in their own territories an organization which wants to disclose information for interstate HIE need only be concerned about compliance with HIPAA and with its own state’s laws. Likewise, an organization in another state which wants to obtain information from that organization need only be concerned about its own state law and HIPAA. If either states’ consent laws pertaining to the transaction are more stringent than HIPAA, the party in that state can apply that law and reject or condition the transaction as necessary to comply with the state law. If neither states’ consent laws are more stringent than HIPAA, HIPAA applies to both parties consistently.

Most if not all states have laws which extend more stringent protections to at least some categories of SHI, and some extend more stringent protections to most if not all types of PHI. 42 CFR Part 2 is a federal law which applies to alcohol and drug abuse patient records and information maintained by any federally-funded alcohol or drug abuse program (“Program”), imposing more stringent protections on such records and information than HIPAA, and may be considered a type of SHI. FERPA, on the other hand, is not concerned with PHI or SHI, but is a separate and parallel system of protection for information maintained by educational institutions, personal information which is specifically excluded from the HIPAA definition of PHI but is instead subject to FERPA’s protections.

5.1. Consents under HIPAA: The Federal Baseline

HIPAA provides a nationwide “floor” for the protection of PHI. HIPAA works this way because it preempts any “more stringent” state or federal law, meaning a law which:

- With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information [i.e., PHI in this Report], for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.\(^{54}\)

Conversely, HIPAA does not preempt state laws which are provide broader or additional individual consent rights.\(^{55}\)

\(^{54}\) See 45 CFR § 160.202 (definition of “more stringent,” subsection 4).

\(^{55}\) Id.
PHI under HIPAA is very broadly defined, as any information in any form or medium is created or received by or on behalf of any entity regulated by HIPAA (health care providers, health plans, and health care clearinghouses, called “Covered Entities”) which

. . . relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual . . . that identifies the individual [or] with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 56

PHI expressly does not include education records subject to FERPA. 57 However, it does include alcohol and substance abuse program records subject to 42 CFR Part 2. 58

Given this broad definition PHI also includes most if perhaps in outlying cases not all information subject to state health information, medical records and health insurance laws, and in many states other laws affecting issues such as genetic information, sexually transmitted diseases. 59 Many of these laws have provisions related to consents, and most states probably have at least one law requiring consents for some types of use or disclosure of information protected by that law which is also PHI protected by HIPAA. Where that occurs, the “more stringent” consent law controls.

The Privacy Rule provides for both “consents” and “authorizations,” but the former seems to be an artifact of the history of the regulations which appears to have minimal practical implications. The Privacy Rule was promulgated and implemented in a series of proposed and final rules from 1999 through 2002. The final rule as published in 2000 (the “2000 Rule”) required health care providers to obtain written, signed consents meeting regulatory requirements before using or disclosing PHI for treatment, payment or healthcare operations (“TPO”) purposes under all but a few circumstances, such as an emergency. 60 Providers could refuse to give care and health plans could refuse to pay if the patient refused to sign such a

56 45 CFR § 160.103.
57 Id.
58 See generally U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment, The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs (June 2004).
59 See Pritts et al, supra note 10.
While there was no rigorous discussion of authorities, it was noted that most hospitals sought consent from patients for use of their information for such purposes.\textsuperscript{62} Any other entity could also obtain a TPO consent, at its option and if the patient was willing, but the theory was that requiring providers primarily responsible for obtaining TPO consents would create an opportunity for truly informed patient consent by discussion with a party with ethical obligations to the patient.\textsuperscript{63} “Authorization,” on the other hand, was seen as a less informative process, available to all types of entity and applicable to most PHI uses and disclosures other than TPO.\textsuperscript{64} The compliance date for the 2000 Rule was April 2003, and before that date revisions were proposed which would eliminate the TPO consent requirement.\textsuperscript{65} While providers supported the consent requirement, many commenters objected that it would interfere with a wide range of functions and activities, and create significant administrative burdens and difficulties in obtaining, tracking and administering the consents.\textsuperscript{66} The provider consent requirement was dropped for these and other reasons in the version of the Privacy Rule which became final in 2002,\textsuperscript{67} and is the version applicable today.

Under the current version of the Privacy Rule Covered Entities may use and disclose PHI for TPO purposes, excepting only psychotherapy notes, without individual consent.\textsuperscript{68} Any Covered Entity may, but is not required to obtain an individual’s consent to use or disclosure of information for TPO (“TPO consent”), and there is no regulatory standard for the form or content of TPO consents.\textsuperscript{69} A TPO consent, if obtained, is not effective as an authorization when that is required under other HIPAA standards.\textsuperscript{70}

\begin{footnotesize}
\begin{enumerate}
\item 2000 Rule at 45 CFR § 164.506(b).
\item 2000 Rule at 82648.
\item 2000 Rule at 82648 – 50.
\item 2000 Rule at 82650 – 51.
\item Id. at 14778 – 80,
\item Id. at 53208 – 211.
\item See 45 CFR § 164.506(a).
\item See 45 CFR § 164.506(b). “Psychotherapy notes” is a defined term which means “notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation” during a counseling session, and does not include “medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of . . . diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.” 45 CFR § 164.501.
\item 45 CFR § 164.506(b)(2).
\end{enumerate}
\end{footnotesize}
any studies of the question, no healthcare organizations are known to be using TPO consents based on HIPAA concerns. While individuals can ask that Covered Entities restrict the use and disclosure of their PHI they are not, with one limited exception, required to accept the request.71

HIPAA deals with non-TPO uses and disclosures in four ways.72

- Disclosures to the individual data subject are not only permitted, but required unless one of a few specifically defined exceptions applies.73 Under regulations to be finalized in the near future Covered Entities which maintain their PHI in electronic form will be required to provide it electronically upon request, and to transmit records to third parties upon the individual’s request as well.74

