June 2014

Behavioral Health Data Exchange Consortium

ONC State Health Policy Consortium Project

Final Report

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0212050.007.000.500.003

RTI Project Number
0212050.007.000.500.003

Behavioral Health Data Exchange Consortium

ONC State Health Policy Consortium Project

Final Report

June 2014

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

This report was funded under Contract No. HHSP23320095651WC, Order No. HHSP23337007T. The contents of this report do not necessarily reflect the opinions or policies of the Department of Health and Human Services or the Office of the National Coordinator for Health Information Technology.

Contributing Authors

Alabama
Gary Parker
IT Project Director
Alabama's One Health Record

Dan Roach
Health IT Coordinator
State of Alabama

Florida
Carolyn Turner
Government Analyst II
Agency for Health Care Administration

Karen Koch
Vice President
Florida Council for Community Mental Health

Kentucky
Julia Costich
Professor
College of Public Health
University of Kentucky

Michigan
Kelly Coyle
Senior Analyst
Michigan Public Health Institute

Nebraska
Wende Baker
Executive Director
Electronic Behavioral Health Information Network

Angeline Petak
Senior Project Manager
Heartland Community Health Network

New Mexico
Shelley Carter
Director of Research and Education
Lovelace Clinic Foundation

Randy McDonald
Research Attorney
Lovelace Clinic Foundation

Ann Greenberg
Privacy Consultant
Lovelace Clinic Foundation

RTI International
Cindy Throop
Stephanie Rizk
Robert Bailey

Subject Matter Experts
Viki Prescott
McBroom Consulting

Katie O'Neill
Legal Action Center

Nageshwara (Dragon) Bashyam
Drajer, LLC

Sherry Reynolds
Alliance4Health

Contents

EXECUTIVE SUMMARY

In August 2011, representatives from Florida, Michigan, Kentucky, Alabama, and New Mexico formed the Behavioral Health Data Exchange (BHDE) Consortium and were later joined by Nebraska and Iowa. The purpose of the consortium was to address legal and technical barriers to the exchange of behavioral health data between health care providers, among organizations, and across state lines and to execute successful pilot exchanges using the solutions developed. This project was funded under the State Health Policy Consortium initiative managed by RTI International on behalf of the Office of the National Coordinator for Health IT (ONC).

To avoid legal and technical complexities associated with the privacy and security of behavioral health data, most current health information exchange activities focus on general physical health data. Behavioral health data require additional protections beyond those of the Health Insurance Portability and Accountability Act (HIPAA), including adherence to 42 CFR Part 2, which limits the disclosure of identifiable information by a federally assisted substance abuse treatment program to any entity, even for treatment, without signed consent from the patient to authorize the disclosure, with limited exceptions. It also restricts the redisclosure of that data by the receiving entity for any purpose without consent.

To overcome barriers to electronic exchange of behavioral health data, the BHDE Consortium participants created a set of common policies and procedures that aligned with federal regulations as well as the laws of the participating states. In addition, participants put these policies and procedures into practice by connecting their state-level systems to allow Direct exchange. Launched in March 2010 as a part of the Nationwide Health Information Network, the Direct Project was created to specify a simple, secure, scalable, standards-based means for sending authenticated, encrypted health information directly to known, trusted recipients over the Internet[1].

The objective of the consortium project was to execute at least one successful pilot demonstrating the ability of providers to exchange behavioral health data electronically across state lines. At the end of the project, data was exchanged between providers in Florida and Alabama, and the necessary frameworks for exchange were established in three additional states.

Participants encountered a number of challenges during the pilot test stage of the project including delays in the state-level implementation of Direct exchange, concerns about the level of knowledge in the provider population about disclosure and redisclosure requirements governing the exchange, and issues related to the cost and process of

[1] www.directproject.org

technically connecting state-level Direct systems. This report provides details about the project's plans, challenges, successes, and products. Highlights include:

- A comprehensive set of policies and procedures that enable providers to exchange behavioral health information between states using Nationwide Health Information Network (NwHIN) Direct exchange protocols and can be replicated in other states and regions;
- Multiple efforts to test and execute the policies and procedures, including exchange between providers in Alabama and Florida, and between providers in Nebraska and Iowa;
- Educational materials for providers, tested intensively by New Mexico and used by participants in state pilots; and
- Lessons learned to support the acceleration of interstate electronic exchange of behavioral health data between providers.

The Florida implementation of Direct subsequently connected (HISP-to-HISP) with Direct instances implemented by state programs in Alabama, Georgia, Louisiana, South Carolina, Michigan, West Virginia, and Wisconsin. These connections were a result of the experience gained and lessons learned through the Behavioral Health Data Exchange Consortium project. Direct messages can now be sent by providers using these services at any time to facilitate care coordination interstate for real-life patients. Perhaps more importantly, these connections have allowed these states to be much more prepared to share patient information if large numbers of citizens are displaced by a potential hurricane or natural disaster.

1. INTRODUCTION

Electronic communication has seen explosive growth in recent years. At the same time, the rapid uptake of electronic health records (EHRs), supported by the programs specified in the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, has significantly increased the availability of electronic patient data. Federally supported programs have also established the necessary technical and policy infrastructure required for the electronic exchange of the data under appropriate circumstances.

