THE CURRENT STATE OF SHARING BEHAVIORAL HEALTH INFORMATION IN HEALTH INFORMATION EXCHANGES

Prepared by National eHealth Collaborative for

SAMHSA-HRSA
Center for Integrated Health Solutions

NATIONAL COUNCIL FOR BEHAVIORAL HEALTH
MENTAL HEALTH FIRST AID
Healthy Minds. Strong Communities.

Substance Abuse and Mental Health Services Administration
SAMHSA
www.samhsa.gov 1-877-SAMHSA-7 (1-877-726-4727)

www.integration.samhsa.gov

SEPTEMBER 2014

SAMHSA-HRSA CENTER FOR INTEGRATED HEALTH SOLUTIONS

The SAMHSA-HRSA Center for Integrated Health Solutions (CIHS) promotes the development of integrated primary and behavioral health services to better address the needs of individuals with mental health and substance use conditions, whether seen in specialty behavioral health or primary care provider settings. CIHS is the first "national home" for information, experts, and other resources dedicated to bidirectional integration of behavioral health and primary care.

Jointly funded by the Substance Abuse and Mental Health Services Administration (SAMHSA) and the Health Resources and Services Administration HRSA, and run by the National Council for Behavioral Healthcare, CIHS provides training and technical assistance to community behavioral health organizations that received SAMHSA Primary and Behavioral Health Care Integration grants, as well as to community health centers and other primary care and behavioral health organizations.

CIHS's wide array of training and technical assistance helps improve the effectiveness, efficiency, and sustainability of integrated services, which ultimately improves the health and wellness of individuals living with behavioral health disorders.

ACKNOWLEDGEMENTS

Special thanks to the following people for their generous assistance in the preparation of this white paper:

- *Michael Lardieri, Vice President, Health Information Technology and Strategic Development, National Council for Behavioral Health*
- *Laura Kolkman, President, Mosaica Partners*
- *Renee Popovits, Principal Attorney, Popovits & Robinson*
- *Linn Freedman, Partner and Leader Privacy & Data Protection Group, Nixon Peabody LLP*
- *Jeff Chang, Project Manager, PCE Systems*
- *Wende Baker, Executive Director, eBHIN*
- *Janet Terry, Privacy Officer, Quality Health Network*
- *Dave Scanga, Legal Counsel, Quality Health Network*
- *AJ Peterson, General Manager, Care Connect, Netsmart*
- *Scott Weinstein, Office of the Chief Privacy Officer, Office of the National Coordinator for Health Information Technology*
- *Maureen Boyle and the Health Information Technology team, Division of State and Community Assistance, Center for Substance Abuse Treatment, Substance Abuse and Mental Health Services Administration (SAMHSA)*

SAMHSA-HRSA
Center for Integrated Health Solutions

1701 K Street NW, Suite 400

Washington, DC 20006

202.684.7457

integration@theNationalCouncil.org

www.integration.samhsa.gov

TABLE OF CONTENTS

WHY INTEGRATION OF PHYSICAL AND BEHAVIORAL HEALTH INFORMATION IS IMPORTANT

Consider these statistics:

- 45.6 million American adults (nearly one in five) suffer from a mental illness, 11.5 million of whom have a serious mental illness[i]
- 8.0 million Americans have a substance use disorder.[ii]
- 29% of all people with a physical health condition also have a behavioral health condition; 68% of adults with a mental illness have at least one medical condition.[iii]
- People living with a serious mental illness are nearly three times more likely to have diabetes and three times more likely to have chronic respiratory disease, compared to the general population.[iv]
- People living with a serious mental illness have 3.5 times higher rates of emergency room visits, four times the rate of primary care visits, and five times the rate of specialist visits.[v]
- Behavioral health medications tend to have more drug-to-drug interactions[vi] and can have physical health-related side effects.
- Average life expectancy for those with serious mental illness ranges from 13 to 30 years less than the rest of the population.[vii]
- Studies show that people with a physical health condition live longer when treated for their behavioral health issues.[viii]
- Mental illnesses are one of the five most costly conditions in the United States[ix]

Now, consider what happens when much of those individuals' behavioral health information —medical history, lab results, medication lists, treatment plans — is locked out of electronic exchange. The lack of this information in a person's health record can put them at risk, potentially leading a provider to prescribe treatment that compromises the person's safety, disrupts their recovery, or otherwise negatively affects their overall well-being.

People requiring both physical and behavioral health services have a unique need for integrated care, which requires potentially complicated coordinated information sharing among diverse providers and treatment settings. Increasingly, primary care physicians are treating both physical and behavioral conditions, which can greatly help in care coordination efforts. However, in cases where people with more severe conditions must see multiple providers, the risk that they will receive only fragmented and inconsistent episodic care increases (e.g., people with depression are three times more likely to be noncompliant with their medical treatment regimens[x]), which contributes to a shorter life expectancy.

Using electronic health information exchange (HIE) to facilitate necessary care coordination could go far in improving both the patient experience and their treatment outcomes. Unfortunately, this is happening in very few places across the nation. There are several reasons for this "digital divide" between behavioral health and physical health data exchange explored in this paper.

Compelling evidence for the benefits of integrated care supported by health IT:

78% of respondents in a 2013 survey of primarily behavioral health providers by Behavioral Healthcare magazine felt that the integration of substance use, medical, and mental healthcare are very important in improving health outcomes.

In a survey by the Colorado Regional Health Information Organization, more than 97% of participants agreed that the ability to securely exchange behavioral health and physical/medical health information electronically across providers will add value to the healthcare system.

CURRENT LIMITATIONS

"Sensitive" Health Data and the Law

To understand and address the barriers to widespread, integrated behavioral and physical HIE, it is necessary to first define what is considered "sensitive health information." It is also helpful to examine the maze of overlapping federal and state laws governing the disclosure and exchange of this information.

The National Committee on Vital and Health Statistics (NCVHS) is responsible for making recommendations to the government on the Health Information Portability and Accountability Act (HIPAA). One of the recommendations NCVHS made in 2010 was for the U.S. Department of Health and Human Services (HHS) to explore the use of technology to help manage "sensitive health information." Part of these recommendations included a refinement of legally defined categories of "sensitive" information. The NCVHS recommendation letter outlines the following categories:[xi]

CATEGORIES DEFINED IN FEDERAL LAW

GENETIC INFORMATION

The federal Genetic Information Non-Discrimination Act of 2008 (GINA) prohibits employers and certain insurers from "request[ing], requir[ing], or purchas[ing]" genetic information. Healthcare providers are regularly requested to provide medical records for a number of legitimate employment and insurance purposes. In order to respond to these requests, records custodians must segregate genetic information that comes under the GINA definition from other parts of the electronic medical record when transmitting records... [Some] [s]tate law definitions may be more limited [than GINA]...

PSYCHOTHERAPY NOTES

Under the [HIPAA] Privacy Rule, a covered entity must obtain authorization for any use or disclosure of psychotherapy notes, with certain limited exceptions...HIPAA defines psychotherapy notes as notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. [NOTE: According to 45 CFR Part 164.501, the definition of psychotherapy notes excludes any summary or notes regarding: diagnosis, functional status, treatment plans, symptoms, prognosis, progress to date, medication prescription and monitoring, counseling sessions start and stop times, the modalities and frequencies of treatment furnished and the results of clinical tests. All of this information can be legally exchanged under the HIPAA Privacy Rule without additional patient consent.]... Therefore, in order to avoid violating the law when disclosing records...it would be necessary for custodians of the medical record to create a separate psychotherapy notes section in the electronic health record to appropriately manage this part of the medical record...

SUBSTANCE ABUSE TREATMENT RECORDS

Federal regulations governing the confidentiality of alcohol and substance abuse treatment records [commonly referred to as "42 CFR Part 2"] impose "restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program." Such a "program" might be an individual care provider, stand-alone facility, unit within a general medical facility, or medical staff of a larger medical facility who hold themselves out to provide alcohol or drug abuse diagnosis, treatment, or referral for treatment. [NOTE: This is an important point. Not all substance use treatment information is subject to 42 CFR Part 2: jurisdiction is based upon the type of facility within which the information is originally stored, not the type of information itself.] These regulations also prohibit the redisclosure of information that originated as substance abuse treatment records; in other words, the protections for these records attach to the [Part 2] record and not the custodian, as under HIPAA. Especially for those medical staff or units within a larger care facility where medical record systems are integrated, the capability to identify and separately manage substance abuse records is critical to proper compliance with the law. But, due to the prohibition on redisclosure, all entities that might possibly receive substance abuse treatment records are at risk of violation if they do not have the capability to identify these records separately. In the meantime...facilities who do not have this capability avoid integrating the records of substance abuse patients into their systems, requiring more than one system for maintaining records, and **denying this population of patients other advantages of electronic medical records and health information exchange.** (Emphasis added)

HITECH ACT CASH PAYMENTS

Under the HITECH Act, patients may require that a provider withhold from a health insurance company information about any service for which the patient has paid in full out of their own pocket. In order to do so, records custodians will need to be able to separate out items or services for which the provider has been paid out of pocket in full.

CATEGORIES DEFINED IN LAWS OF MANY STATES

STATE LAW PROTECTIONS FOR HIV INFORMATION, OR OTHER INFORMATION REGARDING SEXUALLY TRANSMITTED DISEASES

Many state laws give special protections to information concerning testing, diagnosis or treatment for the Human Immunodeficiency Virus (HIV) or other sexually transmitted diseases…In order to comply…custodians of health records may need to segregate information that comes within the different parts of this statutory definition…

STATE LAW PROTECTIONS FOR MENTAL HEALTH INFORMATION

Most states give some kind of special protection to mental health information…State statutes vary in the definitions of mental health information to which they accord special protection, as well as in the contexts to which these protections apply. Accordingly, it is important to identify the types of information that might be included within this category, the contexts in which disclosure limitations might apply, and how the particular types of information might be identified for purposes of disclosure limitations in these various contexts…

STATE LAW PROVISIONS REGARDING ACCESS TO INFORMATION IN THE RECORDS OF CHILDREN AND ADOLESCENTS

State laws differ regarding the rights of adolescents and their parents to the health records of adolescents…Adherence to [these] restriction[s] may require separate handling of records [for] children over 14. Indeed, many of the categories of sensitive information discussed in this letter may require separate handling in the case of adolescents in some states.

Without the capacity for separate management…custodians may be forced to withhold information from health information exchanges when they would not otherwise do so, because they lack the capacity to differentiate the sensitive portion of the record…**In such cases, patients lose the benefits of both EHRs and exchange, and other uses of the information (such as for public health or quality improvement) may also be frustrating.** (Emphasis added)…

ADDITIONAL POTENTIAL SENSITIVE CATEGORIES OF INFORMATION

MENTAL HEALTH INFORMATION (other than as found in HIPAA psychotherapy notes or state law definitions)

Dissemination of information about mental health diagnosis and treatment may pose significant risks to patients, and most people regard it as highly sensitive…[H]owever, [it] may be difficult to identify [mental health information] as it will be scattered throughout many parts of a medical record, as well as across many providers' records and might require the use of advanced natural language processing for identification…In addition to the statutory requirements in state law for mental health, and psychotherapy notes at the federal level, NCVHS believes the category of mental health information includes:

- Psychiatric diagnoses
- Descriptions by patients of traumatic events
- Descriptions or analyses of reports by the patients of emotional, perceptual, behavioral, or cognitive states

Except as required by state law, NCVHS does not believe the following "critical health information" should be included in additional definitions of "mental health information" because of its importance in many contexts:

- Medication lists
- Allergies and non-allergic drug reactions
- Dangerous behavior within medical settings
- Information from medical notes, tests, procedures, imaging or laboratory studies performed in a mental health facility that is not related to the mental health treatment but that would otherwise be considered medical information…

SEXUALITY AND REPRODUCTIVE HEALTH INFORMATION

Information about sexuality and reproductive history is often very sensitive...NCVHS believes the following elements comprise the category of Sexuality and Reproductive Health Information:

- Sexual activity
- Sexual orientation
- Gender dysphoria and sexual reassignment
- Abortion, miscarriage, or past pregnancy
- Infertility and use of assisted reproduction technologies
- Sexual dysfunction
- The fact of having adopted children ...

CONSIDERATIONS APPLYING TO ENTIRE RECORDS

- NCVHS has identified three circumstances in which the entire record might be deemed "sensitive"...
- First, in cases of domestic violence or stalking...
- Second, there are cases in which the identity of a patient being treated is sensitive...
- Finally...the records of adolescents may require special treatment..."

At the federal level, the HIPAA Security and Privacy Rules protect against inappropriate access to sensitive information on mental health, HIV status, reproductive care, developmental disabilities, genetics, and domestic violence, and the HITECH Act further strengthens those protections.

42 CFR Part 2

Substance use treatment information is specifically held to a more restrictive federal expectation. This category of sensitive health information is subject to the Federal Confidentiality of Alcohol and Drug Abuse Patient Records Regulations, which is often referred to as "42 CFR Part 2." The laws around substance use treatment were promulgated with the altruistic intent of helping to combat some of the discrimination and related repercussions (including criminal prosecution) that can prevent people from seeking treatment.

In cases specific to veterans served by the U.S. Department of Veterans Affairs, 38 USC Section 7332 goes one step further, requiring that information relating to drug abuse, alcoholism or alcohol abuse, infection with HIV, or sickle cell anemia can be disclosed only with the specific written consent (VA Form 10-5345) of the veteran.