- For disclosures in facility directory listings and communications to those involved in an individual’s care, the individual must have some opportunity to opt out, not necessarily in writing.75

- No consent is required for mandatory and certain other disclosures to legal and governmental authorities, for organ and tissue donation, for research approved by an institutional review board or privacy board, and to avert threats to health and safety, subject in most cases to limitations or requirements of legal protection.76

- For all other PHI uses and disclosures, a written authorization signed by the individual is required.77 Authorizations must include specific “core” elements, and a set of required

71 See 45 CFR § 164.522.

72 For a detailed listing see Table 2 in the Consents Toolkit.

73 See 45 CFR §§ 164.502(a)(1)(i), .502(a)(2)(i), .524. This access requirement extends to “designated record sets,” defined as “a group of records maintained by or for a covered entity[,]” including medical and billing records of providers; enrollment, payment, claims adjudication and case or medical management records of health plans; and any other records used “in whole or in part . . . to make decisions about individuals.” See 45 CFR §§ 164.501, .524(a)(1). Access may be denied for a few types of records, under limited conditions. See 45 CFR §164.524(a)(2). See generally Dougherty and Washington, Defining and Disclosing the Designated Record Set and the Legal Health Record, 4 Journal of AHIMA 79 (April 2008) at 65-68.

74 See U.S. Department of Health and Human Services, Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed.Reg. 40868 (July 14, 2010) at 40923 – 24 (draft amendments to 45 CFR § 164.524(c)).

75 45 CFR § 164.510.

76 45 CFR § 164.512.

77 See 45 CFR § 164.508.
statements. With a couple of minor exceptions individuals cannot be required to enter into an authorization, and individuals may revoke an authorization at any time.

While HIPAA provides a baseline, many (probably most if not all) states have laws exceeding this baseline for consents in at least some situations. State consent laws have been reviewed extensively in other reports, and it is not our intention to repeat or update such research. However, “[v]ariations across states, in both legal and policy requirements, have made it difficult for organizations to determine, in the context of interstate electronic HIE, when appropriate disclosure requirements have been met that will permit the sharing of PHI.”

State laws in general can vary from requirements for consent in almost all non-emergency disclosures, to laws requiring consent for disclosure of only a few types of SHI. The most common pattern appears to be “No Consent” is acceptable for most disclosures which would be permitted under HIPAA, with some form of Opt-In or Opt-Out required for SHI, principally genetic, substance abuse, mental health, and HIV/STD information, with some states giving additional categories special protection.

Perhaps because of this variation over the HIPAA baseline, a recent study found that only 163 out of 199 HIOs surveyed were implementing at least some privacy policies which exceeded HIPAA requirements. This survey found that respondents were implementing consents as follows:

- Patient consent required to share clinical data deemed to be sensitive (e.g., mental health, STD, AIDS) with another provider for treatment purposes (62)

78 See 45 CFR § 164.508(c).
79 The exceptions are for entry into research-related treatment, for uses and disclosures related to the research; for health plan enrollment and eligibility determinations related to the individual, or underwriting or risk rating; and for health care provided solely for purposes of creating PHI for disclosure to a third party, for purposes of that disclosure. See 45 CFR § 164.508(b)(4).
80 45 CFR § 164.508(b)(5).
82 HISPC Intrastate and Interstate Consent Policy Options Collaborative, Final Report, supra note 2, at 1 – 2.
83 Id. at 3 – 2 – 3 – 5.
84 Id. at 3 – 8.
85 eHealth Initiative, supra note49 at 24.
86 Id.
• Patient consent required to share clinical information with another provider for treatment purposes (opt-in) (61)
• Patient consent required to share clinical information for healthcare operations purposes (31)
• Patient consent required to share aggregated or de-identified information for purposes other than treatment, payment, or healthcare operations (31)
• More stringent restrictions are in place for use and disclosure for research (31)
• Patient consent required to share information for payment purposes (30)

This kind of variability seems likely to pose significant challenges to sharing between (if not necessarily within) HIEs, and monitoring state laws is problematic. Any report on state laws is a snapshot of a short period of time, and it is not easy or inexpensive to track all relevant state law developments on a nationwide basis. While federal law also changes, the simple fact that there are so many states means that identifying and tracking all potentially relevant legislation, regulations, regulatory guidance and judicial interpretations presents a daunting burden.

A service which tracks such laws may ultimately be desirable for effective implementation of a robust NHIN, but is probably not needed for the practical resolution of consent issues for more limited interstate HIE. State law compliance may be a matter which can appropriately delegated to participating organizations on a state-by-state basis in many HIE arrangements. Where this kind of strategy is not implemented, however, tools are available to help participating organizations to identify consent-related laws. The identification and tracking of such laws might be assigned to an office or committee if there is a centralized HIO, or the identification and tracking of each states' laws might be delegated to one or more participating organization in each state.

5.2. Federalism and the Application of State Laws in Other States’ Territories

There are a number of possible solutions to state consent law variations. Model acts and uniform laws, interstate compacts and other types of agreement have all been cited and discussed, and have their advantages and disadvantages. One strategy which has not had much if any previous analysis, however, is delegation of state law consent compliance

87 Cf. Pritts et al., supra note 10, at 4 – 11.
88 See e.g. HISPC, Harmonizing State Privacy Law Collaborative, Roadmap: Analytical Framework and Collaborative Recommendations (March 31, 2009).
89 See e.g. Christiansen, Apgar and Melamed, supra note 57; Pritts et al., supra note 6; HISPC Harmonizing State Privacy Law Collaborative, Roadmap: Analytical Framework and Collaborative Recommendations, supra.
obligations to HIE participants on a state-by-state basis, so that each participant is obliged to comply only with the laws of the state in which it operates.  