Most health information exchange (HIE) activities have focused on the exchange of general clinical data between providers. The Health Insurance Portability and Accountability Act (HIPAA) provides a federal "floor" of regulations setting the permitted uses and disclosure of health information in addition to a framework of safeguards to ensure the confidentiality, availability and integrity of electronic health information so that the exchange of health information is kept private and secure . HIPAA allows for data to be exchanged between entities and their contractors covered by the rule, such as providers, for the purposes of treatment without requiring written consent from the patient. The Federal HIPAA regulations override, or preempt, individual state privacy laws to allow the "floor" to exist, except in circumstances where either Federal and State laws are more restrictive. For example, many states have laws that provide additional protections for the transmission of health information and particularly for sensitive health information such as behavioral health data. Additional federal laws also provide special protections for sensitive health information, including 42 CFR Part 2, which limits the disclosure of identifiable information by a federally assisted substance abuse treatment program to any entity, even for treatment, without signed consent from the patient to authorize the disclosure, with limited exceptions.

To avoid the increased complexity created by these additional consent requirements at both state and federal levels, behavioral health data are often excluded from HIE. As exchange becomes a reality, continuing to exclude behavioral health data leads to increasing concerns about incomplete records and health care disparities. Behavioral health providers and patients alike desire and deserve timely access to their data as well as appropriate, secure data exchange. For this exchange to happen, additional consent management policies and procedures are needed, and providers who send and receive these data must be aware of the requirements inherent in the exchange. Resolving differences in state law requirements for disclosure would also improve the ability to exchange data across state lines.

In 2011, representatives from Florida, Michigan, Kentucky, Alabama, and New Mexico formed the Behavioral Health Data Exchange (BHDE) Consortium. These states worked together to develop common data exchange procedures and policies applicable to Direct exchange. The policies and procedures comply with 42 CFR Part 2 and the various state

statutes that contain more stringent disclosure rules about interstate exchange of other behavioral health information such as mental health data. These policies and procedures were vetted by stakeholders to ensure that they could be implemented in the real world with minimal disruption to workflow. Participating states took part in pilot test activities to connect their exchange system infrastructure and test the ability to send and receive behavioral health data using the policies and procedures. These activities demonstrated that the barriers to the private and secure electronic exchange of behavioral health data could be overcome.

2. PROJECT OVERVIEW AND OBJECTIVES

The Office of the National Coordinator for Health IT (ONC) created the State Health Policy Consortium (SHPC) project to support multistate initiatives to develop solutions to policy challenges specific to interstate health information exchange (HIE). The SHPC is funded by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009. RTI International, the research institute that manages the overall SHPC project for ONC, supported an open solicitation for concepts that fit the requirements and worked with the participating states to develop the scope of work that guided this project. The project involved three main phases: (1) policy and procedure drafting and state review, (2) pilot test development and execution, and (3) post-pilot analysis and reporting.

The purpose of the Behavioral Health Data Exchange (BHDE) Consortium was to facilitate and address barriers to the intra- and interstate exchange of behavioral health data. The project was designed to be flexible, recognizing that the results of the initial research about policies, procedures, and laws would determine the direction and scope of the pilot test activities.

Barriers to the exchange of behavioral health data are not limited to policies and procedures; technical and cultural barriers also exist. A subset of states participating in the solution-building process were charged with conducting a Direct-enabled pilot test to provide a proof-of-concept demonstration that the policies and procedures aligned with the technical capacity to execute the exchange. They also tested the ability of the components, such as a form to provide patient consent for the release of PHI from one provider to another, to withstand real-world use.

3. POLICY AND PROCEDURE ACTIVITIES AND OUTCOMES

The scope of the Behavioral Health Data Exchange (BHDE) Consortium project included developing and pilot testing policies and procedures that enable behavioral health provider participation in interstate health information exchange (HIE) for patient treatment purposes. The project focused on using the "Push" transaction model via Nationwide Health Information Network (NwHIN) Direct exchange protocols. Federal law (42 CFR Part 2) and mental health information protection laws of participating states were considered when drafting the policies and procedures. The goal was to create policies and procedures that could be replicated in other states and regions. Specifically excluded from the scope of this project are the exchange of psychotherapy notes (as defined by HIPAA Privacy Rule); laws specific to minors; the exchange of other types of sensitive data such as human immunodeficiency virus (HIV), sexually transmitted diseases (STDs), and family planning; and data from educational institutions. Also, the team decided not to address disclosure in emergency situations. Restricting the scope of the project was intended to ensure that tangible outcomes could be achieved in a timely way.

3.1 Approach

Policies and procedures were created following several principles:

- Policy and procedure development should focus on those that enable "Push" transactions using Direct exchange protocols and exclude "Pull" (query) transactions. They should have an interstate focus and be limited to use of data for treatment purposes only. All HIEs, are HIPAA business associates, and therefore are bound by their Business Associate Agreements which set requirements under which they must comply with and are directly liable for violations of the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule, our focus should be on issues unique to behavioral health.
- Policies and procedures should focus on meeting minimum requirements of federal and state laws to the extent allowed by project scope.
- Policies and procedures should be feasible and practical for providers to implement and provide more than one option for implementation where possible.