42 CFR Part 2 Disclosure Checklist

Determining when 42 CFR Part 2 is applicable and how to legally access information about substance use treatment requires practitioners to work through a series of questions.

What programs are covered by 42 CFR Part 2?

42 CFR Part 2 applies to any program that

1) holds themselves out as providing, and provides alcohol or drug abuse diagnosis, treatment, or referral for treatment; AND

2) is regulated or assisted by the federal government.

What information is protected?

42 CFR Part 2 "imposes restrictions upon the disclosure and use of alcohol and drug patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program." (42 CFR § 2.3(a)) The restrictions on disclosure apply to any information disclosed by a Part 2 program that "would identify a patient as an alcohol or drug abuser" (42 CFR §2.12(a) (1)) Even acknowledging that an individual is or was a patient at a 42 CFR Part 2 facility is a breach of the regulations.

How can protected information be shared?

Information can be shared with written consent. A written consent form requires nine specific elements outlined in the regulation (42 CFR § 2.31(a)).

At the state level, many jurisdictions have enacted legislation holding the exchange of differing types of sensitive health data to an even higher standard than those of HIPAA or 42 CFR Part 2. Michigan Health Information Network's (MiHIN) Comparative Analysis Matrix[xii] and the Illinois Consent Law Comparison[xiii] demonstrate this type of legal complexity.

While 42 CFR Part 2 is limited to substance use data held by a recognized treatment facility, many healthcare providers and HIEs are either unaware that not all sensitive health information is held to the same standard, are operating in a state with more stringent privacy regulations than HIPAA and/or 42 CFR Part 2, or are technically unable to separate out sensitive information in the patient record.

HIPAA Privacy Rule vs. 42 CFR Part 2 A Comparison of Disclosure Provisions:

42 CFR PART 2	HIPAA PRIVACY RULE
Programs may not use or disclose any information about any patient unless the patient has consented in writing (on a form that meets the requirements established by the regulations) or unless another very limited exception specified in the regulations applies. Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure.	HIPAA permits uses and disclosures for "treatment, payment and health care operations," as well as certain other disclosures without the patient's prior written authorization. Disclosures not otherwise specifically permitted or required by the privacy rule must have an authorization that meets certain requirements. With certain exceptions, HIPAA generally requires that uses and disclosures of personal health information be the minimum necessary for the intended purpose of the use or disclosure.

Limited Exceptions for 42 CFR Part 2 Disclosure without Consent:

- Medical emergencies
- Child abuse reporting
- Crimes on program premises or against program personnel
- Communications with a qualified service organization of information needed by the organization to provide services to the program
- Public Health research
- Court order
- Audits and evaluations

The Substance Abuse and Mental Health Services Administration (SAMHSA) conducted a thorough comparison of 42 CFR Part 2 and HIPAA, available at: www.samhsa.gov/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf

Professional Ethics

Further complicating the sensitive health information space, some professional codes of ethics establish specific requirements for patient confidentiality. For example, the American Psychological Association's Ethical Principles of Psychologists and Code of Conduct indicate that psychologists should disclose confidential information without the consent of the patient "only as mandated by law, or where permitted by law for a valid purpose, such as to (1) provide needed professional services; (2) obtain appropriate professional consultations; (3) protect the client/patient, psychologist, or others from harm; or (4) obtain payment for services from a client/patient, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose."[xiv]

The American Psychiatric Association's (APA) position on patient confidentiality is also relatively cautious. Section 4, paragraph 1 of the APA Principles of Medical Ethics: "Psychiatric records, including even the identification of a person as a patient, must be protected with extreme care… Growing concern regarding the civil rights of patients and the possible adverse effects of computerization, duplication equipment and data banks makes the dissemination of confidential information an increasing hazard. Because of the sensitive and private nature of the information with which the psychiatrist deals, he or she must be circumspect in the information that he or she chooses to disclose to others about a patient." Section 4, paragraph 2 further states: "A psychiatrist may release confidential information only with the authorization of the patient or under proper legal compulsion. The continuing duty of the psychiatrist to protect the patient includes fully apprising him/her of the connotations of waiving the privilege of privacy…"[xv]

In 2010, the APA issued a Position Statement on Confidentiality of Computerized Records that foreshadows remedies being pursued today (emphasis added):

> ***"Patients should be able to benefit from the potential improvements in the delivery and quality of care with electronic health records, without being forced to relinquish the privacy and confidentiality of their personal health-related information.*** Approaches to electronic health record access should consider the diverse settings in which electronic health records will be used, including their use in emergency and other acute settings where rapid access to medically necessary information is essential. Such approaches should also consider that patients have a broad range of needs, preferences and abilities to provide informed consent about the implications of electronic record access. At the very least, computerized records should give patients as much control over their information as they have with paper-based records. In addition, computerized records should not force patients to choose between either making all or none of their information available. Electronic health record design and implementation should leverage technology to give more flexible approaches to access for sensitive information. As health information technology continues to advance and evolve, the complexities and potential consequences of computerized records make it essential for psychiatrists to be aware of the implications for their patients and advocate for a culture of confidentiality and respect for patients."[xvi]

A study published in the Journal of the American Medical Association on August 19, 2013 surveyed 3,336 adults about their preferences and concerns related to sharing their health information electronically. The study found that:

"Participants cared most about the specific purpose for using their health information… The user of the information was of secondary importance, and the sensitivity was not a significant factor. These preferences should be considered in policies governing secondary uses of health information."

Unfortunately, the available HIE technology limits people receiving medical or behavioral health services from being able to identify and segment specific parts of their record. We are all limited to sharing all or nothing.

Technical Barriers Preventing Integrated Data Sharing

Right now, most behavioral health information exchange must occur in an "all or nothing" format. In other words, most EHRs do not yet have the capability to sift through data elements and specifically redact or restrict sharing of specific information. This has become a significant obstacle for HIEs, given 42 CFR Part 2's consent requirements. However, some HIEs have developed technical solutions allowing them to include behavioral health information.

Standards for data segmentation are needed to address this issue in a way that will make granular data exchange interoperable. Data segmentation refers to the process of sequestering from capture, access, or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.[xvii]

Technically, the challenge is to come to consensus on a standard method that will enable the implementation and management of disclosure policies that originate from the patient or are required by law. This must be done in an interoperable manner within an electronic HIE environment, so that individually identifiable health information may be appropriately shared for: 1) patient

treatment and care coordination; 2) third party payment; 3) analysis and reporting for operations, utilization, access quality, and outcomes; 4) public health reporting; and 5) population health, technology assessment, and research.[xviii] A variety of collaborative state and federal efforts are working on this challenge, most notably the Data Segmentation for Privacy (DS4P) Initiative of the Office of the National Coordinator for Health Information Technology's (ONC) Standards & Interoperability Framework.[xix] ONC is also reviewing the feasibility of a voluntary certification process for behavioral health EHRs.

Another concern is the segmented data fields themselves. Most exchange in the HIE environment is currently happening through the production and sharing of a comprehensive continuity of care document (CCD). There is broad concern among the behavioral health community that the standard CCD does not include fields required for it to be useful in a behavioral health context. There is an ongoing push from behavioral health leaders to address this through both Health Level Seven International (HL7) and the ONC Standards & Interoperability Framework.

Business Barriers Preventing Integrated Data Sharing

According to Claudia Williams, Director of the ONC State HIE Program, there are 38 states that want to "integrate primary care, acute care, and behavioral health even more than through payment reforms."[xx] However, for providers' business operations and their affiliated HIEs, there are several sticky issues in the way of success.

One issue is the exclusion of most behavioral health providers in the Meaningful Use Incentives Program. Because of limited resources and a lack of financial incentives, there has been a slower rate of adoption of health IT in the behavioral health and substance use treatment communities. Behavioral health providers face the same challenges that medical providers faced when adopting EHRs, such as lack of financial resources to purchase and maintain systems, lack of IT workforce to implement and maintain systems, and lack of training support. The National Council for Behavioral Health and others are leading active efforts to address this inequity.

A second issue is related to the inability of HIEs to process granular consent data. This requirement, in effect, negates a 42 CFR Part 2 facility's ability to fully participate in exchange, leading to a negative incentive for providers and facilities that operate with sensitive data to participate in an HIE. This is an issue for most HIEs across the country. This is unfortunate, because the behavioral health community is a potentially significant customer base, especially for those HIEs that may be struggling to find ongoing financial sustainability.

Third, exchange technologies are often expensive. Even if HIEs were able to bring behavioral health providers to the table and encourage the integration and sharing of physical and behavioral health information, it is unlikely that many behavioral health providers operating in the safety net would be able to afford the various technical interfaces and applications needed to exchange sensitive data securely and confidentially.

Trust Barriers Preventing Integrated Data Sharing

Violations of 42 CFR Part 2 are subject to a fine of $500 for the first case and not more than $5,000 for each subsequent case. Further, while one might expect that enforcement of 42 CFR Part 2 would be assigned to SAMHSA, instead that role is assigned to Department of Justice, requiring the attention of a U.S. Attorney. These penalties might ordinarily be regarded as a slap on the proverbial wrist, but consider the rapid-fire volume of data exchange happening in an HIE environment; "subsequent cases" could inadvertently multiply quickly and without immediate notice. They may also be subject to additional penalties under individual state law. Shaun Alfreds, Chief Operating Officer from Maine's HealthInfoNet, summed up the issue in one sentence: "[A] single large scale breach would put us out of business."

Choosing to err on the side of caution and protection of patient confidentiality, many HIE initiatives are currently restricting information sharing to only physical health data. Some of these restrictions are due to more stringent state laws. A striking example of this is the MetroChicago HIE, which serves a population of 9.4 million people. In testimony before the Data Security and Privacy Committee of the Illinois Health Information Exchange Authority, MetroChicago's legal counsel Marilyn Lamar explained why MetroChicago HIE has chosen to exclude some sensitive information from the HIE:

"...[R]estrictions imposed by laws written long before electronic health information exchange was even contemplated have caused the MetroChicago HIE to ask its participants to not transmit mental health and developmental disability information. This may ultimately result in the exclusion of a significant amount of data as an increasing percentage of the population takes medications for behavioral health problems. The current IMHDDCA [Illinois state law regarding sensitive information], designed with the best of intentions to protect the interests of a vulnerable population, may actually work against the individuals it was designed to protect when it is applied in the HIE context. ***Unless it is changed, the current law will prevent behavioral health patients from receiving the benefits that an HIE will provide to other patients. Behavioral health patients will wind up on the wrong side of the digital divide."***[xxi] *(Emphasis added)*

42 CFR Part 2 Compliant Consent Forms: The "To Whom" Issue

The consent form requirements in 42 CFR Part 2 include some granular consent areas that most HIEs are not yet technically equipped to handle. Several HIEs, led by CurrentCare in Rhode Island, are working with SAMHSA on challenges presented by 42 CFR Part 2. One of the most difficult areas on the specified consent form isthe "To Whom" section. Because most HIEs do not yet have the capability to restrict or segregate data by individual provider, and because they are rapidly adding exchange participants, they have suggested to SAMHSA that it be appropriate to accept "all providers involved in my care" or "treating provider" instead of limiting consent to a continually changing list of "providers in the HIE as of the date the form was signed."

As we have seen, meaningful choice about where their information is going and presumably how it will then be used or redisclosed is one of the most important concerns for patients. SAMHSA guidance on the "to whom" issue has maintained that a 42 CFR Part 2-compliant consent form must include the names of individuals or organizations who will be the recipients of Part 2 data. According to SAMHSA's 2010 Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange, "The purpose of this requirement is to ensure that patients are sufficiently informed about the disclosures that will be made under the consent. Many individuals throughout the country still do not have computers or access to the Internet, and many AHIO affiliated health care providers do not have the resources to provide patients with access to the Internet at the HIO providers' offices. Thus, Part 2 consents should identify, by attachment if necessary, all the HIO affiliated members that are potential recipients of the Part 2 data." [xxii]

This is the issue remaining before coming to full consensus on the new standardized multi-state consent form developed through the SAMHSA-HRSA Center for Integrated Health Solutions (CIHS) over the past year.

Nine Required Elements of a 42 CFR Part 2 Compliant Consent Form:

1. The specific name or general designation of the program or person permitted to make the disclosure.
2. The name or title of the individual or the name of the organization to which disclosure is to be made.
3. The name of the patient.
4. The purpose of the disclosure (i.e. treatment, payment, research...).
5. How much and what kind of information is to be disclosed.
6. The signature of the patient or other person authorized to sign in lieu of the patient.
7. The date on which the consent is signed.
8. A statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer.
9. The date, event or condition upon which the consent will expire if not revoked before.

42 CFR Part 2 Restrictions on Redisclosure and Use of Sensitive Patient Data

Each disclosure made with the patient's written consent must be accompanied by the following written statement:

"This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2). **The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent** of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug use patient."