This strategy is based on a fundamental principle of federalism: That no state has the authority to apply its laws to activities occurring in the territory of another state.

... The Commerce Clause ... precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State. In Southern Pacific Co. v. Arizona, 325 U.S. 761, 775 (1945), the Court struck down on Commerce Clause grounds a state law where the "practical effect of such regulation is to control [conduct] beyond the boundaries of the state . . . ." The limits on a State's power to enact substantive legislation are similar to the limits on the jurisdiction of state courts. In either case, "any attempt 'directly' to assert extraterritorial jurisdiction over persons or property would offend sister States and exceed the inherent limits of the State's power." Shaffer v. Heitner, 433 U.S. 186, 197 (1977).  

This includes laws attempting to impose penalties for conduct which is illegal in one state for actions in another state where the same conduct is not illegal.

This means, for example, that a physician practice in Indiana, a state which has relatively few consent requirements for treatment disclosures, may transmit information about a New York resident, a state which has much stronger consent requirements, to a hospital in Minnesota, which also has much stronger consent requirements, without complying with the consent laws of either New York or Minnesota. The Indiana practice must comply with Indiana consent laws, and cannot be penalized by New York or Minnesota for failing to comply with their consent laws.

This result seems contrary to the frequently cited choice of law principle that each state has an interest in protecting the interests of its resident, so that its law should be applied when one or more of its residents' interests may have been harmed. Under this principle it might be claimed that the Indiana practice's release of information about a New York resident without following New York consent requirements violated the New York resident's right to privacy as provided in New York law. However, recent U.S. Supreme Court caselaw prohibits this result.

The key case in this area is BMW of North America v. Gore. Gore, decided in 1996, is perhaps best known as the case in which the Court held that a punitive damages award of $2 million for

---

90 For multi-state enterprises, the following analysis will apply based on a state-by-state basis depending on the state in which a given its participating facility is operating.


93 State law information from HISPC Interstate Disclosure and Patient Consent Requirements Collaborative, Final Report, supra note2 at Section 3.

failing to disclose that a car had been repainted was “grossly excessive” and so unconstitutional, but did so in part by holding that punitive damages under one state’s laws could not be awarded based on activities in other states which may have been legal in those other states.

In particular, the damages award in Gore was based on evidence that the defendant, BMW, had failed to disclose that cars had been repainted in 983 transactions, 14 of them in Alabama, the state whose law was applied.95 The U.S. Supreme Court rejected the use of evidence of activities in other states as a basis for Alabama punitive damages:

No one doubts that a State may protect its citizens by prohibiting deceptive trade practices and by requiring automobile distributors to disclose presale repairs that affect the value of a new car. But the States need not, and in fact do not, provide such protection in a uniform manner. Some States rely on the judicial process to formulate and enforce an appropriate disclosure requirement by applying principles of contract and tort law. Other States have enacted various forms of legislation that define the disclosure obligations of automobile manufacturers, distributors, and dealers. The result is a patchwork of rules representing the diverse policy judgments of lawmakers in 50 States.96

... 

We may assume, arguendo, that it would be wise for every State to adopt Dr. Gore’s preferred rule, requiring full disclosure of every presale repair to a car, no matter how trivial and regardless of its actual impact on the value of the car. But while we do not doubt that Congress has ample authority to enact such a policy for the entire Nation, it is clear that no single State could do so, or even impose its own policy choice on neighboring States. ... 

We think it follows from these principles of state sovereignty and comity that a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors’ lawful conduct in other States. ... Alabama may insist that BMW adhere to a particular disclosure policy in [Alabama]. Alabama does not have the power, however, to punish BMW for conduct that was lawful where it occurred and that had no impact on Alabama or its residents. Nor may Alabama impose sanctions on BMW in order to deter conduct that is lawful in other jurisdictions.97

By the same token New York, for example, could not punish an Indiana physician practice which transmitted information about a New York resident to Minnesota from its own Indiana records without obtaining consent in compliance with New York law.

95 Gore, 517 U.S. at 564.
96 Id. at 568 – 70 (footnotes omitted).
97 Id. at 570 – 73 (footnotes omitted).
This analysis does suggest, however, that if a state wanted to ensure that its residents do not unknowingly lose privacy rights they have under state law when their information is transferred to a less-protective state, it might require some form of consent to interstate transfer, and/or that in-state organizations obtain agreement from out-of-state HIE participants to comply with the state’s requirements before transferring information out of state. In the former case the consent requirement could be anything from published notice to opt-in, opt-out or even directive. In the latter case the agreement might take the form of something like a HIPAA Business Associate Contract, or a 42 CFR Part 2 Qualified Service Organization Agreement. Either approach would come with some degree of additional burden on interstate HIE, but would also have the benefit of providing clearer rules to guide it.

5.3. Alcohol and Drug Abuse Treatment Program Records

42 CFR Part 2 defines specific treatment of patient information as it relates to alcohol and chemical dependency diagnosis and treatment. It is intended to regulate the privacy of patients with past or present alcohol and chemical dependency diagnosis and treatment, and is much more stringent than HIPAA and most state laws. “In sum, the information protected by [42 CFR] Part 2 is any information disclosed by a Part 2 program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a Part 2 program.”

Entities which must comply with 42 CFR Part 2 (“Programs“) include:

1. A program which is a federally assisted provider of alcohol or drug abuse diagnosis, treatment or referral for treatment. A program is considered federally assisted if it:
   a. Is authorized, licensed, certified, or registered by the federal government
   b. Receives federal funds in any form, even if the funds do not directly pay for the alcohol or drug abuse services; or
   c. Is authorized to conduct business by the federal government (e.g., certified as a Medicare provider, authorized to conduct methadone maintenance treatment, or registered with the Drug Enforcement Agency (“DEA“) to dispense a controlled substance used in the treatment of alcohol or drug abuse); or
   d. Is a facility in which diagnosis and treatment is conducted by the federal government

98 U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration and Office of the National Coordinator for Health Information Technology, Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (2010).