3.2 Determining Use Cases

The team reviewed the Direct exchange use cases for Meaningful Use Stage 1 found on the Office of the National Coordinator for Health IT (ONC) Direct Project website and created use cases for the BHDE project. ***Attachment 1*** contains the final use cases and shows how they correlate to the ONC Direct Use Cases found on the website as of November 26, 2011 (http://wiki.directproject.org/User+Stories).

The team discussed but decided not to include an emergency scenario because it would have different requirements under 42 CFR Part 2, non-emergency situations would require

the team to think through the execution of all steps in the process rather than bypassing those allowable under a "break the glass" scenario, and also because the ONC Direct Project Use Case site did not include any emergency use cases.

3.3 Development of Draft Policies and Procedures

After establishing principles for policy and procedure development and identifying use cases, the supporting subject matter experts (SMEs) conducted a review of existing materials and documents provided by the states and by RTI. Sources included the following:

- *Health Information Security and Privacy Collaboration (HISPC) Reports on State Law, Business Practices, and Policy Variations: Report on State Law Requirements for Patient Permission to Disclose Health Information*, by Joy Pritts[2];
- *HISPC Interstate Disclosure and Patient Consent Requirements Collaborative Final Report*[3];
- *HIPAA Privacy and Security Rules*[4];
- 42 CFR Part 2[5];
- June 2010 and December 2011 Frequently Asked Questions (FAQs) published by the Department of Health and Human Services (HHS)[6];
- *State Health Policy Consortium (SHPC) Upper Midwest HIE Consortium Final Report on Interstate Consent Management* (unpublished);
- Examples from other states, such as sample consent forms, policies and procedures from participating states and from other states (e.g., Nebraska and New York).

Each state described any existing state laws requiring patient consent[7] to enable disclosure between treating providers and provided supporting citations and documentation. A summary of this state law review is provided as ***Attachment 2***.

[2] http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf
[3] http://www.healthit.gov/sites/default/files/c1_1_1_final_rpt.pdf
[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html
[5] http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&rgn=div5&view=text&node=42:1.0.1.1.2&idno=42
[6] http://www.samhsa.gov/HealthPrivacy/docs/EHR-FAQs.pdf and http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf
[7] States use various terms to refer to the concept of obtaining approval from a patient to share health information with an outside party, including "consent," "authorization," and "release." Under the HIPAA Privacy Rule, the terms "consent" and "authorization" mean two different things. The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain a patient "consent" for uses and disclosures of protected health information for treatment, payment, and health care operations. See 45 C.F.R. § 164.506(b). Covered entities that do so have complete discretion to design a process that best suits their needs. By contrast, an "authorization" is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. See 45 C.F.R. § 164.508(a). An

3.4 Review of Draft Policies and Procedures

Draft policies and procedures were provided to consortium members in advance of the in-person project meeting held in Washington, DC, on December 12, 2011. The purpose of the meeting was to review the draft policies and procedures, solicit feedback and suggestions from participating states, and transition to the pilot-planning phase of the project.

The group reviewed and discussed each individual policy, as well as sample Qualified Service Organization Agreement (QSOA) language and example consent forms. Revisions to the draft policies and procedures were made as a result of the meeting.

3.5 Analysis of December 2011 SAMHSA Guidance

In December 2011, HHS's Substance Abuse and Mental Health Services Administration (SAMHSA) released guidance in the form of revised FAQs on health information exchange and 42 CFR Part 2. Project SMEs conducted a detailed review and analysis of the new FAQs as applied to the project. They determined that the new FAQs did not impact the draft policies and procedures. ***Attachment 3*** summarizes that analysis.

3.6 Review of Final Policies and Procedures

On January 5, 2012, participating states were given a final version of the policies and procedures, which can be found in ***Attachment 4***, to review for compliance with the state's laws and for clinical and technical feasibility. The review process followed by each state is summarized in ***Attachment 5***. The states completed their review on March 30, 2012.

Comments from the review process emphasized the need for provider education about consent requirements. They also raised questions about how the implementation and use of Direct exchange either changed or did not change the consent requirements. The review demonstrated that the policies and procedures themselves did not need to change.

authorization is a detailed document that must contain specific elements set forth in the Rule. See 45 C.F.R. § 164.508(c). Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. We use the term *consent* to refer to this concept generally, unless we are directly quoting a state statute or regulation.

4. STATE PILOT TEST PREPARATION

The pilot tests were designed to demonstrate that policies and procedures could be implemented to support the participation of behavioral health providers in clinical messaging using the Nationwide Health Information Network (NwHIN) Direct exchange standards. Implementation of Direct exchange by states through the Office of the National Coordinator for Health IT (ONC) State Health Information Exchange (HIE) Cooperative Agreement programs was an essential component of pilot test preparation, and the timing of the pilot tests had to be coordinated with the states' implementation of Direct exchange.

In addition to working with the individual state teams participating in the Behavioral Health Data Exchange (BHDE) Consortium, RTI coordinated with ONC to identify consultants who could directly support the participating states with Direct exchange technical advice and guidance about engaging behavioral health providers. During the pilot test preparation stage, consortium participants contacted behavioral health providers in their states to solicit participation in the pilot tests.