ENVIRONMENTAL SCAN OF CURRENT SENSITIVE HEALTH INFORMATION EXCHANGE

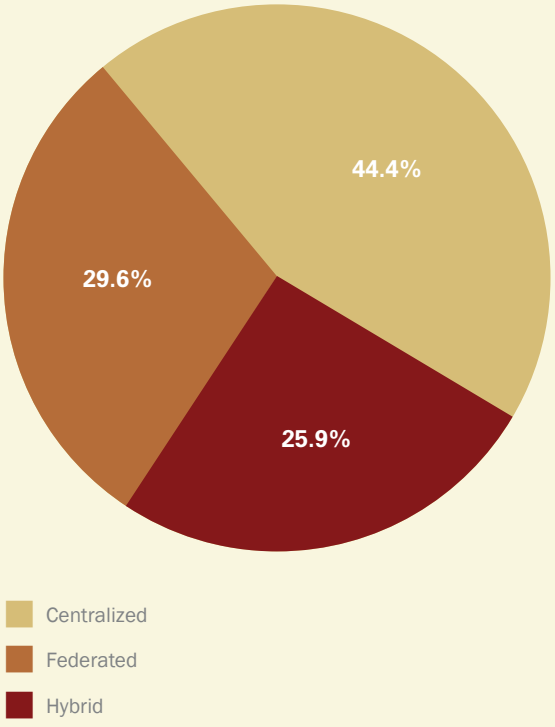
NeHC Survey of HIEs

In September 2013, National eHealth Collaborative (NeHC) surveyed 135 HIE initiatives (including public, private and enterprise HIEs) nationwide to identify the current level of HIE-enabled sensitive and behavioral health data exchange. They sought information on data exchange models, consent policies (opt-in, opt-out or hybrid), consent management mechanisms, and whether they are currently or plan to share various types of sensitive data.

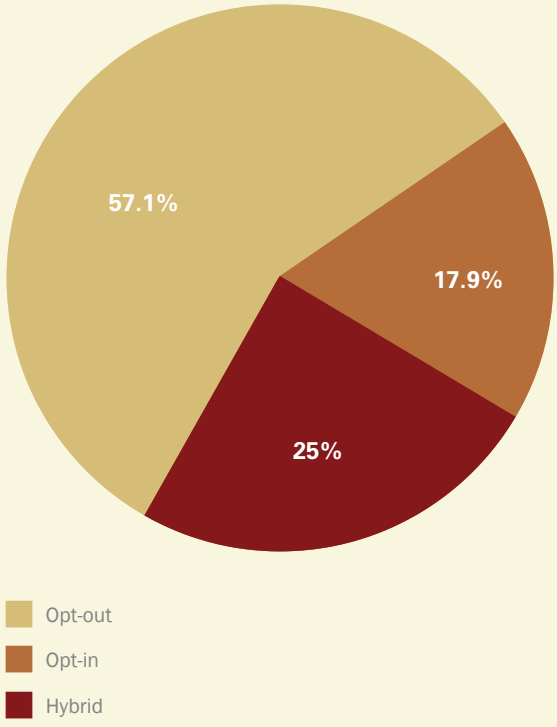
Twenty-eight production-level HIEs responded to the NeHC survey. The results indicate that many HIEs are still early in the process of developing systems to securely exchange behavioral health data. A large percentage of respondents indicated an interest in engaging in this type of exchange in the future. Only three HIE initiatives reported that they were not planning to implement electronic consent management mechanisms. Interestingly, 68% of respondents reported that their state had information disclosure laws that are stricter than HIPAA.

The NeHC survey findings also provided evidence that HIEs are increasingly using direct secure messaging as a trusted option for transporting sensitive data, especially data covered by 42 CFR Part 2. When asked, "Are you sharing sensitive health data that is subject to 42 CFR Part 2 (information related to substance use treatment)?," the number of HIEs that indicated that they were planning to exchange was equal to the number that indicated that they were not planning to exchange this data. However, upon review of the comments, it becomes clear that many are already exchanging this data through direct secure messaging, and that it is viewed as a trusted alternative mechanism for exchanging patient data that would otherwise have been locked out of exchange.

What is your HIE's data exchange model?

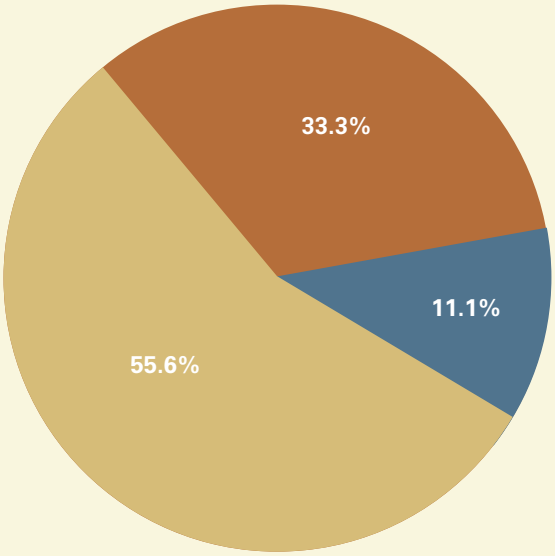


What is your HIE's consent model?

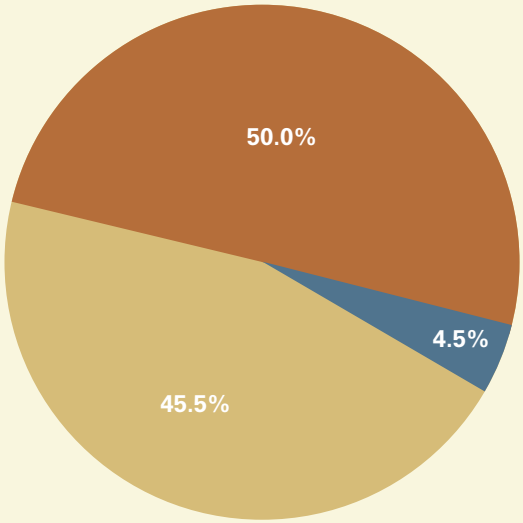


1. Hybrid, or dual, opt-in and opt-out consent models means that an HIE operates on an opt-in policy (i.e. patient must consent in writing before information is shared) for behavioral health information simultaneous with an opt-out policy (i.e. medical data is shared unless patient gives written prohibition) for all physical health data.

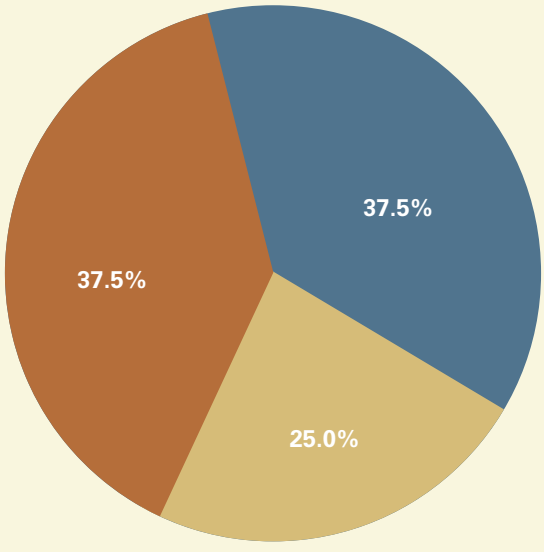
Does your HIE have a mechanism to handle consent management electronically?



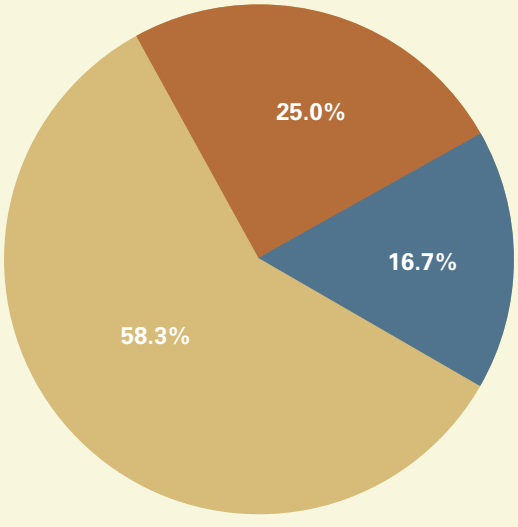
If your HIE cannot manage behavioral health consents electronically, are you providing direct secure messaging service to behavioral health providers?



Are you sharing sensitive health data that is subject to 42 CFR Part 2 (information related to substance use treatment)**?**



Are you sharing sensitive health data that is NOT subject to 42 CFR Part 2 (information related to mental health, reproductive health, HIV status, domestic violence, developmental disability)**?**



Which HIEs successfully exchange sensitive health data? How are they accomplishing this given the broad differentiation in legal protections and significant technical issues?

The following case studies demonstrate how some HIEs are already playing a critical role in coordinating behavioral healthcare. Not every case study profiled is able to actively share all types of behavioral health data. However, each case study does present a set of attributes that provides valuable insight for organizations looking to pursue this area of exchange.

Health Information Exchange in Behavioral Healthcare

In 2012, CIHS led a program to support sharing of health records among behavioral health providers and primary care providers through a state HIE. Five state HIE sub-awardees were charged with developing the infrastructure necessary to support the exchange of sensitive health information and the development or adaptation of HIE systems within that infrastructure. These HIE sub-awardees worked to determine barriers to inclusion of behavioral health information within the state HIE, identified technology and policy solutions for compliance with federal and state confidentiality regulations and — because they identified the primary challenge around technical capacity to be consent management — jointly developed a standardized multi-state consent form template that is computable in an HIE environment. [NOTE: Wording in the "To Whom" section of the Sample 42 CFR Part 2 Compliant Consent Form is still considered a barrier that requires clarification.] Prior to this program, no state HIEs were sharing behavioral health information through the HIE. Since the writing of this report, several states have begun to share mental health and substance use information through the HIE.

Here we outline the accomplishments and challenges of the five state grantees. For a full description of the initiative, plus a variety of resources, including sample forms (e.g. the multi-state consent form under consideration), toolkits, communications templates, and other materials go to www.integration.samhsa.gov/operations-administration/hie.

GRANTEE: Rhode Island Quality Institute

Rhode Island Quality Institute (RIQI) runs CurrentCare, the first state HIE to implement full integration of physical and behavioral health data exchange. Rhode Island is a fully opt-in state; their consent policy was codified in law by the Rhode Island Health Information Exchange Act of 2008. CurrentCare takes an all-or-nothing approach to health data exchange. Using a uniform authorization form, by joining CurrentCare, patients consent to the sharing of all of their health information, including that related to behavioral health and substance use treatment. CurrentCare has been successful thus far in establishing a trust relationship with their patients, as evidenced by a 90% opt-in rate for all patients that are approached to join the HIE.

Like all HIEs, CurrentCare must abide by HIPAA and 42 CFR Part 2. They do this by segregating Part 2 patient information from other patient records. When a provider logs on to CurrentCare to see a patient's record, they are presented with two tabs. One of the tabs provides access to information covered by HIPAA rules, including physical and mental health data; the other tab is specifically labeled as containing Part 2 information. When clicking on this tab, the provider is presented with the legal prohibition on redisclosure of the information they are about to access. They must read the 42 CFR Part 2 redisclosure statement and attest for a second time to having a treatment relationship with the patient before any sensitive data is displayed.

So far, all of Rhode Island's community mental health organizations and two of the Part 2 programs in the state have signed up to participate with CurrentCare and use the standardized consent form to enroll their patients. CurrentCare segregates all data received from these organizations behind the Part 2 tab data.

GRANTEE: Kentucky Health Information Exchange

The Kentucky Health Information Exchange (KHIE) will be the second state HIE to actively exchange behavioral and physical health data together. The KHIE team created a modified multi-state consent form to be used by state mental health hospitals and Cabinet for Health and Family Services contracts for mental health and alcohol and substance use services. Many community mental health centers in Kentucky are currently receiving lab results via push of a CCD from KHIE. Because many of Kentucky's mental health centers treat all data as subject to 42 CFR Part 2, KHIE is working with its technology vendor Netsmart to add 42 CFR Part 2 language either into the CCD or by a tag on individual records.

As a grantee, Kentucky also developed an extensive provider toolkit for use in recruiting new participants as well as an easy-to-use patient education document. In conjunction with the written toolkit, KHIE collaborated with the University of Kentucky's continuing education program to develop four video training modules that include the option for continuing education credit.

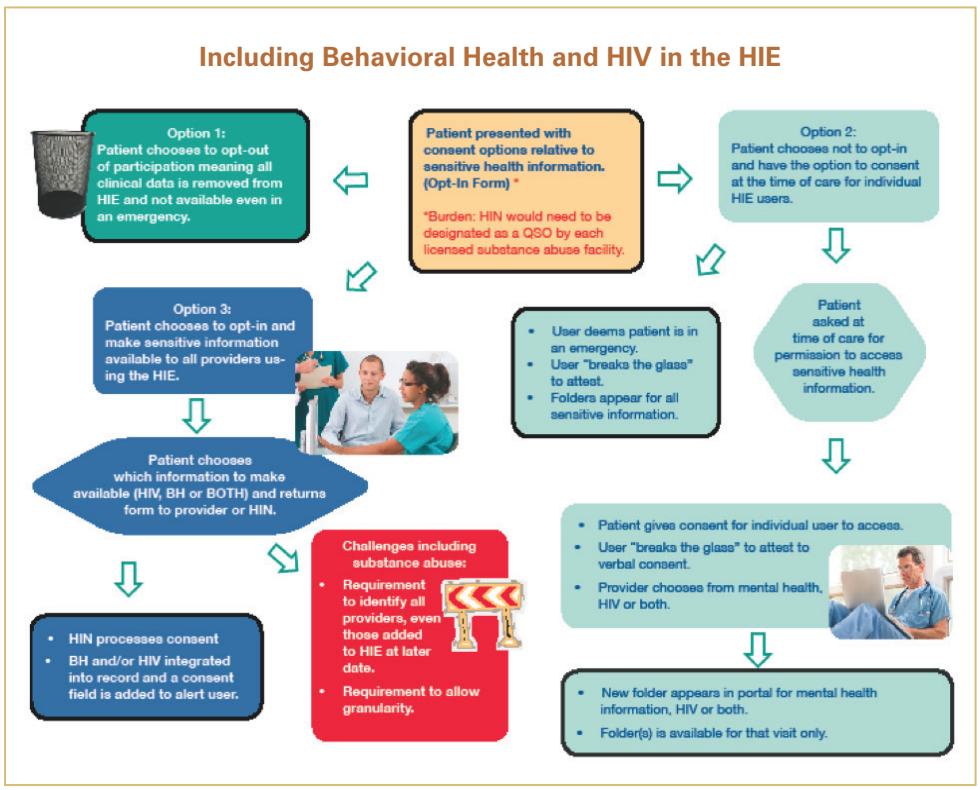
GRANTEE: HealthInfoNet

Maine's HealthInfoNet is a mature statewide HIE that is active in the campaign to reduce the stigma of mental health disorders. Through this and other work, they have gained an understanding of the concerns of Maine's residents around behavioral health information sharing.