99 42 CFR § 2.11.
2. An entity which includes a “covered program.” A covered program exists when services are provided by a specialized unit or staff within a general medical facility (or “mixed use” facility) that includes alcohol and chemical dependency diagnosis, treatment and/or referral.

For-profit drug and substance abuse programs and private practitioners that do not receive federal assistance of any kind are not considered covered by 42 CFR Part 2. However, most drug and alcohol treatment programs are federally assisted, and most states provide special protections for information about individuals involved in alcohol and chemical dependency diagnosis and treatment. This means that even when 42 CFR Part 2 does not apply to a program or provider, a specialized state privacy law may. As a result many health care providers (e.g., hospitals, physicians, etc.) which are not required to adhere to 42 CFR Part 2 have adopted significantly more stringent privacy requirements for alcohol and chemical abuse-related information out of concern about potential state law exposures.

Unlike HIPAA, which generally permits disclosure of PHI without consent or authorization for the purposes of treatment, payment, or healthcare operations (“TPO”), 42 CFR Part 2 requires patient consent for almost all disclosures of covered information. 42 CFR Part 2 is so stringent in its limitations on disclosure of covered information that even a court-issued subpoena is not sufficient to authorize disclosure of covered information without the individual’s consent. 42 CFR Part 2 also requires all authorizations for release of covered information to include a re-disclosure clause so that (for example) when a patient authorizes a covered provider to release covered information to the patient’s health plan, the health plan is required to obtain the patient’s authorization prior to re-disclosure to another individual or entity. An authorization must also specifically identify the third party individual or entity allowed to view or use the covered information, and cannot be made generally available to categories of entity (e.g. “any hospital treating this individual”).


102 Id.

103 See U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment, The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs (June 2004) at 4 – 7.

104 42 CFR § 2.32.

105 42 CFR § 2.2.
The principal exception to the authorization requirement is for disclosures to a qualified service organization (“QSO”). A QSO is a person or organization that:

- Provides services to a covered program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting or other professional services or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy (similar to a Business Associate pursuant to HIPAA); and
- Has entered into a written qualified service organization agreement (“QSOA”) with a covered program where the party acknowledges that in receiving, storing, processing or otherwise managing covered patient records from the program, it is fully bound by 42 CFR Part 2; and
- Will work through the courts to block any efforts to access covered patient records, except as permitted by 42 CFR Part 2.

No patient authorization is required for covered information disclosure to a QSO. These requirements create significant issues for HIE participation by entities subject to 42 CFR Part 2, particularly if covered information is stored by parties other than the Program, including (for example) information made available through a record locator service (“RLS”), which would be covered by 42 CFR Part 2 if it identified the individual with the Program.

At the initiation of any HIE involving 42 CFR Part 2-protected information, the originating Program would have to ensure it had obtained an appropriate authorization, identify any party authorized to receive the information, and provide a re-disclosure provision to accompany the disclosure. Therefore, if the information were forwarded to a RLS serving point-to-point HIE, either the repository operator would have to be a QSO, or the re-disclosure provision would have to bind the repository operator. Either way, prior to re-disclosure of the information to a requesting party, such as another provider, the repository operator would have to obtain a new authorization from the individual, confirm the disclosure was within that authorization, and provide a re-disclosure provision which the receiving party would in turn have to comply with before any future re-disclosure of the information.

This kind of re-disclosure “chain” may be difficult to implement and manage, which may be why behavioral health providers tend not to participate in open HIE arrangements. If and when they do participate, information from covered providers must be segregated from general PHI, subject to specialized access controls to ensure any disclosure is within authorization and accompanied by a re-disclosure provision.

---

106 42 CFR § 2.11.
107 42 CFR § 2.12(b)(4).
42 CFR Part 2 therefore requires an opt-in consent process administered by the originating Program as gatekeeper, and managed across all subsequent re-disclosures by other parties. Its requirements do not prevent the exchange of covered information via electronic HIE, but do require the segregation of that data to the extent that only intended recipients of the health data can view or use the data. And after data is transmitted, its recipient also becomes a gatekeeper, because it is also required to obtain authorization from the individual who is the subject of the data before re-disclosing the data.

The burdens of these requirements may be alleviated if the HIE operator has a QSOA with the Program. If a QSOA is implemented no authorization is needed for disclosure of information to the QSO, so the HIE operator could maintain a repository or RLS including the protected information, to administer on behalf of the Program. Each disclosure by the HIE operator as QSO, however, would have to be subject to confirmation of patient authorization, including identification of the recipient as specifically authorized. A HIO might therefore support information storage, receiving and reviewing requests for disclosures to third parties (managing the authorization process) on behalf of gatekeeping Programs.

5.4. Family Educational Rights and Privacy Act

Health and education operate as two distinct and separate enterprises on both the federal and state levels despite extensive and ongoing efforts to implement a wide range of health policies through school systems. Very little meaningful work has been done to facilitate the electronic sharing of student health information between the education system and the health system in the context of electronic record systems and the provision of healthcare services. Consequently, patient permission issues also have not been extensively examined.

Sharing student health data with the healthcare system is a complex task, given the size and scope of the two sectors and variety of organizations and organizational arrangements each presents. The complexities presented by institutional factors are only increased by the federal and state laws which apply to each, in overlapping but non-coordinated ways. The difficulty of addressing these issues may partially explain the lack of work in this area.