4.1 Pilot Test Planning

The purpose of the pilot phase was to test the procedures and policies developed during the initial phase of the project and to create the technical infrastructure required to execute ongoing exchange across state lines. The project team committed to testing the framework in a real-world setting to answer the following questions:

- Do policies and procedures comply with the HIPAA Privacy and Security Rules and 42 CFR Part 2 requirements and state-specific privacy laws?
- Are the policies and procedures comprehensive, accurate, and understandable by all parties (health IT stakeholders, providers, patients)?
- Do the policies and procedures withstand real-life use or do they need to be adjusted to account for variables that were not previously considered?

Determining Resource Needs

Technical and associated labor costs for pilot tests were difficult to predict because the initial set-up cost for developing interfaces between health information service providers (HISPs) to enable the exchange of Direct secure messages was quite variable. The variability existed because each of the states participating in the pilots were at different stages in establishing their Direct technical infrastructure. For example, some states had HISPs that were operational, some states were in the process of procurement. To address this challenge, funding was initially allocated for participation in policy and procedure development and initial pilot planning. Once participants reached the pilot planning stage, separate awards were made to support the pilot implementation work. These awards were based on the specific technical implementation needs of each state, and ranged between

$9,500 and $28,500. This division allowed for accurate estimation of pilot costs after the planning phase was completed, rather than allotting a flat estimate at the outset of the project.

Selecting Use Cases for Testing

Two of the three use cases developed earlier in the project to guide policy and procedure development were identified as most relevant to the planned pilots:

- Direct User Story #1: Primary Care Provider Refers Patient to Specialist Including Summary Care Record
- Direct User Story #3: Specialist Sends Summary Care Information Back to Referring Provider

Florida included a third use case that was compatible with their established referral patterns; this use case involves a specialist sending a summary care record to another specialist. See ***Attachment 3*** for a complete description of each use case and the data flow envisioned.

Interstate Versus Intrastate Exchange

The initial application for State Health Policy Consortium (SHPC) support submitted by the BHDE states focused on intrastate exchange issues. During the scope development stage prior to award, participants agreed to address interstate exchange as well, to align with the purpose and goals of the SHPC project. The states were not all in close geographic proximity but were open to exploring possible data exchange scenarios with each other and with other states. Nebraska joined the project in early 2012 and proposed to exchange data with Iowa. The flexibility of the SHPC funding mechanism allowed them to join the project after it was already under way. Prior to joining, Nebraska had progressed at least as far as the other states in the consortium and offered the project another interstate exchange pilot test opportunity. As a result, Nebraska and Iowa agreed to conduct an interstate pilot test, as did Alabama and Florida. New Mexico completed an intrastate pilot test of the transfer of information between two clinics (one behavioral health and the other primary care) in a rural setting. Kentucky and Michigan did not complete state-level Direct exchange implementation in time to participate in the project's pilot test phase.

Format of Data

The pilot tests used summary care information in PDF format. Although the ultimate goal of data exchange is to exchange standardized, machine-readable data, exchanging standardized data in PDF format serves an important purpose within the project context. Special protections prevent behavioral health data from being redisclosed without the patient's explicit permission. Current electronic health record (EHR) systems cannot effectively segment behavioral health data from other clinical data; once the EHR system

reads patient data, those data become part of the patient record and could be redisclosed along with other patient information if requested by a third party. Until these data segmentation issues are resolved, exchanging data in PDF format allows the receiving physician to read the information without it being incorporated into existing electronic systems in a machine-readable format. Alabama, Nebraska, and New Mexico transmitted summary of care information in PDF format. Florida transmitted records as specified by providers in PDF format. None of the pilot test participants transmitted data in a continuity of care document (CCD) format.

Recruiting Processes for Each Pilot

Florida and Alabama

The Florida Council for Community Mental Health recruited member facilities to participate in the pilot.

Nebraska and Iowa

The Electronic Behavioral Health Information Network (eBHIN) had an existing referral pattern between the Federally Qualified Health Center operating in Council Bluffs, Iowa, and the publicly funded behavioral health providers across the Missouri River in Nebraska. Although Nebraska residents can receive primary care services in Iowa, they may only access publicly funded behavioral health services on a low- or no-cost basis in Nebraska. This pattern provided the basis for the testing of simulated data, but once the capability is built it will also provide the basis for real data exchange because the referral pattern already exists.

New Mexico

The New Mexico Project Team originally planned to recruit providers through a large behavioral health care organization located in Albuquerque and a primary care provider in rural New Mexico. When recruitment efforts proved unsuccessful, the team contacted five behavioral health providers throughout the state. After introducing the BHDE project and its goals to each of the providers, the team successfully recruited NonviolenceWorks, located in Taos, New Mexico. NonviolenceWorks had an existing referral pattern with a primary care provider, the Taos Medical Group, which agreed to participate. As a result, by the end of August 2012, New Mexico's pilot project had successfully secured a behavioral health provider and a primary care provider who regularly corresponded with each other regarding patient referrals and follow-up care.