HealthInfoNet developed a creative, focused strategy for facilitating the consent and exchange of behavioral health information. One of the first data integration milestones for HealthInfoNet was to advocate for a change in Maine State Law 1331 that allowed patient-level behavioral health information to be shared in the state.

HealthInfoNet now offers four different consent options: 1) do nothing – data is not shared outside of an emergency situation, 2) share all data, 3) share all data with a named provider during a visit, or 4) opt out of exchange entirely. For substance use treatment information, HealthInfoNet determined that the unresolved "to whom" issue around the 42 CFR Part 2 consent requirements made inclusion of that data too risky for error so they currently exclude it from exchange.

HealthInfoNet, as part of their grant program, also convened the Behavioral Health Information Technology Hanley Strategic Action Taskforce facilitated by the Daniel Hanley Center for Health Leadership to gather recommendations on how to best integrate behavioral with physical health. Over the past year, they brought together a behavioral health consortium to expand the local CCD, develop new bidirectional interfaces, offer a direct secure messaging solution and develop a new set of educational communications for consumers and providers.



GRANTEE: Oklahoma Health Information Exchange Trust (OHIET)

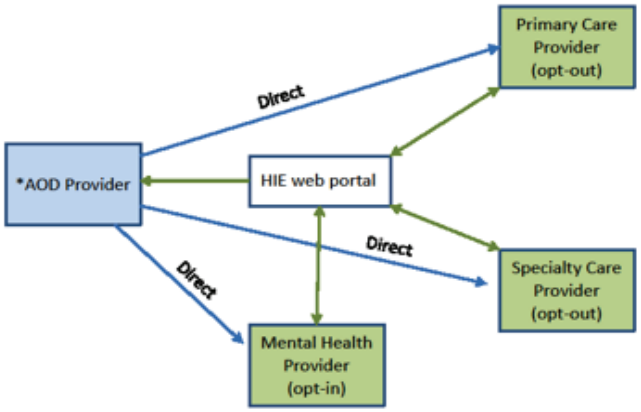
Behavioral health providers have been involved with the Oklahoma Health Information Exchange Trust (OHIET) since they began HIE planning in 2004.

OHIET developed a statewide voucher program to discount the cost for a provider to join an Oklahoma HIE. The voucher program was two-tiered: Tier 1 supported providers with web portal access and direct secure messaging services. Tier 2 supported providers that were able to connect to an HIE via their EHR. Thus far, OHIET has funded 152 direct connections and 365 clinical connections from 27 behavioral health providers statewide.

Substance use treatment or alcohol or other drug (AOD) treatment providers were eligible for Tier 1 voucher funding, providing them with the ability to see a patient's physical health records through the HIE portal, which improves the standard of care for substance use clients.

Of note, OHIET published a guideline for participants that recommended substance use treatment records should still only be shared using direct secure messaging until 42 CFR Part 2 is revised or the HIE is able to implement the technical ability to filter segmented data through participant EHRs.

Behavioral Health Information Exchange in Oklahoma



*AOD information will be shared through Direct. AOD providers can access clients' primary care information through HIE web portal.

GRANTEE: Illinois Health Information Exchange

Illinois behavioral health providers have been included in governance of the Illinois Health Information Exchange (ILHIE) since they were named in the 2010 Medicaid reform legislation that originally authorized the HIE, however, ILHIE is not yet exchanging much behavioral health data. Some ILHIE users are exchanging sensitive data using direct secure messaging protocols.

The primary roadblock to behavioral health information sharing in Illinois is an especially strict state law regarding consent for the exchange of mental health records, regardless of origin or location. A strong contingent of leaders and stakeholders in Illinois has come together to advocate for a change in the law to accommodate the electronic exchange of sensitive information.

As part of their grant, the Illinois HIE team conducted consumer outreach and opinion collection, and created consumer and provider-facing education resources. They created a toolkit that includes educational materials, a template consent form, and easy-to-use instructions for completion of the form. ILHIE also developed an HIE Readiness Assessment that they distributed to behavioral health providers and facilities to prepare them to become active exchange partners.

Highlights from the CIHS HIE Project

Illinois	Changed state mental health law to be similar to HIPAA Provided Direct Secure Messaging addresses to behavioral health providers
Kentucky	Began to utilize the national 42 CFR compliant consent Form template across all behavioral health providers in KY Developed on line CEU courses on data privacy and HIE. Available to anyone here: www.cecentral.com/node/745
Maine	Began sharing mental health data via HealthInfoNet the state HIE Developed a Consumer Education packet which can be utilized as a framework by other HIEs
Oklahoma	Provided direct Secure Messaging addresses to behavioral health providers across the state who are sharing mental health and substance information with medical providers via Direct Secure Messaging protocols
Rhode Island	First statewide HIE to share mental health and substance use information and physical health information through the statewide health information exchange

Other State HIE initiatives

CORHIO Behavioral Health and HIE Project

In April 2012, Colorado Regional Health Information Organization (CORHIO) released the findings from a multi-pronged project to identify issues preventing the exchange of behavioral health data.

CORHIO first undertook a comprehensive review of state and federal laws and regulations regarding behavioral health information sharing. Two possible barriers to sharing health information identified were 42 CFR Part 2 and the Disclosure of Confidential Communications clause of the Colorado Mental Health Practice Act. CORHIO worked with a variety of healthcare stakeholders to amend the Mental Health Practice Act clause to align Colorado statute with federal law. Aside from federally assisted substance use treatment programs, existing laws and policies no longer create a barrier to appropriate sharing of behavioral health information. Both behavioral and physical health providers are covered under HIPAA and practice under the same set of laws and regulations in Colorado.

CORHIO then facilitated a series of community meetings throughout the state to gather input from stakeholders on opportunities, concerns, and priorities for including behavioral health information in HIE. The results of this effort show that the behavioral health community in Colorado is supportive of better information sharing across care settings. Indeed, the strongest recommendation to come out of this project is to begin sharing behavioral health information today.

Other recommendations included:

- Involve the behavioral health community in statewide health information exchange leadership – starting today.
- Endorse a broader, statewide health integration agenda to promote better coordinated, less fragmented care.
- Develop a communication and outreach plan that supports education for all stakeholders regarding HIE and targeted education for physical health professionals to help them work better with the behavioral health community.
- Support revisions to public policy to address barriers to sharing information and partnering with key constituencies, including advocating for a revision to restrictive federal substance use treatment program regulations.
- Modify CORHIO's Health Information Exchange (HIE) operations to develop a granular consent model and enable consumer access to treatment data available within the exchange.

CORHIO is making an effort to onboard behavioral health organizations as participants in the HIE. The organization recently announced that 20 additional facilities have signed up to join the CORHIO HIE and begin the technical development work necessary to start accessing patient information.

Electronic Behavioral Health Information Network

The Electronic Behavioral Health Information Network (eBHIN) is one of two known HIEs focused primarily on the secure exchange of behavioral health data. eBHIN has brought together a diverse group of stakeholders to govern and enable a growing network that is making the coordination of behavioral and physical healthcare easier, safer, and more efficient for the people of southeast and western Nebraska. eBHIN is not a statewide HIE.

eBHIN uses a centralized data repository with standardized patient record exchange that supports an opt-in consent policy. To participate in the HIE, patients must give consent that allows both the primary behavioral health provider and any other provider in the network to access their data. eBHIN currently has an opt-in rate of approximately 75% and is seeking to expand its offerings statewide.

The eBHIN platform is HIPAA and 42 CFR Part 2 compliant. With written consent, patient information is pushed from the EHR to create a shared behavioral health record, accessible by other behavioral health organizations that are participating in the HIE. The data within the record may include emergency contact information, substance use history summaries, diagnosis information, insurance information, trauma history summary, medication, allergies, employment information, mental health board disposition, living

situation and social supports, and billing information. This shared record, or "EHR Lite," securely stores patient data, automates required public reporting, and provides aggregate population analytics.

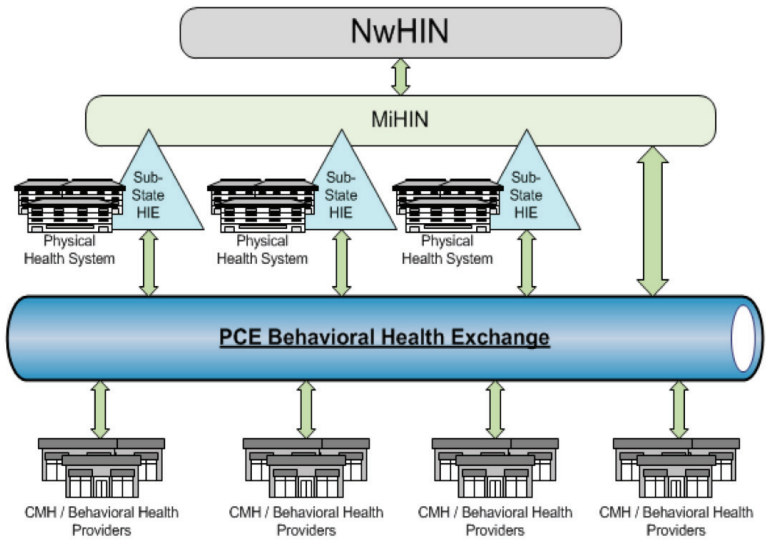
eBHIN is working with the Nebraska Health Information Initiative (NeHII), the state HIE, to develop a plan for integrating the state's opt-out policy with eBHIN's opt-in requirements. eBHIN has also been working with their technology vendor NextGen to develop and incorporate new data standards and value sets that are most relevant in a behavioral health setting. With an eye toward future growth and sustainability, eBHIN is currently looking for support to develop its next set of offerings around transit, bundling services, and analytics to serve ACO needs.

Michigan State Health Information Network and sub-state HIEs

The Michigan State Health Information Network (MiHIN) announced that they would be providing access for exchange with behavioral health providers in Michigan. PCE Systems, a provider of exchange services for the Michigan behavioral health community, has signed on as a Virtually Qualified Data Sharing Organization (VQO) through MiHIN. As a MiHIN VQO, PCE has the ability to securely send and receive health information through MiHIN to other Qualified Data Sharing Organizations (QO's) connected to MiHIN. This agreement will allow Michigan's behavioral health providers to send their information to PCE Systems, the sub-state HIEs will connect their physical health networks with the behavioral health and substance use treatment organizations connected to PCE's information exchange network, PIX (PCE Information Exchange). PIX will send the information to them. PCE has also implemented a Direct HISP in order to handle preferences for exchange using secure messaging.

The PIX system stands alongside sub-state HIEs to provide consent-evaluation and data routing services to and from behavioral health and substance use treatment facilities. PIX can share a wide range of data elements, including CCD/CCR/CDA, demographics, insurance information, admissions, medications, lab results, diagnosis, allergies, treatment plans, clinical documentation, appointments, care team information, staff service activity logs, admissions, and consents. To date, PCE has not sought any grant money or development fees for its work on the PIX system, the system is funded through fees from providers who use their EHR.

PCE/Michigan Behavioral Health Information Exchange Model Overview

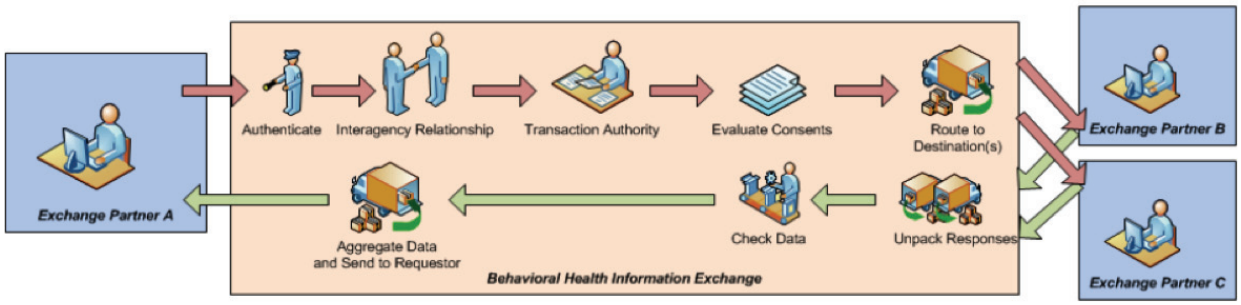


PCE implemented nationwide health information network protocols using a CONNECT 4.2 gateway to interface with MiHIN, Michigan's HIE backbone. MiHIN's CONNECT gateway brokers requests to query the PCE behavioral health HIE. On the behavioral health side, PCE has implemented a consent management "gatekeeper" that evaluates requests received to ensure appropriate authorization and consent are in place before transmitting a response that contains behavioral health information.