Federal law in this area parallels HIPAA; the equivalent privacy law for educational institutions is the Family Educational Rights and Privacy Act (FERPA),108 which governs educational records. Both laws have generated complex federal regulations that impose minimum requirements for protecting personally identifiable information. At the same time, both regulatory regimes provide organizations with substantial discretion in sharing information.109

---

109 It may be helpful to remember that health and education issues were once the province of a single federal agency. Federal policymakers made a conscious decision to separate these policymaking functions. The Department of Health, Education and Welfare came into existence April 11, 1953. In 1979, the Department of Education Organization Act was signed into law, providing for a separate Department of Education. HEW became
The complexity of the regulations implementing both sets of federal privacy requirements have provoked cautious interpretations by educational and healthcare entities out of strong concerns over legal liabilities. These responses, in turn, have created barriers to the legitimate sharing of information within each sector. Consequently, attention to the sharing of personally identifiable information electronically between educational and healthcare organizations in the context of health information exchanges is rare.

FERPA was enacted in 1974 to protect the privacy of student education records, including health records generated and maintained by a covered institution.\footnote{20 U.S.C. § 1232g; 34 CFR Part 99. See Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records (November 2008).} The law, which has been amended many times since then, applies to all schools that receive funds under an applicable program of the U.S. Department of Education. According to the Departments of Education and Health Human Services, that means “virtually all public schools and school districts and most private and public postsecondary institutions, including medical and other professional schools.”\footnote{U.S. Departments of Education and of Health and Human Services, \textit{Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records} (November 2008).}

The rights granted by the law are given to parents concerning their children’s educational records. Those rights transfer to the student when he or she reaches 18 or attends a school beyond the high school level. Students, who have had these rights transferred to them, are referred to as “eligible students.”

Generally, FERPA requires parents and eligible students to give permission to release information from the student’s education records, subject to the following exceptions:

- To school officials with legitimate educational interest;
- To organizations conducting certain studies for or on behalf of the school;
- To appropriate officials in cases of health and safety emergencies;
- To other schools to which a student is transferring;
- To specified officials for audit or evaluation purposes;
- To accrediting organizations;
- To appropriate parties in connection with financial aid to a student;
- To comply with a judicial order or lawfully issued subpoena; and
• To state and local authorities, within a juvenile justice system, pursuant to specific State law.112

Schools also may disclose "directory" information such as a student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance without permission. However, schools must inform parents and eligible students of the directory information and allow them a reasonable amount of time to request that the school not disclose this information.

Schools must notify parents and eligible students annually of their rights under FERPA. The manner in which this notification is handled is up to the educational institution.

Uncertainty over the Application of FERPA

Substantial confusion in a number of areas – including the definitions of an educational record and educator — have stymied data sharing within and among educational institutions. The need for clear guidance on sharing student information was recognized by the Education Department in its draft National Education Technology Plan 2010. It noted “Clear guidance on how schools can collect and share data without compromising student safety and anonymity would empower educators and learners to take full advantage of emerging technologies and tools without fear of violating FERPA.”113

The draft report is worth quoting in detail as its conclusions will sound remarkably similar to the challenges facing healthcare in the electronic health record area:

Two types of challenges to realizing the vision of sharing data across systems are technical and regulatory. On the technical front, multiple student data systems, the lack of common standards for data formats, and system interoperability pose formidable barriers to the development of multi-level assessment systems.

For example, student and program data today are collected at various levels and in various grain sizes to address different needs in the educational system. State data systems generally provide macro solutions, institution-level performance management systems are micro solutions, and student data generated by embedded assessment are nano solutions. Providing meaningful, actionable information that is collected across multiple systems will require building agreement on the technical format for sharing data.

On the regulatory front, regulations such as the Family Educational Rights and Privacy Act (FERPA) serve the very important purpose of protecting the rights of individuals but also can present barriers to data sharing and the improvement of

112 20 U.S.C. § 1232g; 34 CFR § 99.31

education through research. Many of the barriers to research and data sharing posed by FERPA in its original form were reduced or eliminated through a 2008 revision of the act. Still, varying interpretations of FERPA requirements and differences in district and state policies have made data sharing a complex, time-consuming, and expensive process.

Reducing the technical and regulatory barriers to data aggregation and sharing would facilitate efficient use of data that are already being collected to make judgments about students’ learning progress and the effectiveness of education programs.114

The confusion and uncertainty over FERPA were openly revealed in government reports investigating the tragic Virginia Tech killings. A Presidential commission said in its 2007 report:

**Critical Information Sharing Faces Substantial Obstacles**: Education officials, healthcare providers, law enforcement personnel, and others are not fully informed about when they can share critical information on persons who are likely to be a danger to self or others, and the resulting confusion may chill legitimate information sharing.115

In response to the killings, the Education Department issued a regulation on Dec. 9, 2008 that clarified when school officials could share information without permission. In the preamble of the proposed rule, the department said it was modifying the regulation in response “to changes in information technology and address other issues identified through the Department’s experience administering FERPA, including the need to clarify how postsecondary institutions may share information with parents and other parties in light of the tragic events at Virginia Tech in April 2007.”116

Although there may be improved coordination in handling students in emergencies, uncertainty remains. Access to non-health records is proving to be an ongoing challenge today.117

---

114 Id.


117 A thorough examination of the effectiveness of the regulations have been are outside the scope of this project. It is worth noting that a 2006 survey of school guidance counselors found that one of the most challenging ethical dilemmas faced by these professionals involved student confidentiality, dual relationship with faculty, parental rights, and acting on information of student danger to themselves or others. Bodenhorn, *Exploratory Study of Common and Challenging Ethical Dilemmas Experienced by Professional School Counselors*, Professional School Counseling 10.2 (2006)
Reconciling FERPA with HIPAA

Despite a joint effort by HHS and the Department of Education to clarify how HIPAA and FERPA interacted in November 2008 and the Education Department’s new FERPA rules, trying to sort out how and when to share information remains a complicated process that may discourage the sharing of information between the two sectors. 118

To illustrate the complexity – and thus the concern -- generated when HIPAA and FERPA must be reconciled, we present some common scenarios and key points to consider in determining which set of regulations govern:

• An Institution which is a HIPAA covered entity but treats students and non-students:
  — Students’ records would be treated as “education records” or “treatment records” so they are governed by FERPA.
  — Non-students’ records would be treated as “protected health information” so they would be governed by HIPAA.