4.2 Provider Education Work

As noted in section 3.6, the review of the final policy and procedures led consortium participants to recognize that, while the instructions provided were compliant with Federal and local laws, there was a need to educate providers about the requirements for exchange,

appropriate disclosure, and storage of behavioral health data. Some stakeholders expressed concern with the prospect of releasing information to a provider without some level of assurance that the provider did in fact understand the information contained in the policies and procedures document. The consortium decided to form a workgroup to prepare documents that would help establish trust between participants in the pilot tests by providing quick and easy references for both providers involved in the exchange.

The workgroup initially focused on developing two "checklist" documents – one for the sending provider and one for the receiving provider – to outline the general mechanics and expectations for exchanging behavioral health information using Direct (see ***Attachments 6*** and ***7***). Some items on these checklists, such as calling the requesting provider to validate the request and establishing the correct Direct e-mail address, were not required but served to engender trust by increasing both provider's level of comfort with the disclosure. Other checklist items, such as ensuring that written consent was provided and that re-disclosure requirements[8] were understood, served as a sort of "attestation" that both providers fully understood the content of the policies and procedures document (see ***Attachment 8***).

All states reviewed the materials created by the provider education workgroup prior to their use in the pilot activities. New Mexico performed the most rigorous review of the materials, creating a Provider Notebook which combined all of the materials developed by the group into a guide for exchanging behavioral health data (see ***Attachment 8***). More detailed information about New Mexico's development of the Provider Notebook is provided in Section 4.4. Feedback from consortium participants, participating pilot test providers, and stakeholders was incorporated into the final versions of these materials.

4.3 State-Level Technical Readiness

Each state's technical readiness to participate in a pilot test was assessed prior to pilot implementation. The assessment collected information on the following dimensions:

- Description of the providers participating in the pilot, including information such as the type of organization, number of providers involved in the data exchange and access mechanisms for Direct services.
- Providers' system capabilities were outlined to understand providers' system support for exchanging health data using Direct exchange and understand providers' system support for exchanging behavioral health data using Direct exchange.
- Consent management, including information on how consent is collected for data exchange and how consent is stored and accessed.

[8] The HIPAA Privacy Rule allows for disclosure for treatment, payment or healthcare operations unless the patient has requested restriction to the use or disclosure of the PHI and the health care provider agrees to, or is required to honor the request. See 45 CFR 164.506. See also 45 CFR 164.522(a).

- State HIE technical information, including State HIE Direct implementation details, HISP-to-HISP communication details, details on trust establishment, and details on Direct certificates.

As part of the readiness assessment, a baseline on Direct capabilities was established in each state in January 2012. Although Florida and Alabama State HIE implementations of Direct were operational, Kentucky, Nebraska, New Mexico and Michigan implementations were still in the planning and procurement stages. Detailed planning calls were then conducted to determine the next steps needed to implement the pilot tests.

While each BHDC state had to take into account unique aspects of their technical and organizational readiness, the framework below provided a specific set of steps that each could take in order to determine what their participation in the pilot would look like. Because it was produced to gather specific data through more broadly applicable components, it also serves as a good model for other states seeking to engage in similar interstate data exchange efforts.

Step 1: Identify pilot organization(s).

States with operational Direct services need to identify the provider organizations that will participate in behavioral health data exchange within and/or across states.

Participants: State HIE organization

Step 2: Establish document workflow.

This enables both the State HIE and the provider to understand the technology and communication environment surrounding the exchange. States with identified participating provider organizations need to identify:

- what use case(s) participants are willing to execute,
- how medical records will be accessed and exchanged,
- how consent will be linked to the data being exchanged, and
- how providers and patients will be educated.

Participants: State HIE organization in collaboration with provider organization(s)

Step 3: Prepare pilot organizations.

Step 3a. Have pilot organizations sign the participants' agreements.

Step 3b. Ensure that the Pilot organizations are trained and ready to use Direct Services.

Step 3c. Determine technical connectivity between the pilot sites including any intermediate HISPs that will be used. This step will identify the edge systems and protocols that will be used to integrate the pilot sites with their HISP. Identifying the edge systems and protocols will help determine how the systems will integrate with their existing workflows or identify modifications to workflows.

Participants: State HIE in collaboration with the pilot organizations identified

Step 4: Issue certificates and publish certificates for Direct services, if required.

The State HIE may manage certificates for its pilot organizations according to Direct protocols. Pilot organizations may use another HISP or have their own HISP which will issue certificates. In these cases the State HIE should verify that the pilot organization has published certificates (i.e., public keys) according to Direct protocols.

Participants: State HIE will perform this step as applicable

Step 5: Coordinate state HIE implementation activities across state lines.

States with operational state-level HISPs need to do the following:

Step 5a. Exchange Trust Anchors with the neighboring state/exchange partner,

Step 5b. Exchange test messages with the neighboring State HIE installations.

Participants: State HIE in collaboration with the pilot organization and other State HIE programs with whom data is being exchanged

Step 6: Manage pilot participation integration activities.

Integrate the clinical workflow with the Direct Services and execute the selected use cases. This assessment and the planning provided a mechanism for each state to incrementally execute the tasks needed to conduct a successful interstate pilot of behavioral health data exchange. Each state's detailed pilot plans are described in the next section.

Participants: State HIE in collaboration with the pilot organizations and the other states involved in the data exchange

4.4 Pilot Plans

Florida and Alabama

Florida and Alabama decided to test the use case that was most consistent with their established referral patterns, where a community mental health center in one state requests health records from a community mental health center in another state. They viewed it as the simplest and most straightforward use case from a logistics perspective and a good starting point for initial exchange efforts.