This consent (which was primarily developed by a collaboration of Michigan stakeholders) is written to comply with 42 CFR Part 2. The PCE network treats all data as highly sensitive, negating the need to segment between sensitive and physical health data. When using PIX, a 42 CFR Part 2 notification appears on the login screen regardless of the type of information viewed; a second level notification also appears alongside the information that is exchanged.

The Upper Peninsula Health Information Exchange (UPHIE), a MiHIN Qualified Organization and sub-state HIE, announced plans to immediately undertake a behavioral health information exchange pilot with MiHIN and PCE.

Behavioral Health Data Query Process Detail



RecoveryNet

RecoveryNet is a collaborative of ten behavioral health providers that serve 111,000 people in the Rochester, NY area. RecoveryNet's main goal is to advocate for and protect community based substance use treatment as a care option for patients.[xxiv]

A top objective for RecoveryNet was to ensure uniformity among clinical documentation in use by all RecoveryNet partners. This allows the collaborative to track and measure outcomes throughout the network.[xxv] With the help of a grant from SAMHSA (separate from the CIHS grant initiative), RecoveryNet was able to mobilize all partner agencies to decide on and implement a common format for all clinical documentation.

The SAMHSA grant also provided funds toward the implementation of an electronic health record. The collaborative implemented Netsmart's Tier, an EHR geared toward behavioral health care, to facilitate the electronic reporting of client outcomes exchange to Monroe County's Addiction Recovery Employment System (ARES).

Additionally, RecoveryNet was awarded a grant from New York State's HEAL 5 initiative. This grant provided the resources to provide electronic interfaces and administration for smaller RecoveryNet partners that could not host an EHR locally.

Rochester RHIO

Rochester RHIO is a regional health information exchange serving 13 counties in the Greater Rochester, NY area. Rochester RHIO's behavioral health experience began in 2008 as a function of a community grant. The grant funded a large behavioral health network to purchase EHRs, which needed to be interoperable with the HIE. The RHIO worked with regional hospitals to provision lab results through a separate interface and worked with vendors and organizations of vendors that were proficient in interoperability.

In 2011, the RHIO worked with federally qualified health centers doing a health home project with behavioral health providers. They convened a workgroup of behavioral health leaders, including a smaller group working on privacy and consent with behavioral health. There were some issues with using the SAMHSA FAQs, as legal interpretations of 42 CFR Part 2 and some entities were hesitant to use qualified service organization agreements (QSOA). According to Rochester RHIO, the challenge is getting consensus that the QSO model works well.

Rochester RHIO operates two core HIE models – push (e.g. Direct) and a query-based web portal. Rochester RHIO uses the New York State consent form.

In terms of Rochester RHIO's consent model, all information in the HIE is gated to be viewed. In other words, there must be consent from patients for covered entities to view health information. About 40% of the Rochester RHIO population has provided consent for exchange thus far. According to Rochester RHIO, the key to making the consent process successful for the initial patient population and substance use population is education. Getting physicians in the loop first and then providing broad education for patients

was a critical part of Rochester RHIO's efforts. They used the local trust fabric to get the word out through providers and medical societies and used trusted physician sources to inform consumers. There were positive articles published about the RHIO that came from hospitals and medical societies. They then moved into radio and web advertising. Point-of-care materials have been successful in increasing the presence of the RHIO in public and lessening the amount of time physicians must spend educating patients about the RHIO.

The RHIO is exploring how to expand its services to further support behavioral health providers. Rochester RHIO has considered segmenting behavioral health data based on location or type; an HL7 message can be submitted separately through the RHIO, which allows for inclusion of disclosure language on the reports. They are now working through how the CCD that an EHR may generate will persist across exchanges.[xxvi]

Texas Clinical Management for Behavioral Health Services

Clinical Management for Behavioral Health Services (CMBHS) is a web-based clinical recordkeeping system for Texas state-contracted community mental health and substance use service providers. In addition to an EHR, CMBHS serves as a clinical tool for tracking and measuring trends and outcomes. Information is shared with the state and providers within the system to better coordinate and provide quality care.

The CMBHS consent form is 42 CFR Part 2 compliant.[xxvii] To accommodate patient preferences regarding the specific information they wish to share and with whom, CMBHS separates a patient record by category and stores each as a separate document in a centralized database.

CMBHS has adopted a set of principles to guide their HIE:[xxviii]

1. Health information exchange across a "network of networks" that includes locally-controlled and state-managed information systems that facilitate coordination of care, improve administrative processes, and simplify program oversight activities.
2. CMBHS is intended to serve as a component within the state vision for HIE. CMBHS is intended to provide a single system for DSHS behavioral health contractors to provide and receive data about clients who receive, or have received, Texas Department of State Health Services (DSHS) sponsored behavioral health services. CMBHS is a key resource to support continuity of care across organizations including, but not limited to, DSHS-contracted providers, state hospitals, private health entities, and other state and local agencies.
3. Partners in the CMBHS-supported behavioral HIE network, including DSHS and the local mental health authorities (LMHA), will use national data standards where practical and collaborate on establishing and adopting best practices to facilitate HIE.
4. DSHS will consider service providers' and LMHAs' resources, including staffing, technology, and funding, when developing and implementing technology services. There is a shared and joint responsibility to pursue resources from multiple sources and efficiently manage them to advance the use of HIE.
5. LMHAs are not required to utilize CMBHS as their EHR for managing mental health clients. LMHAs will interface with CMBHS for reporting, data access, and certain care coordination purposes.
6. Automated information exchange across mental health and substance abuse (MHSA) contracted care providers will minimize duplicative administrative activities. The development and rollout of technology improvements is dependent on program goals and requirements, available funding, data standards, and providers' technological resources.
7. Any new functionality added to CMBHS should follow a collaboratively developed change management process. The description of functionality will include a justification for the functional change, information about the effect on client care, and applicable fiscal analysis. The timeframe for functionality change should provide adequate time for relevant technology and business process changes.

RECAP: IMMEDIATELY AVAILABLE STRATEGIES FOR EXCHANGING SENSITIVE AND PROTECTED DATA IN AN HIE ENVIRONMENT

Sensitive health data exchange strategies currently in use by HIEs include[xxix]

- Data silos that segregate sensitive information from other personal health information.
- Dual opt-in and opt-out consent models for behavioral and physical health data collection and exchange.
- Short consent durations and latency periods to encourage provider onboarding.
- Direct-enabled secure point-to-point messaging capabilities that push CCDs and other clinical documents between individual providers [This is an extremely popular and useful strategy for exchanging data that is subject to 42 CFR Part 2 restrictions. This method of exchange does not make data available for population health services or individual interventions around preventive screenings or other non-acute treatments. Aggregated analysis of patient data can lead to improved clinical decision support for providers and others].
- Consent management handled through a participant's EHR as opposed to at the HIE level – most relevant for HIEs with a federated data exchange model.
- Patient-driven transmission of information between providers and care settings through the use of Blue Button's view, download, and transmit functionality.
- Use of a secured third party provider portal to view data in the HIE – does not allow for the transmission of data that could then be redisclosed without consent.
- Participation in an HIE that is designed to accommodate the exchange of behavioral health data (e.g. eBHIN in Nebraska).
- Use of QSOAs[xxx] to connect multiple providers at once in a trusted way – all providers are listed on the QSOA so patients can easily see where their information is being exchanged *[NOTE: This strategy does not override the 42 CFR Part 2 requirement that HIEs have two-level consent to disclose any information to another trusted party].*

SUPPORTIVE FEDERAL AND STATE GUIDANCE AND INITIATIVES

SAMHSA/ONC guidance on electronic implementation of 42 CFR Part 2

SAMHSA and ONC have published extensive guidance about how to manage the exchange of behavioral health information, most notably that covered by 42 CFR Part 2, in an HIE environment. They have also sponsored a series of related webinars by the Legal Action Center.[xxxi]

On June 17, 2010, SAMHSA and ONC released Frequently Asked Questions (FAQs) for Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE).[xxxii] These FAQs provide guidance on the application of 42 CFR Part 2 and identify methods for including substance use information into HIEs that are consistent with the Federal statute. Several key FAQs are excerpted below:

Q1 Does the federal law that protects the confidentiality of alcohol and drug abuse patient records allow information about patients with substance use disorders to be included in electronic health information exchange systems?

A1 Yes. Part 2 permits patient information to be disclosed to Health Information Organizations (HIOs) and other health information exchange (HIE) systems; however, the regulation contains certain requirements for the disclosure of information by substance abuse treatment programs; most notably, patient consent is required for disclosures, with some exceptions.

NOTE: This consent requirement is often perceived as a barrier to the electronic exchange of health information. However, as explained in other FAQs, it is possible to electronically exchange drug and alcohol treatment information while also meeting the requirements of Part 2. (Emphasis added)

Q4 For the purposes of the applicability of 42 CFR Part 2, does it matter how HIOs are structured?

A4 No. HIOs may take any number of forms and perform a variety of functions on behalf of the health care providers and other entities participating in the HIO network.

Q5 Does 42 CFR Part 2 permit the disclosure of information without a patient's consent for the purposes of treatment, payment, or healthcare operations?

A5 Unlike HIPAA, which generally permits the disclosure of protected health information without patient consent or authorization for the purposes of treatment, payment, or health care operations, Part 2, with limited exceptions...requires patient consent for such disclosures. Some types of exchange, however, may take place without patient consent when a qualified service organization agreement (QSOA) exists or when exchange takes place between a Part 2 program and an entity with administrative control over that program....

Q6 Under Part 2, can a Qualified Service Organization Agreement (QSOA) be used to facilitate communication between a Part 2 program and an HIO?

A6 Yes. A QSOA under Part 2, which is similar but not identical to a business associate agreement under Parts 164.314(a) and 164.504(e) of the HIPAA Security and Privacy Rules, is a mechanism that allows for disclosure of information between a Part 2 program and an organization that provides services to the program, such as an HIO. Examples of services that an HIO might provide include holding and storing patient data, receiving and reviewing requests for disclosures to third parties, and facilitating the electronic exchange of patients' information through the HIO network. Before a Part 2 program can communicate with a Qualified Services Organization – in this case the HIO – it must enter into a two-way written agreement with the HIO. Once a QSOA is in place, Part 2 permits the program to freely communicate information from patients' records to the HIO as long as it is limited to that information needed by the HIO to provide services to the program. The HIO may also communicate with the Part 2 program and share information it receives from the program back with the program. Patient consent is not needed to authorize such communication between the HIO and Part 2 program when a QSOA is in place between the two.

Q8 If Part 2 information has been disclosed to the HIO, either pursuant to a Part 2-compliant consent form authorizing such disclosure or under a QSOA, may the HIO then make that Part 2 information available to HIO affiliated members?

A8 An HIO may disclose Part 2 information that it has received from a Part 2 program to HIO affiliated members (other than the originating Part 2 program) only if the patient signs a Part 2-compliant consent form. Patient consent is not needed to authorize such communications between the HIO and Part 2 program when a QSOA is in place between the two.

Q9 How do different HIO patient choice models regarding whether general clinical health information may be disclosed to or through an HIO (e.g., no consent, opt in or opt out) affect the requirements of 42 CFR Part 2?

A9 Regardless of which model the HIO adopts for exchanging general clinical information, the HIO must still comply with the requirements of 42 CFR Part 2 with respect to Part 2 information. This means that even if an HIO adopts a "no consent" model for other information, the patient's Part-2 compliant consent must be obtained to disclose Part 2 information to or through the HIO...