• A third-party healthcare provider is covered by HIPAA and provides services to students on school grounds but not “under contract” or “control” of the educational institution:
  — The records could be both PHI Education Records because they are created and maintained by the third party.
  — If the healthcare provider is “under contract with” or “controlled” by educational institution, then the records would be governed by FERPA, regardless of the location where services provided.

• A student health clinic is operated by an educational institution and engages in HIPAA covered electronic transactions:
  — The clinic could be HIPAA covered entity.
  — Records on students could be “education records” or “treatment records” that are excluded from PHI under HIPAA.

• An educational institution requested to disclose treatment record to a third-party covered healthcare provider:

The Society for College and University Planning, in a July 2007 report on trends in higher education noted that FERPA is being used by some institutions as a reason for not sharing individual student data, even though it was never meant to impede educational research. See Society for College and University Planning, Trends in Higher Education (July 2007) at 9.

118 It is important to note that HIPAA and FERPA are not the only laws that operate at the intersection of health and education. A good overview of the legal environment is found at Centers for Law and the Public’s Health: A Collaborative at Johns Hopkins and Georgetown Universities A CDC Review of School Laws and Policies Concerning Child and Adolescent Health, 78 Journal of School of Health 69 (February 2008).
The records could be “education records” or “treatment records” while in control of educational institution.

The data could be PHI when in control of the third-party covered entity.

• A student is a patient at a university hospital which is available to the general population, not just students:

  — Assuming the university hospital engages in covered transactions, it would be considered a HIPAA Covered Entity.
  
  — The medical records would be PHI because it is not providing services to the individual as a student.

• An individual is both a student and an employee of an educational institution, which is considered a HIPAA Covered Entity. FERPA would govern, unless

  — The records related solely to an individual in his or her capacity as an employee.
  
  — If the records were viewed solely as employee records, then HIPAA would still not necessarily apply.\(^{119}\)

These scenarios suggest an environment in which educational institutions must be alert and well-informed to appropriately handle the use and disclosure issues affecting student records.

Complicating the analysis is the Individuals with Disabilities Education Act (IDEA).\(^{120}\) Under this law, healthcare providers are often part of a team of educators who develop an individualized education plan for a disabled student. These records are arguably covered by FERPA as education records. However, determining whether an educator is a healthcare provider operating under HIPAA or IDEA can be confusing and inserts another level of complexity into the possibility of exchanging student information between educational and healthcare entities.

IDEA focuses on children’s educational needs in the context of their physical, mental, emotional, developmental, and learning disabilities. Under IDEA, a disability is defined as "mental retardation, hearing impairments (including deafness), speech or language impairments, visual impairments, serious emotional disturbance, orthopedic impairments, autism, traumatic brain injury, or other health impairments or specific learning disabilities.”\(^{121}\)

IDEA is intended to give all children a right to a public education that emphasizes special education and related services designed to meet their unique needs and prepare them for further education, employment, and independent living. Federal enforcement of IDEA is also

---

\(^{119}\) Sharing Student Health Information under the New FERPA Final Rules, Melamedia, LLC Audio Seminar (February 18, 2009).


\(^{121}\) IDEA § 308(a).
overseen by the Education Department and state and local boards of education, and intersects with section 504 of the Rehabilitation Act because students entitled to special education services generally qualify as disabled students under that law.

The Intersections of Health and Education

Despite this complex data environment, U.S. policy over many years has consistently dealt with a wide variety of childhood health issues within the nation’s educational system under the auspices of public health. In many cases, the issue of patient permission does not arise because of statutory and regulatory exceptions for public health surveillance and response.

The strategy of tapping into the education system to confront health issues is not expected to change in the foreseeable future. Consequently, new opportunities to foster more efficient data sharing between the education and health sectors can be expected.

A good example of this intersection is the campaign against childhood obesity. Health programs that are relevant to this campaign and are or may be implemented within schools include:

- Child Nutrition and Women and Infant Care (WIC) Reauthorization. The law encompasses several food programs as well as child and maternal health issues;
- The Americans with Disabilities Act;
- Pregnancy Discrimination Act;
- Social Security Act, which provides disability insurance;
- Deficit Reduction Act, which gives states the flexibility to reform their Medicaid programs; and
- No Child Left Behind Act, which address risk factors for disease.122

In addition, many other programs rely on the participation of the educational system to address substance abuse, mental health issues and a variety of other health issues affecting children.

The Patient Protection and Affordable Care Act of 2010 (the healthcare reform act, “ACA”) explicitly involves schools in the provision of healthcare in educational settings.123 ACA creates a grant program to expand school-based health centers (“SBHCs”) to offer comprehensive primary health services. These services will include treatment for physical conditions but mental and substance abuse issues. The centers must be integrated into the school environment and preference will be given to centers with a large population of children eligible for medical assistance.

---


For the purposes of this Report the key provision is that these services require parental or guardian consent consistent with federal, state and local laws, including HIPAA.124 The new grants and programs provide an opportunity for developing a system for obtaining permission to share medical records among education and healthcare organizations, subject to a caveat that because the program is aimed at medically underserved child populations, efforts to create patient permission programs will have to consider strategies for attracting permissions from those populations that are not medically underserved. At the same time nothing in the law waives or supersedes FERPA, HIPAA or other privacy law requirements.