Florida and Alabama exchange scenarios:

- A Florida behavioral health provider requests a patient's records from a prior stay at an Alabama provider (a behavioral health facility – 42 CFR Part 2 program).
- An Alabama provider (a behavioral health facility – 42 CFR Part 2 program) requests a patient's records from a Florida provider.

The team decided to use de-identified data in the exchange because it was seen as more realistic than dummy data. All data was de-identified using the implementation specifications described in 45 CFR 164.514. While it did not contain identifiable information for a specific patient, it did contain actual clinical data and therefore provided a more "real-world" example. In addition to these plans, the team determined that the participant organizations would complete the checklists developed by the provider education work group (see ***Attachments 6*** and ***7***). The checklists serve as a guide to best practices in the handling of mental health and substance abuse treatment records and guide the process of making and responding to a request.

Nebraska and Iowa

Nebraska and Iowa decided to test use cases involving the exchange of behavioral health data between primary care and behavioral health providers. From the outset, it was important for eBHIN to involve project stakeholders in the adoption of the BHDE policies and procedures and the development of education materials. Stakeholders included Nebraska eBHIN, Nebraska Health Information Initiative (NeHII), Iowa Health Information Exchange (IHIE), and the Nebraska Information Technology Commission (NITC). This collaboration was accomplished through individual meetings with pilot participants, technical calls with vendors, and monthly stakeholder meetings. Through these meetings, eBHIN developed qualification standards for participation, refined the confidentiality agreement, and contributed to education materials.

Providers wishing to connect with other providers for the purpose of exchanging behavioral health data using Direct sign a confidentiality agreement and acknowledge they have received and understand the participant education materials. Although one of the Nebraska pilot participants expressed a desire for much more expansive educational materials, which eBHIN acknowledged as potentially very helpful, eBHIN decided to adopt the educational materials developed by the BHDE Consortium because of the limitations of time and resources to develop and vet additional materials. eBHIN did include an additional 1-page information sheet intended for the consumer.

The second part of the pilot test planning phase related to technology discovery. eBHIN began the project hoping to connect the Nebraska-based behavioral health provider to an Iowa primary care provider via Nebraska's HISP, Axolotl, and Iowa's HIE and HISP, Informatics Corporation of America (ICA). Through the technical discovery process, vendors discovered an incompatibility between these systems in the way the PDF and secure message would be encrypted, sent, and received. Specifically, NeHII and IHIE are currently using incompatible protocols, SMTP/XDM and SOAP/XDR respectively, at this time. Although it is feasible to implement a system to bridge these two protocols, it would be a significant challenge. Furthermore, each vendor has indicated that they will be

supporting the other protocol in future releases, so expending effort in developing a bridge between these two systems would not have been a wise use of funds during the time of the pilot project window[9].

New Mexico

Creation of a Provider Notebook

New Mexico decided to test use cases involving the exchange of behavioral health data between primary care and behavioral health providers within the state. To prepare behavioral health and primary care providers for the pilot phase of the project, the New Mexico project team created a Direct Secure Messaging Provider Notebook (Provider Notebook). It includes information that was vetted by the provider education workgroup and information the team gathered to assist providers in the pilot implementation process.

The Provider Notebook describes the overall goals of the project and includes the final versions of the materials created under the project, including:

1. Direct Secure Messaging Fact Sheet – Overview, Disclosure, and Re-disclosure of Behavioral Health Data (including a statement about 42 CFR Part 2);
2. Protected Health Information Request Form;
3. Patient Consent Form;
4. Checklist for Making a Request;
5. Checklist for Responding to a Request;
6. New Mexico Health Information Collaborative (NMHIC; the state's HIE) Direct Secure Messaging User Guide;
7. NMHIC Direct Secure Messaging User Setup;
8. Contact Information; and
9. the Pilot Participant's Response Form (***see Attachment 8***).

Engagement with the Providers

Prior to the pilot implementation phase, the New Mexico project team sent the Provider Notebook to the two providers considering participating in the pilot for feedback on its utility and clarity. The team then met with the providers to gather their feedback and answer questions about the notebook they might have. While the behavioral health provider did not have any questions, the primary care provider stated she was not aware of the nuances

[9] Nebraska was able to begin work on a pilot to exchange behavioral health data after the completion date of this project. This work is anticipated to reach completion by the end of 2013.

associated with behavioral health data exchange described in the notebook. Both providers agreed to participate in the pilot test.

42 CFR Part 2 and Provider Consent Forms

The project team requested copies of the patient consent forms used by the two providers to compare with the form established by the Provider Education Workgroup. Although the providers' patient consent forms give general consent, they do not acknowledge the requirements of 42 CFR Part 2. Interestingly, the primary care provider's patient consent form had slightly more detail than the behavioral health provider's form. This omission of 42 CFR Part 2 by both providers, but in particular by the behavioral health provider, indicates that providers (even behavioral health providers) may have limited knowledge and understanding of 42 CFR Part 2 regulations and may need additional explanation prior to exchanging patient behavioral health data.