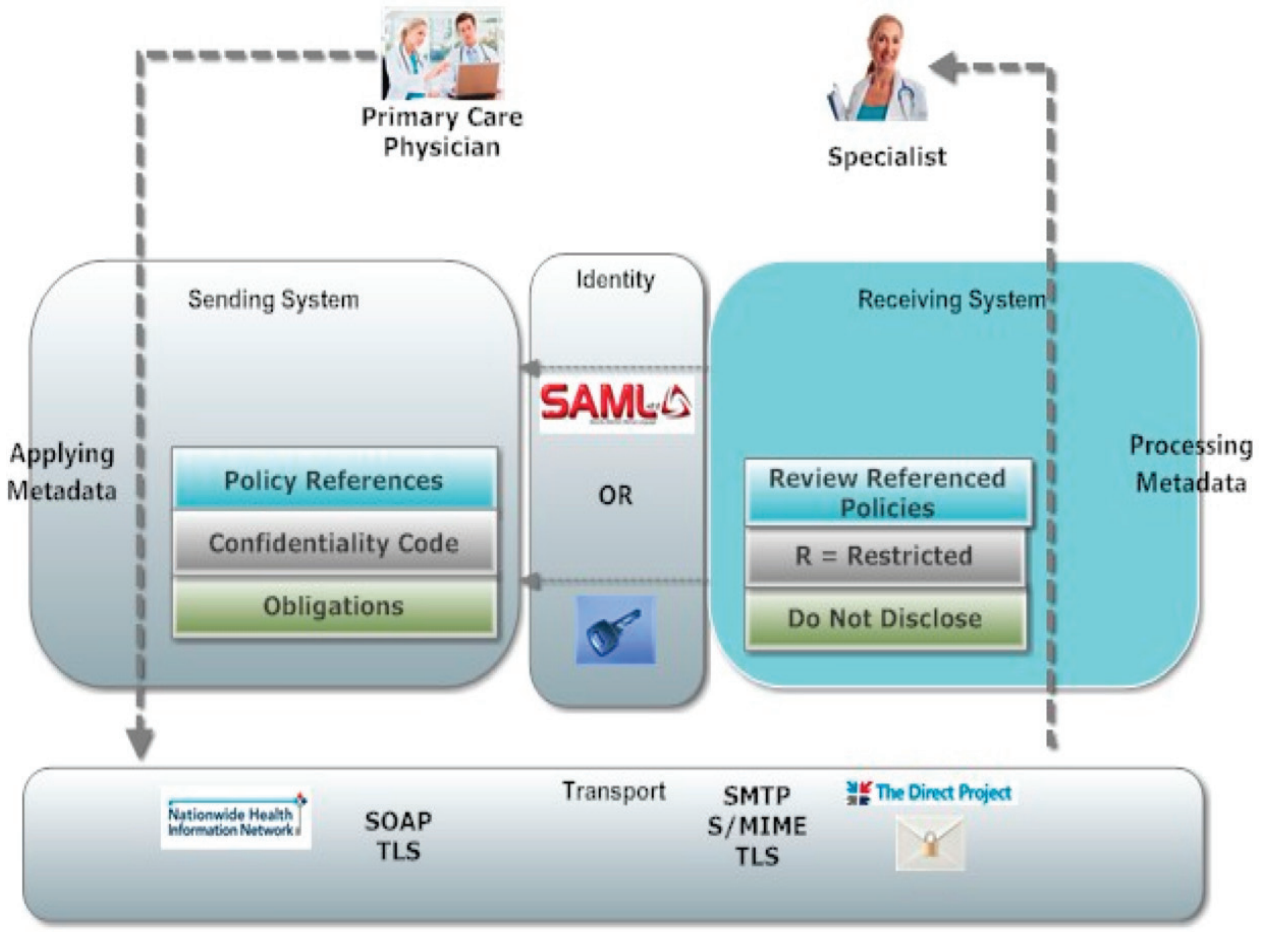
Q18 Under Part 2, can an HIO use a consent form that provides for disclosure to "HIO members" and refers to the HIO's website for a list of those members?

A18 No. 42 CFR Part 2, § 2.31(a)(2) states that consent forms must include the names of the individuals or organizations who will be the recipients of the Part 2 data...

Standards & Interoperability Framework: Data Segmentation for Privacy (DS4P) Initiative

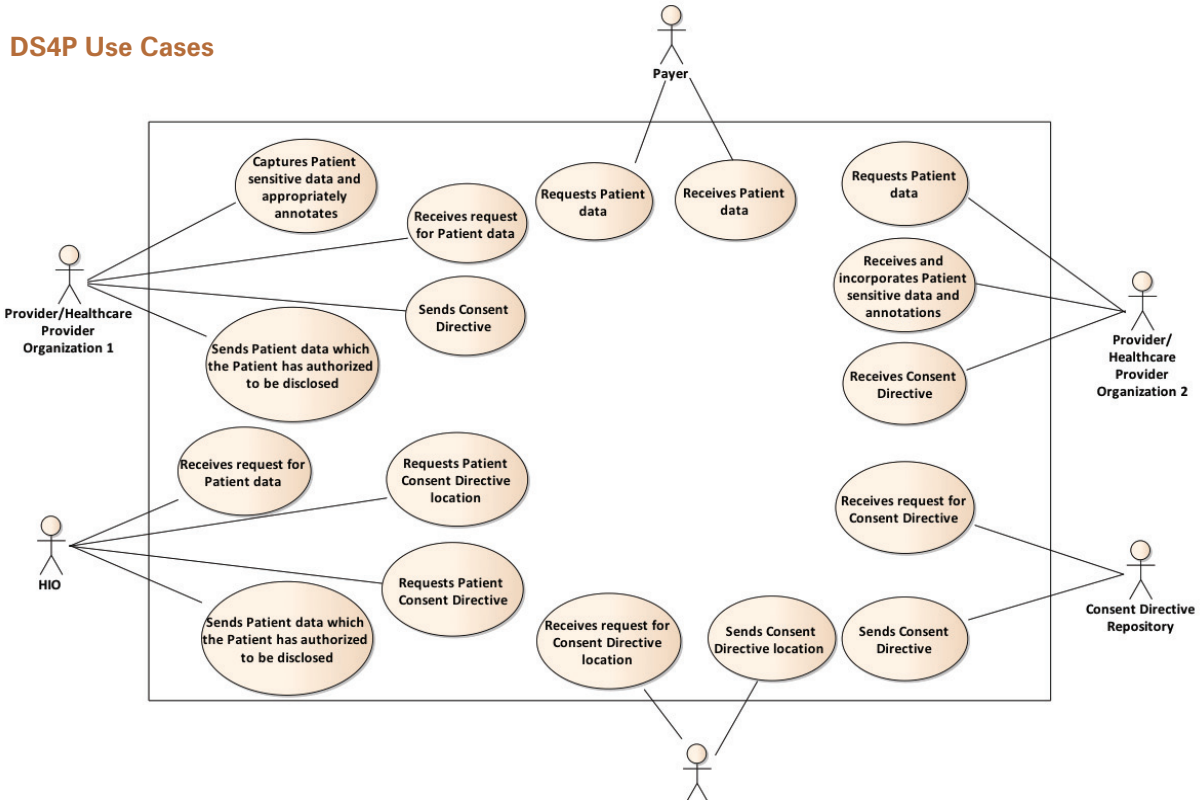
One of the best ways to overcome many of the issues around 42 CFR Part 2 is by making data more granular, thereby offering an opportunity to share only those data elements approved by the patient. The Data Segmentation for Privacy (DS4P) Initiative of ONC's Standards and Interoperability (S&I) Framework brought together leaders to develop and harmonize standards that will allow this to happen across multiple platforms and care settings.

Data Segmentation Approach



The purpose of the DS4P Initiative is to enable the electronic implementation and management of varying disclosure policies in an interoperable manner. The goal of DS4P is to produce one or more pilot projects that allow providers to share portions of an EHR while not sharing others, such as information related to substance use treatment.[xxxiii]

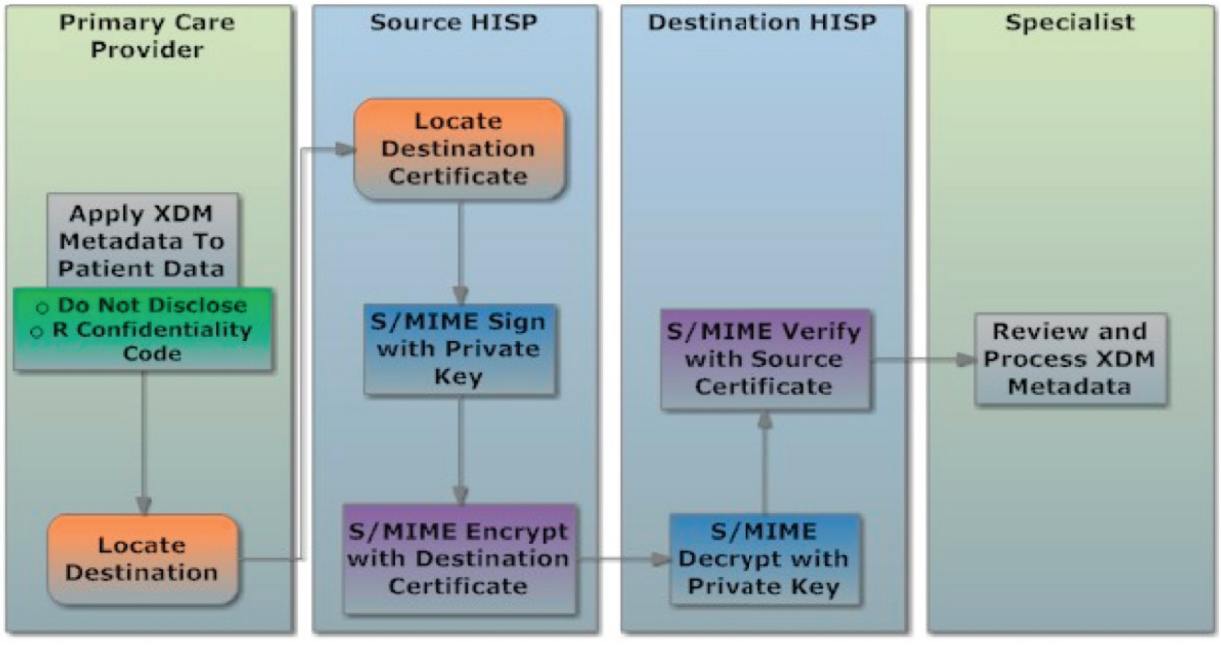
DS4P Use Cases



The DS4P initiative defined four use cases, with user stories and requirements supporting a standards-based privacy protection architecture (specifically application of data segmentation for interchange across systems). Existing relevant standards, implementation guides, prototypes, and technologies were used as much as possible in developing a reference model.[xxxiv] The HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 went through HL7 Normative ballot from August 12 to September 16, 2013.

Data Segmentation Push Based Approach

Confidentiality Code	Set confidentiality level for patient data
Obligation Code	Define obligations for use of patient data
Purpose of Use	Determine if requested purpose is allowed



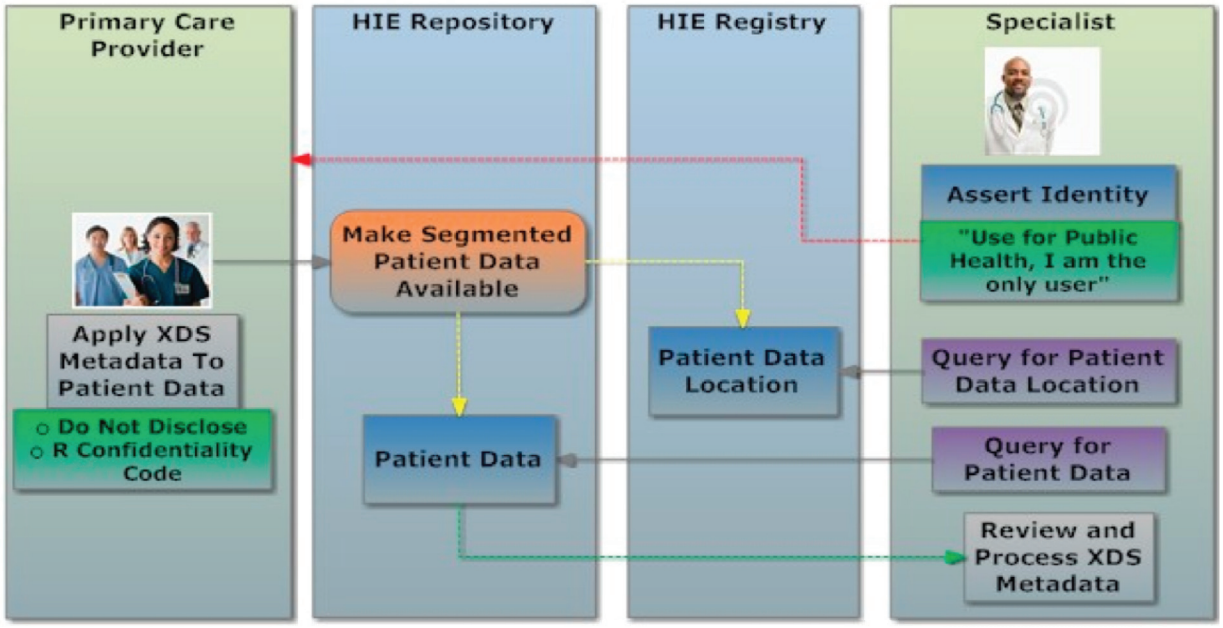
According to workgroup participants, there are three major areas to address for data segmentation to work properly:

- Determine information covered by privacy policy
- Determine what information a patient has consented to share or not
- Apply appropriate metadata

Five DS4P pilot projects are working to demonstrate the use of metadata to identify protected health information using both "push" and "pull" exchange models.

Data Segmentation Pull Based Approach

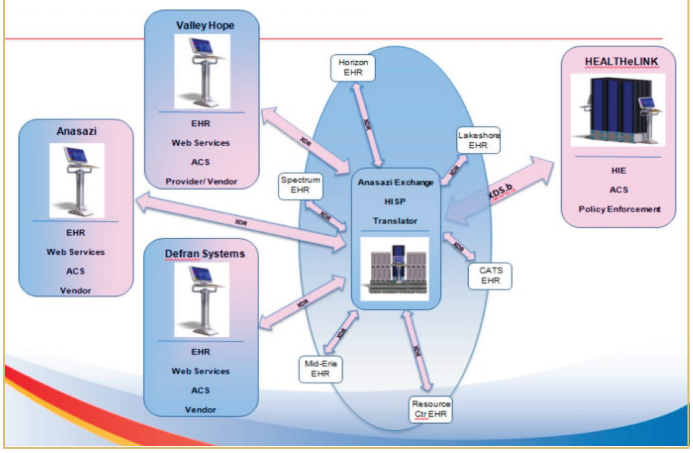
Confidentiality Code	Set confidentiality level for patient data
Obligation Code	Define obligations for use of patient data
SAML Assertion	Assert Identity



SATVA Pilot Ecosystem

The first pilot, a concept developed by the Software and Technology Vendors Association (SATVA), a trade association of EHR vendors serving the field of behavioral health, uses the Direct protocol to transmit a CCD. The CCD is enclosed within an encrypted "envelope" that, when opened, displays the recipient's obligations for handling the specially protected information.