**Healthcare Reform as an Opportunity**

The importance of obtaining patient permissions may be magnified as federal and state policymakers will face the task of implementing provisions in recently enacted healthcare reform legislation that provides grants for creation of SBHCs to increase student access to preventive health services.125

The new grants for school-based health centers under the healthcare reform laws provide an opportunity for building more effective bridges with healthcare in regard to consent. At the beginning of each school year, students typically are given a variety of permission forms for parents to sign.

Testing healthcare authorizations in this environment might usefully demonstrate methods for coordinating care and information exchanges between the school-based healthcare organizations and the healthcare system at large. A pilot program might, for example, address the issue of duplicative forms, which create both administrative burdens and confusion. Steps toward resolution of this issue would be useful for both educational and healthcare organizations that have to deal with this kind of issue on a regulator basis.

Such a pilot – regardless of its specific purpose – also could test various approaches to obtaining electronic consents from parents. For example, back-to-school nights or days dedicated to parent-teacher conferences could provide an opportunity to establish a process by which parents could be educated about the utility of electronic records and the benefits of providing consent for healthcare services.

This initiative could be tied directly to the new school-based healthcare services encouraged by the healthcare reform law. School systems that participate will have to engage in some education and outreach efforts to publicize the new services, and it might prove an effective vehicle for encouraging EHR-based consents for an already disadvantaged population that could benefit the most from electronic sharing of health information.

**Addressing College and University Systems**

124 See ACA § 399Z-1(c)(2)(C)(vi).

125 ACA § 399z-1(b).
Opportunities exist for institutions educating eligible students on the college level as well. This young population is accustomed to electronic interfaces and already sees some of the benefits. Student clinics in these settings also could provide a setting for testing approaches to obtaining consents that cover both FERPA and HIPAA and ease the sharing of health information.

Like parents in the K-12 system, eligible students at the college level are presented with a variety of permission forms to sign. Consequently, the same type of pilots testing authorizations for multiple purposes might prove useful. As important, discussions among healthcare professionals and educators in creating pilot and demonstration project would provide the basis for establishing trust and understanding that could create the foundation for better health data flows.

6. The Problem of Diverging Standards

This Report has focused primarily on obtaining permission, as deemed appropriate and as required by law, prior to the exchange of an individual’s health data and strategies to assist in increasing interstate HIE. As has been noted in more than one Case Study, interstate and intrastate technology barriers may represent at least an equal challenge in expanding HIE within and between states in terms of connectivity and reasonably ensuring specific permissions required or desired are adhered to across the exchange.

Mayo and Kaiser both raised the concern that, even when agreement has been reached within a state and between states over the form of consent and the granularity of that consent, absent a common technical framework, HIE will be significantly obstructed, especially if different consent requirements proliferate at the state level.

ONC, of course, is charged with identification and management of national HIT policies and technical standards, and is the logical lead organization to drive nationwide (if not necessarily federally-mandated) consent standards. ONC projects have already put substantial work into this area, including development of many of the reports referenced in this Report and relevant technical standards.

Mayo and Kaiser in particular noted that NGA and ONC can and should play a key role as states move forward with their HIE efforts, with NGA as an important representative of states and state needs. Between the two organizations, the likelihood of adopting HIE practices and networks that can communicate with each other across state lines and with NHIN are vastly improved.

Technical challenges do not exist only on the state level, but also at the local level. A number of intrastate HiOs have been formed and at this point interconnectivity or interoperability is becoming a significant issue for some. Also, depending on the individuals a provider or healthcare organization serves, the provider or healthcare organization may be required to implement or develop differing interfaces to transfer health data from one local HIE to another.
when serving the healthcare needs of the same individual. CareSpark noted that its ability to work with another HIE has been impeded by the other HIE’s failure to adopt commonly accepted standards. This raises the question whether a failure to address these issues on a nationwide basis would risk creating “exchange pockets” that cannot effectively share and transmit data.

There is also a challenge – or opportunity – in trying to connect any HIE to educational institutions. Most school-based health centers are still primarily paper-based. College and university health centers in some cases are often connected electronically to other college or university systems, perhaps especially for universities with medical schools serving the student as well as general population. As HIEs are formed at least some pilots should be encouraged to connect to school-based care facilities (primary, secondary and higher education), and try to develop common rather than divergent standards and practices.

Technology should be implemented (or if necessary developed) which can accommodate differing laws and changes in those laws. The same technical kind of technical mechanisms which are effective for consent processes under HIPAA should be adaptable to more stringent state law, to drug and alcohol records under 42 CFR Part 2 and to FERPA-protected educational records.

7. DISCUSSION OF REPORT FINDINGS AND TOOLS

The nationwide baseline standard for consents, as articulated by HIPAA, is “No Consent” for treatment, payment and health care operations (TPO) disclosure, combined with specific Opt-out or Opt-in processes for sensitive health information. In some states there may be consent standards for disclosure of information which is not sensitive health information but is otherwise protected health information requiring HIE participants in those states to default to the higher state requirements. A few states may also have laws which apply to redisclosure of information received under some conditions, as does 42 CFR Part 2.

Under the U.S. federal system, however, higher state standards do not apply to organizations that participate in the same HIE from other states, unless they agree to them contractually. This applies to the HIE arrangements reviewed in the Case Studies as follows:

- **Enterprise HIOs**, where there are legally integrated sets of companies doing business in more than one state, may be subject as a legal unit to the various consent laws of the different states, or may determine that uniform organization-wide standards are

---

126 This kind of contractual agreement would only be enforceable by other parties to the contract, not as a matter of the other state’s law.
preferable for compliance and risk management purposes. Enterprises therefore tend to default to the requirements that vest the most control in individuals.\textsuperscript{127}

- **Standard HIO** may or may not determine that it is appropriate to require a uniform consent standard, reconciled to default to the state or federal legal standard which vests the most individual consent control. Defaulting to the most stringent consent law may be desirable particularly if a repository or other centralized node is implemented where information from multiple states may be stored, as a matter of compliance and risk management, and to help ensure public trust. The governing body or other controlling stakeholders may determine that adherence to a higher standard is an appropriate requirement for participation in the HIE.