Provider Understanding of 42 CFR Part 2.
During the pilot phase, there were clear indications that a knowledge gap exists within the general patient population related to the disclosure, storage, and re-disclosure of information governed by 42 CFR Part 2 regulations. While behavioral health providers and those that exchange patient data on a regular basis may have more familiarity with the requirements, providers in the larger exchange community do not. The project team focused on ensuring that all providers involved in the pilot exchanges were familiar with these disclosure requirements, but in order for these types of exchanges to happen more regularly, a significant and widespread education campaign is essential.

Pilot Test Preparation

In preparation for pilot test implementation, Direct exchange accounts were established for each provider. A technical liaison gave account and login information to each provider to test prior to transferring data; this security specialist was available to provide assistance to providers as they set up their accounts. As the date for the pilot test approached, both providers informed the project team that they were not yet ready to transmit data; due to their busy schedules, they had not had a chance to activate their Direct exchange accounts. The project team ultimately walked the providers through the process. To avoid similar issues with the pilot test portion of the project, the Project Team created a pilot script to walk the providers through the process of transferring "test" data.

5. PILOT IMPLEMENTATION

5.1 Pilot Results

Florida and Alabama

The Florida and Alabama pilot implementations were completed in two phases. The first phase involved applying the technical requirements to enable the connection of the Florida implementation of Direct exchange with Alabama's implementation of Direct exchange. In Florida, development work to set up for exchange between health information service providers (HISPs), including establishing the necessary test environment, was conducted from February to June 2012. This work included finalizing the certificate requirement with Verisign for creation of Direct compliant security certificates. Alabama's technical foundation for the One Health Record HISP began in February 2012, and testing and account administration were completed in March 2012.

In June 2012, the Florida and Alabama HISPs administratively exchanged and imported their respective trust anchors to establish a connection between the Florida HISP and the Alabama HISP. Both Florida and Alabama HISPs used Direct Domain Name Server (DNS) to discover the appropriate public keys for message encryption and signature verification. Additional technical work involved obtaining the Federal Bridge Certification Authorization (FBCA) certificate in Florida. The test exchange in June used self-signed certificates because of these delays; they were later updated to the FBCA certificate for the Florida health information exchange (HIE) in July.

Not all Technical issues are created equal
In the case of Florida and Alabama's pilot exchange, technical issues that resulted from the first test exchange were easily remedied by optimizing file size and implementing an automatic DNS cache refresh process. More often than not, these technical glitches can, and should be, tackled immediately.

The second phase of the pilot consisted of participant organizations sending interstate messages. Once the organizations agreed on the date and time to initiate exchange, the pilot was carried out as planned. Direct e-mail addresses were exchanged using conventional e-mail on August 25, 2012. The Alabama facility, East Central Alabama Mental Health Authority, sent the first message on August 27, 2012, as scheduled. Florida participants experienced a minor technical delay in successfully receiving the message because the files were too large to pass through the system. File size limits were subsequently increased so that messages could be read. The first message read on August 28, 2012, was from Manatee Glens in Bradenton, Florida.

In a separate test exchange, Apalachee Center, a behavioral health facility in Tallahassee, FL, sent a message on October 2, 2012, to Alabama's One Health Record. A problem in transmission occurred because of the need to refresh the DNS cache in Alabama; the problem was resolved and successful transmission occurred. Subsequently, Alabama

implemented an automatic refresh process. On October 29, 2012, Circles of Care, a behavioral health service provider in Melbourne, FL, also successfully exchanged messages with One Health Record.

Nebraska and Iowa

At the conclusion of the project, Nebraska and Iowa were continuing to work through technical issues complicating Direct exchange across systems. The technology incompatibilities were surmountable, but not within the time constraints of the project.

While Nebraska and Iowa's work with the consortium did not result in a pilot test prior to the conclusion of the project, it did provide Nebraska with the organizational infrastructure (i.e., uniform consent, policies and procedures, and participation agreements) necessary for future work. Once the technical issues are resolved, Nebraska providers will be ready and able to use Direct to exchange behavioral health data. At the time of this report, Nebraska continued to address initial technical barriers and planned to implement their pilot activities during Summer 2013.

New Mexico

In early December 2012, the project team scheduled a call with the IT security specialist and providers to walk through and implement the pilot test. The IT security specialist walked the providers through the process and, with the assistance of the prewritten script, the providers were able to initiate and complete a transfer of test data. The process of initiating and completing the transfer of "test" data took a little more than an hour.

Due to the "live" pilot test implementation, there were periods of inactivity for each provider while information was being uploaded and transferred via Direct exchange to the other provider. It is worth remembering that having both providers present at the same time is not a real-world situation; typically these exchanges will be asynchronous. Providers often complete other tasks while waiting for contact or follow-through on requests for patient information.

Although the providers paid close attention to the entire process, it was not entirely intuitive. Despite having the Provider Notebook on hand, which included a Direct Secure Messaging User Guide, the providers encountered situations when more clarification was needed from the IT security specialist. With continued use, it is likely that the process will become as routine and as reasonably effortless as sending a fax or e-mail.