Data Segmentation for Privacy SATVA Pilot Ecosystem



"By standardizing the metadata that will be placed on the 'envelope' that SATVA is piloting, DS4P will make it easier for EHRs from different vendors to understand the distribution limits and legal requirements that are attached to the enclosed patient record," said Scott Weinstein of ONC. As a result, the receiving EHR can either keep the document separate or "segmented" from the rest of the person's medical record, or incorporate the problems, medications, etc. with the protective metadata so that the EHR can subsequently share the person's medical information appropriately.[xxxvi] SATVA is working with Anasazi Software, Valley Hope Association and HEALTHeLINK HIE to implement this pilot.

A more technically complex approach is proposed for "pull" transactions, such as when providers query HIOs for patient records. This approach starts with the same CCD, inclusive of multiple segments, but proposes to add metadata to each segment. These metadata include confidentiality codes that indicate the section's confidentiality level and special privacy protections (using the HL7 Obligation codes set).[xxxvii]

Segments that require normal (HIPAA) protection would be coded with an N, while more sensitive sections of data would be coded with an R (for "restricted"). The highest confidentiality code would be a V, signifying "very restricted" information.[xxxviii] According to Weinstein, "Organizations would have to determine what parts of the [CCD] should be tagged with the available codes based on jurisdictional, organizational, and patient sharing policies."

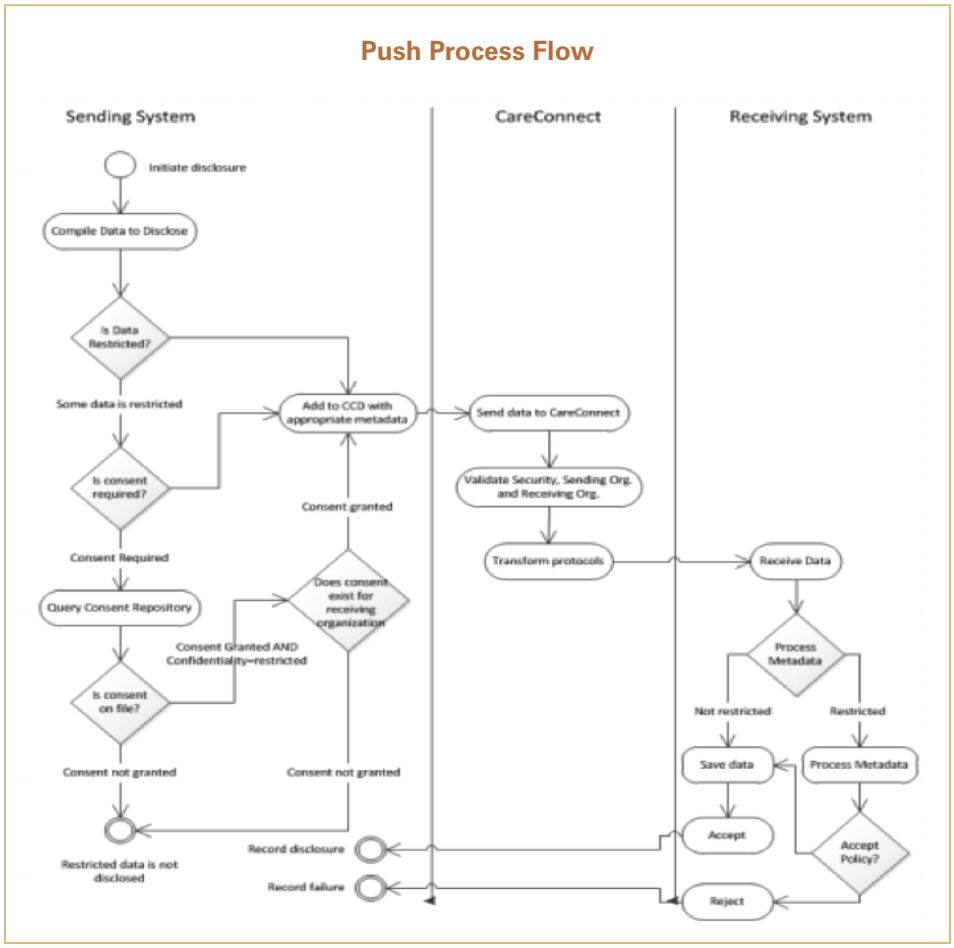
For example, the SATVA pilot tags the entire CCD coming from the Part 2 facility with an "R" because all information coming from dedicated Part 2 facility is to be treated as Part 2 information by the receiving entity.

VA-SAMHSA Pilot

A Veterans Administration (VA) and SAMHSA DS4P pilot created a rules engine that "tagged" certain data entries in the CDA as "PSY" (mental health) or "ETH" (substance use) based on clinical content and then assigned confidentiality codes of "N," "R," or "V" to the respective data segments based on local laws or policies applicable to that content.[xxxix] A March 2013 demonstration of the rules engine showed how sensitive information can be tagged so that when it is sent to another provider with the patient's permission, the receiving provider will know that they need to obtain the patient's authorization to further disclose the information with others. In other words, privacy metadata from the SAMHSA EHR electronically explained to the VA EHR system that substance use treatment information within the clinical document is protected by federal confidentiality laws and can only be used for certain authorized purposes, and cannot be further disclosed without the patient's consent.[xl]

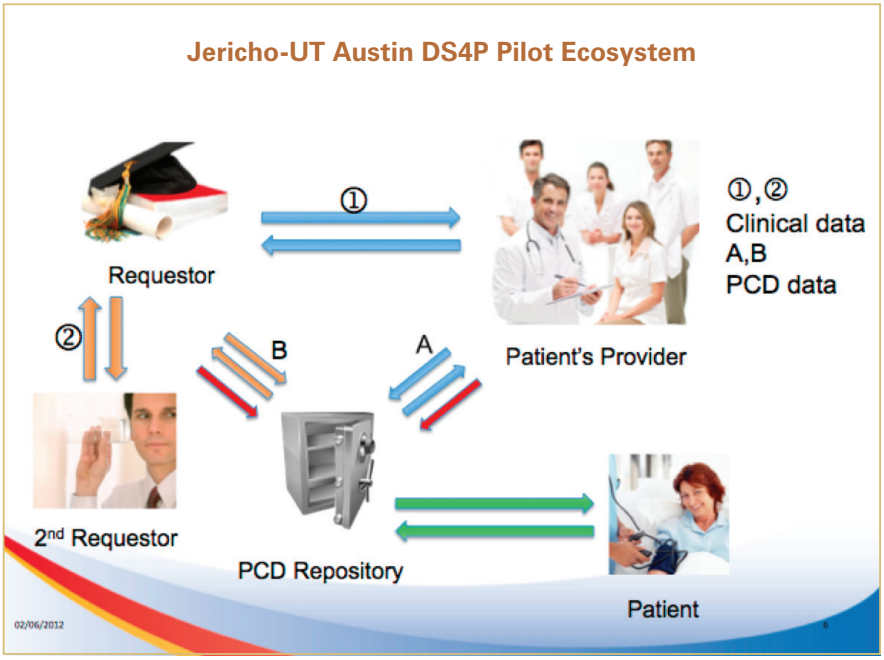
Netsmart Pilot

Behavioral health EHR vendor Netsmart is working with the Illinois Health Information Exchange Authority, the Kansas Health Information Network (KHIN) and the Tampa Bay Network on a DS4P pilot to demonstrate both push and pull scenarios. Tampa Bay will implement solutions addressing the direct push or pull of information between organizations. KHIN is introducing the registry and repository model to the pull of information. Exchange of data subject to 42 CFR Part 2 will be part of both implementations.



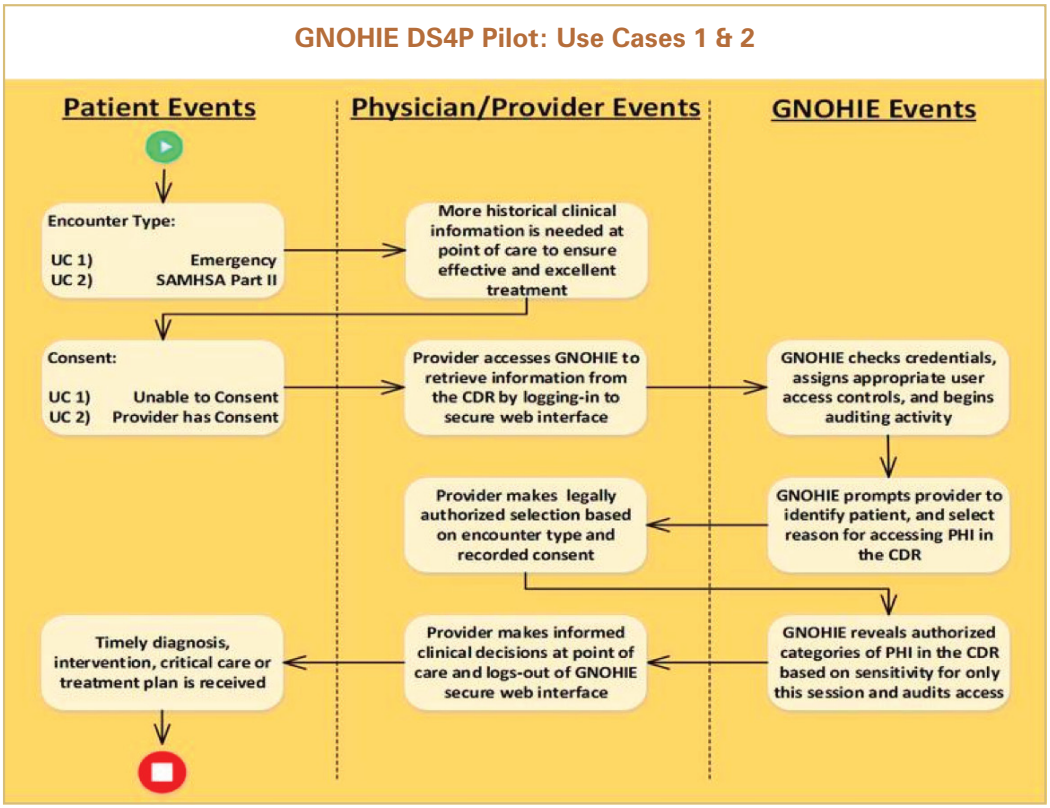
University of Texas Austin-Jericho Systems Pilot

A pilot project led by the University of Texas Austin and Jericho Systems is designed to demonstrate the use of patient consent directives (PCDs) exchanged over the eHealth Exchange, supporting centralized storage and retrieval of a PCD from a repository, with an emphasis on privacy metadata. The goal of the project is to "present a secure, scalable solution that allows consumers to evaluate if their PCD is operating as they planned." This should help consumers to avoid possible medical identity theft or cases of mistaken identity.



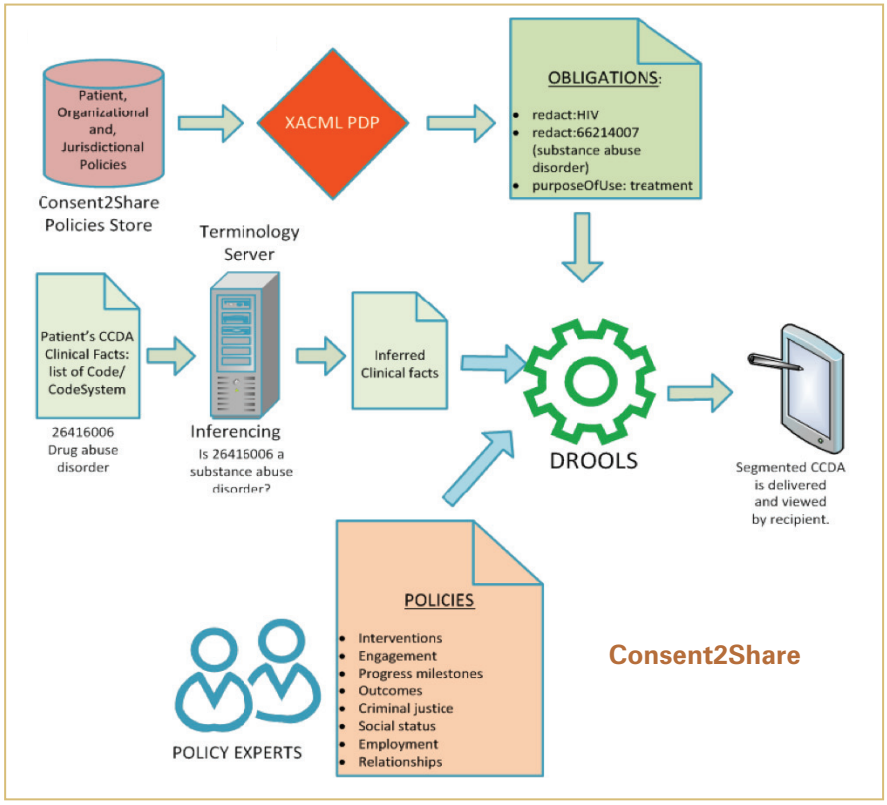
Greater New Orleans HIE Pilot

The fifth DS4P pilot, headed up by the Greater New Orleans HIE (GNOHIE) is addressing the issue of metadata and segmented exchange with a community-governed HIE that has a centralized data repository and several years of clinical information gathered from multiple sources. GNOHIE is working with the Louisiana Public Health Institute and Mirth Corporation on this demonstration of DS4P standards and specifications.



Consent2Share open source software

In an effort to accelerate the application of a standardized consent model that will allow for the exchange of 42 CFR Part 2 data, SAMHSA and the VA are building Consent2Share, a piece of open-source software that can sit in front of an EHR or HIE as a gateway to data segmentation.