- **Utility HIOs** do not need to (though it may) impose a uniform consent standard on participants. The HIE operator does not attempt to determine or impose specific consent standards, but makes Gatekeepers responsible for compliance as a matter of both policy and for specific disclosures.

The dominant model for obtaining consent delegates responsibility to Gatekeepers, entities which are usually but not necessarily health care providers, and which have a direct relationship to the individuals providing consent. Gatekeepers are necessarily the source not only of information content for “downstream” HIE participants, but also for “Consent Metadata” indicating any conditions to consent applicable to redisclosure of the information disclosed. Non-Enterprise HIOs do not tend to have direct individual relationships or administer consents, but may provide mechanisms for communicating Consent Metadata. In general, it is not clear that robust mechanisms for communicating Consent Metadata have been widely implemented.

Under the concepts developed above, the findings of this report may be summarized as follows:

1. The specific allocation of consent policy development authority and responsibility depends on the governance and architecture of the specific HIE arrangement. To the extent HIE participants are integrated under a unified legal umbrella, such as an Enterprise HIE, their risks may be most appropriately managed by a central authority. Likewise, to the extent a HIE operator assumes responsibility for managing disclosure transactions, it may be appropriate for that operator to establish consent obligations for such transactions, as in a Standard HIO. In more decentralized arrangements, such as Utility HIEs using point-to-point architecture, it may be not only more practical but more appropriate to expect participating organizations to be responsible for their own consent compliance in using the HIE.

2.

\textsuperscript{127} This analysis depends materially on the specific details of the affiliated entities and their corporate and contractual relationships, so this determination needs to be made by specific analysis of the enterprise in question.
3. Recipients of health information are only required to use and disclose information received through HIE in accordance with the law that applies to the recipient, including applicable federal law reconciled with the law of the state where they are located. Additional redisclosure limitations may be imposed by agreements such as business associate contracts, qualified services organization agreements or HIO agreements, or may be a condition to receipt by electronic agreement or by law under the 42 CFR Part 2 redisclosure provisions. Downstream recipients are not otherwise required to comply with the law of the state in which the health information originated.

Both Gatekeepers and downstream redisclosers are subject to HIPAA’s various consent requirements if they are Covered Entities or Business Associates. Since most if not all entities participating in HIE are one of these or the other, HIPAA provides a national baseline for consent requirements.

4. Many state laws vest greater control of health information in individuals than HIPAA does, especially with respect to sensitive health information such as AIDS/HIV status, genetic information, and behavioral health status. Similarly, 42 CFR Part 2 provides for a higher degree of control for drug and alcohol treatment, consistent with the sensitivity of such information.

Recommendations

1. State agencies, and state-supported public-private initiatives, should develop guidance and standards for intra- and interstate HIE to help organizations best meet the requirements under both federal and state law. This can be done by developing and providing clear guidance in HIE projects and initiatives, which can help resolve consent obstacles to HIE in the short term pending longer-term policy solutions.

2. HIOs should develop authoritative guidance for Gatekeepers, based upon standards and analyses developed by state agencies or broader stakeholder groups which include state participation.

3. If sensitive health information is intended to be included in HIE, consent processes should be implemented which communicate and enforce permission limitations when they are more stringent than HIPAA limitations. Except where 42 CFR Part 2 or rarely a state redisclosure law applies, such limitations may not be enforceable in the absence of a contract between the parties, so contractual enforcement mechanisms (such as a HIO agreement) should be considered. Alternative solutions, if feasible may include access controls which prevent disclosures for non-permitted transactions.

4. If highly granular access controls are not available, it may be appropriate to exclude transactions involving sensitive health information at the HIO participation level, or on a case-by-case information disclosure transaction basis at the operational level.
5. There needs to be better sharing of information between health care organizations and educational institutions, this, however, is prevented by a lack of focused activity or projects in this area. In order to avoid or minimize the growth of incompatible healthcare and educational consents systems and standards it would be desirable to develop initiatives and projects to bring the two systems together.

There is no single model for HIE consent, and choices in this area will continue to have to balance the values of administrative efficiency and clinical improvement against patient control and public trust. The balance will vary depending on the governance and architecture of the HIE, and state and regional preferences.

It is useful to consider consents as a process including documentation of individual notice and intent rather than the documentation itself, and to analyze consent issues in terms of the policy choices vesting more or less individual control over disclosures and the contractual and technical mechanisms which may be used to enforce those choices. This type of analysis will not eliminate consent variations as an obstacle to HIE, but should allow for a more efficient, governance- and architecture-specific analysis of what choice means in a given HIE arrangement. This in turn can allow for better specification of consent-related responsibilities, and less confusion about legal issues.

At some point, a uniform nationwide HIE consent model may be adopted by the federal government, or by coordinated action of the states. The process for developing and implementing such a solution would be time-consuming, and it is not clear what set of consent processes would find broad public support. Variations in state law represent variations in public sentiment or established health care practices and expectations and variations in federal law itself indicate that some variation is probably inevitable and even desirable.

In the absence of a national uniform solution, consent processes for HIE will have to adapt flexibly to variations in law and preference. Operational strategies based on a process perspective which recognizes the distribution of consent functions among HIE participants can only help all stakeholders manage such adaptation.