Consent2Share is a patient-facing user interface powered by a suite of open source tools. It is built on a vendor-agnostic platform and can connect with any certified EHRs that can produce a CCD/CDA. Key features of Consent2Share include:

- Multi-device user interface.
- Secure two-factor authentication.
- The ability to capture two levels of consent: patient-to-provider and provider-to-provider redisclosure of information.
- A suite of granular consent options aligned with patient preferences.
- A built-in engine to test uploaded medical records against the preferred consent model.
- Electronic signature functionality for paperless consents.
- Modular business rules capability that can be customized for variations in state disclosure laws.
- Connectivity to publish information directly to secondary data users such as biobanks, cancer registries, public health, clinical trials and researchers as appropriate.
- A patient education module with educational videos on relevant information.

Behavioral Health Data Exchange Consortium

Representatives from Florida, Michigan, Kentucky, Alabama, and New Mexico joined together to form the Behavioral Health Data Exchange Consortium through the efforts of the State Health Policy Consortium led by ONC. As part of this project, the states developed a common set of data exchange procedures and policies that are in compliance with 42 CFR Part 2 as well as with various state statutes.

Each state was represented by subject matter experts in legal policy and/or behavioral health, and states have recruited behavioral health providers and others to participate in demonstration projects. Also participating in the Consortium were representatives of ONC, SAMHSA, the Legal Action Center, and subject matter technical experts on direct exchange protocols.

Other Consortium deliverables include:

- Recommended policies and procedures for the interstate exchange of behavioral health data
- Documentation of decision trees for policies and procedures

- Example authorization/consent forms
- Process workflows for common interstate use cases
- Pilot projects to demonstrate interstate exchange of behavioral health data using Direct exchange protocols and the policies and procedures developed by the Consortium
- Evaluation of pilot experiences including stakeholder feedback
- Final report published in August 2013

SAMHSA Consent Management and Data Segmentation for Privacy Conference — August 26, 2013

Broad stakeholder representation provided in-depth discussion on a number of important issues for HIE and integrated care, including:

- Feedback from potential end users on Consent2Share
- Functionality needed to make Consent2Share useful across diverse settings (HIEs, ACOs, Part 2 programs, community health centers, etc.)
- The diversity of privacy policies that are likely to be implemented now and in the future
- The legal and policy framework that will influence what data segmentation choices may be given to patients
- Issues that will impact dissemination of data segmentation functionality
- The process for developing technical specifications for implementing data segmentation privacy policies

Behavioral Health Patient Empowerment Challenge

On August 27, 2013, SAMHSA, ONC, the White House Office of National Drug Control Policy (ONDCP) and the National Institutes of Health (NIH) issued a Behavioral Health Patient Empowerment Challenge. This award challenges software developers to demonstrate mobile applications that use evidence-based strategies to empower patients in their efforts to access treatment for and/or self-manage their personal behavioral health disorders. The top three finishers were invited to the Technology Innovations for Substance Abuse and Mental Health Treatment Conference, where the final winner was given an opportunity to present their application to conference attendees.

Federal Technology Innovations for Substance Abuse and Mental Health Treatment Conference — September 16, 2013

ONDCP and SAMHSA, in partnership with ONC and NIH, hosted the Technology Innovations for Substance Use and Mental Health Disorders Conference at the White House on September 16, 2013. The conference explored the future of health information technology for behavioral health and promoted the dissemination of innovative, evidence-based technologies to advance substance use disorder and mental health treatment through a series of expert panel discussions.[xli]

New ONC HIT Policy Committee workgroup to explore voluntary certification criteria/framework for LTPAC and behavioral health

As part of its HIE acceleration strategy, ONC has indicated that it will ask the Health IT Policy Committee to explore the potential and scope for long-term, post-acute care (LTPAC), and behavioral health voluntary certification programs that could increase EHR adoption, interoperability, and exchange.[xlii]

CONCLUSIONS AND RECOMMENDED NEXT STEPS

There is widespread consensus that behavioral health information should be integrated with physical health information to support improved care coordination, quality, cost effectiveness and patient satisfaction. However, this must be done in a manner that complies with applicable law and respects the privacy and security of sensitive information. Significant progress is being made to overcome these challenges, as demonstrated in the case studies described in this paper. There are several additional steps that can be taken to educate and encourage stakeholders and to consider policy changes and providing additional guidance to the stakeholder community.

Educate

- Educate behavioral health patients about their rights to privacy and data access.
- Educate stakeholders, especially HIEs and HIE participants, about 42 CFR Part 2, including strategies and workarounds to make compliance less overwhelming (e.g. Direct secure messaging use cases).
- Educate stakeholders, especially HIEs and mainstream technology vendors, about why waiting to incorporate behavioral health data can be harmful to patients and why starting that incorporation now can be helpful in long-term financial sustainability.
- Look for and disseminate short-term data exchange methods that can be used until critical mass of EHR/HIE adoption by non-eligible providers is achieved.

Encourage

- Encourage HIEs to include behavioral health representation in governance.
- Encourage behavioral health technology vendors to be active in mainstream standards development activities (e.g. Standards & Interoperability Framework).
- Encourage behavioral health providers to obtain direct secure messaging capabilities.
- Encourage faster incorporation of behavioral health data exchange requirements and data segmentation standards by technology vendors.
- Encourage rapid dissemination and implementation of outcomes from the DS4P initiative and Consent2Share.
- Encourage dissemination and use of the multi-state consent form that was developed by the state HIE grantees.

Consider

- Consider new guidance that includes suggested best practices in addition to regulatory information.
- Consider establishing one national standard that applies to all types of sensitive health information.
- Consider a collaborative process to determine stakeholder opinion on whether to amend consent requirements under 42 CFR Part 2.
- Consider relaxation or reinterpretation of 42 CFR Part 2 restrictions on “To Whom.”
- Consider a collaborative public-private process to develop, disseminate, and implement non-regulatory risk mitigation strategies that will encourage sharing of sensitive data.
- Consider “safe harbor” regulations for uniform privacy compliance that would satisfy the strictest state laws but allow for technology solutions providers to implement consent management functions in a standards-based way.

REFERENCES

i Substance Abuse and Mental Health Services Administration, *Results from the 2011 National Survey on Drug Use and Health: Mental Health Findings*, NSDUH Series H-45, HHS Publication No. (SMA) 12-4725. Rockville, MD: Substance Abuse and Mental Health Services Administration, 2012. www.samhsa.gov/data/NSDUH/2012SummNatFindDetTables/NationalFindings/NSDUHresults2012.htm

ii ibid

iii Robert Wood Johnson Foundation. *Policy Brief: Mental disorders and medical comorbidity,* February 2011. www.rwjf.org/content/dam/farm/reports/issue_briefs/2011/rwjf69438

iv Mayer, Robert. *Incentives and Innovations*. SAMHSA presentation. Statistics from JEN Associates, for Medi-Cal FFS, 2007. www.hitsanfran.treatment.org/Pdfs/Mayer_Robert_508.ppt

v Ibid.

vi Data Security and Privacy Committee of the Illinois Health Information Exchange Authority. *MetroChicago Health Information Exchange,* March 2012. Testimony of Marilyn Lamar, Esq. www2.illinois.gov/gov/HIE/Documents/MCHC%20Testimony%203-29-12.pdf

vii Colton CW, Manderscheid RW. *Congruencies in increased mortality rates, years of potential life lost, and causes of death among public mental health clients in eight states*. Prev Chronic Dis [serial online], April 2006. www.cdc.gov/pcd/issues/2006/apr/05_0180.htm.

viii Lardiere, Michael. *The Behavioral Health Landscape*, June 7, 2012. National eHealth Collaborative University webinar. www.nationalehealth.org/behavioral-health-landscape-recording

ix Lardiere, Michael. *The Behavioral Health Landscape*, June 7, 2012. National eHealth Collaborative University webinar. www.nationalehealth.org/behavioral-health-landscape-recording

x Robert Wood Johnson Foundation. *Policy Brief: Mental disorders and medical comorbidity*, February 2011. www.rwjf.org/content/dam/farm/reports/issue_briefs/2011/rwjf69438

xi National Committee on Vital and Health Statistics. *Recommendations Regarding Sensitive Health Information,* November 2010. Letter to the Honorable Kathleen Sebelius, Secretary, U.S. Department of Health and Human Services. www.ncvhs.hhs.gov/101110lt.pdf

xii State of Michigan. *MiHIN Shared Services Strategic Plan*, April 2010. www.michigan.gov/documents/mihin/MiHIN_Shared_Services_Strategic_Plan_4-30-10_320156_7.pdf

xiii Popovits & Robinson, P.C. *Required elements of valid consent form*, June 2012. www.cihslive.browsermedia.com/operations-administration/Consent_Law_Comparison_Table.pdf

xiv Crowe & Dunlevy, P.C. on behalf of the Oklahoma Department of Mental Health and Substance Abuse Services. *Inclusion of behavioral health information in exchanges: Can it be done?*, 2012. White paper. www.cihslive.browsermedia.com/operations-administration/OK-Legal_aspects_of_sharing_BH_data_white_paper.pdf

xv Ibid.

xvi Ibid.

xvii Data Segmentation in Electronic Health Information Exchange: Policy Consideration and Analysis ONC S&I Framework Whitepaper www.healthit. gov/policy-researchers-implementers/advancing-privacy-and-security-health-information-exchange.

xviii Ibid.

xix Office of the National Coordinator for Health IT. *Standards and Interoperability Framework,* Data Segmentation for Privacy Initiative. Wiki. wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage

xx SAMHSA-HRSA Center for Integrated Health Solutions. *Health Information Exchange/State Designated Entity Sub Awards Meeting*, February 3, 2012. Meeting Minutes. Not available online.

xxi Data Security and Privacy Committee of the Illinois Health Information Exchange Authority. MetroChicago Health Information Exchange, March 2012. Testimony of Marilyn Lamar, Esq. www2.illinois.gov/gov/HIE/Documents/MCHC%20Testimony%203-29-12.pdf

xxii Legal Action Center on behalf of SAMHSA and ONC. *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*, June 2010. www.samhsa.gov/healthprivacy/docs/EHR-FAQs.pdf

xxiii Manos, Diana. *PCE Systems to Partner with Michigan HIE,* January 15, 2013. Healthcare IT News. www.healthcareitnews.com/news/pcesystems-partner-michigan-hie

xxiv RecoveryNet. *A Model of Community Collaboration,* 2011. Presentation. 76.12.14.38/PDF/HealthcareReform/RECOVERYNETSMART.pdf

xxv Mosaica Partners on behalf of Arizona Health Information Exchange Unconnected Providers Program. *HIE Environmental Scan: Behavioral Health Care,* December 2012. White paper. c.ymcdn.com/sites/www.azhec.org/resource/resmgr/docs/behavioral_health_care_-_hie.pdf

xxvi SAMHSA-HRSA Center for Integrated Health Solutions. *Health Information Exchange/State Designated Entity Sub Awards Meeting* February 3, 2012. Meeting Minutes. Not available online.

xxvii Texas Department of State Health Services. *Clinical Management for Behavioral Health Services (CMBHS)*. www.dshs.state.tx.us/cmbhs/default.shtm

xxviii Mosaica Partners on behalf of Arizona Health Information Exchange Unconnected Providers Program. *HIE Environmental Scan: Behavioral Health Care,* December 2012. White paper. c.ymcdn.com/sites/www.azhec.org/resource/resmgr/docs/behavioral_health_care_-_hie.pdf

xxiv Adapted from Boyle, Maureen. *Patient Choice, Confidentiality, and the Affordable Care Act,* August 13, 2013. Behavioral Healthcare Magazine webinar. www.behavioral.net/webinar/patient-choice-confidentiality-and-affordable-care-act

xxx Ibid.

xxxi Legal Action Center on behalf of SAMHSA.*Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*, June 2010. Webinar series. www.lac.org/index.php/lac/webinar_archive

xxxii Legal Action Center on behalf of SAMHSA and ONC. *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*, June 2010. www.samhsa.gov/healthprivacy/docs/EHR-FAQs.pdf

xxxiii Office of the National Coordinator for Health IT. *Standards and Interoperability Framework, Data Segmentation for Privacy Initiative.* Wiki. wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage

xxxiv Ibid.

xxxv Weinstein, Scott.*Data Segmentation for Privacy Initiative,* August 26, 2013. SAMHSA Consent Management and Data Segmentation for Privacy Conference presentation. Not available online.

xxxvi Grantham, Dennis.*Confidentiality alternatives for exchanging electronic medical records take shape*, June 7, 2013. Behavioral Healthcare. www.behavioral.net/article/confidentiality-alternatives-exchanging-electronic-medical-records-take-shape?page=show

xxxvii Ibid.

xxxviii Ibid.

xxxix Ibid.

xl Office of the National Coordinator for Health IT. *Standards and Interoperability Framework, Data Segmentation for Privacy Initiative.* Wiki. wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage

xli ONDCP, SAMHSA, ONC and NIH.*Technology Innovations for Substance Use and Mental Health Disorders Conference,* September 16, 2013. www.federalregister.gov/articles/2013/08/30/2013-21213/technology-innovations-for-substance-abuse-and-mental-health-treatment-conference-and-related-health

xlii Office of the National Coordinator for Health IT. *New HIE Resources on HealthIT.gov* August 9, 2013. New This Week on HealthIT.gov electronic newsletter. Not available online.