The project team received feedback from both providers on the Provider Notebook and the pilot implementation process. Both providers stated the pilot implementation process worked well. One provider noted that the Provider Notebook clearly explained how the services can be used and appears to answer any questions clearly. The Behavioral Health provider did not reference 42 CFR Part 2, but referenced the sample consent form provided,

saying it meets the needs of providers transferring and receiving patient specific information that could contain alcohol or substance abuse information. The primary care physician stated that after participating in the pilot project, she became aware of specific standards for 42 CFR Part 2, with which she had not previously been familiar.

The behavioral health provider was excited by the potential benefits of Direct exchange to behavioral and mental health providers: "Opportunities to use this new and much needed system are plentiful. Since the onset of electronic [health] records, confidentiality has changed significantly, especially in the area of releasing records via e-mail or faxing." The provider added that "The product [Direct exchange] is an excellent package for maintaining confidentiality."

Providers need support.
The use of Direct to support the exchange of behavioral health data is a strong use case, given that this data is not widely included in discussions related to more advance query/response HIE systems. It allows data to move quickly, securely, and electronically between providers when there is no large system to support the exchange. However, Direct secure messaging is still in early stages of adoption and as mentioned previously, many providers are not familiar with the 42 CFR Part 2 requirements. Education on both Direct and disclosure requirements for behavioral health data is essential to improving the environment for electronic exchange of the data.

5.2 Successes and Challenges

Demonstrating the ability to exchange behavioral health data electronically is a huge step forward to reduce disparities for patients with specially protected information who have been left out of previous HIE initiatives. This study shows that when data are needed for treatment, no barrier should exist for exchanging that information electronically as long as all parties adhere to the state and federal requirements for the disclosure of that information. As the availability of Direct exchange grows among providers using electronic records and states continue to pursue execution of the governance framework that allows messages to be transmitted between HISPs, behavioral health providers should feel empowered to take advantage of these functionalities.

Although the basic technical and policy barriers were shown to be surmountable, a number of challenges remain to be resolved in future work. EHR systems must begin to provide a mechanism for segmenting and/or flagging data that require specific processes for disclosure or redisclosure. Without such functionality, it is incumbent upon providers to understand the requirements for manually segmenting this data, which creates a barrier and, because of the challenges presented by legal and technical complexity, can erode trust between providers that the data will be handled appropriately. This functionality would also allow for the exchange of structured data that could be incorporated into the receiving provider's system rather than sent in a static format such as PDF.

In addition, widespread understanding and agreement about the requirements for consent and disclosure of behavioral health data are still major challenges to overcome. Although these requirements may be better known to behavioral health specialists, the majority of providers do not know how to appropriately manage the receipt and redisclosure of this information. Participants in this project worked to create materials that helped to de-mystify these requirements and engender trust between providers, but expanding this type of trust environment beyond the pilot projects is a much more significant task. Such expansion will require a significant education campaign and assurance about the appropriate safeguards, particularly as policies and procedures built for a "push" environment using Direct exchange are revised to support robust query-based or "push/pull" models of HIE.

The primary lessons learned through this project include:

1. **Behavioral health data exchange is complex, but possible.**

   This project was successful in proving that specially protected information can be transmitted between states using available electronic HIE technologies. Although initial cultural and technical barriers were significant, clarification of the legal requirements for exchange reassured participants that they could comply with them using an available technological solution. Participants then became more comfortable taking the steps required to exchange behavioral health data. Using Direct messaging as the technical solution to execute the exchange within an appropriate trust environment reduced obstacles to exchange. Technical issues related to the implementation of Direct between states were fairly easy to overcome. Although additional barriers may be encountered as attempts are made to scale this solution more broadly, the project resolved legal and technical barriers to achieving the exchange of behavioral health data electronically both within states and across state lines. This is an initial but essential first step which highlights that behavioral health data can be exchanged using currently available solutions, and should be considered in future HIE plans.

2. **Provider education is key to success.**

   Educational materials and process documentation must be shared with providers to reassure them that required policies and procedures are in place before they will be comfortable engaging in behavioral health data exchange. While the initial goal of the consortium was to develop solutions to the policy and technical issues preventing exchange, a clear finding emerged that provider education was a third and equally important requirement for success. The work on the provider education materials and Provider Notebook is of significant importance moving forward. Having these materials available, along with a process to verify that providers have read and understand them, is essential for the private and secure exchange of behavioral health data. If the success of this project is to be scaled, widespread understanding

within the provider community about proper handling of the data in an electronic environment is required.

3. **Cooperation and flexibility are invaluable when addressing complex problems.**

   Successful pilot implementation would not have been possible without the enthusiastic commitment of consortium participants at the local and state level and the contributions of legal and technical subject matter experts at the national level. Also, the flexible nature of the State Health Policy Consortium support enabled an iterative approach to resolving the complex issues encountered. Support was provided in stages and subject matter experts were added as needed. The flexibility designed into SHPC allowed Nebraska and Iowa to join the consortium midway and make significant contributions. The ability to support the involvement of multiple states at different levels of involvement allowed the overall project to progress, despite the limitations that some states experienced in participating in the pilot test implementation.

5.3 Continuing Work

The work performed during the scope of this project has been a catalyst for additional work that continued during the report writing phase as participants expanded their projects and applied the lessons learned.

The Florida implementation of Direct subsequently connected (HISP-to-HISP) with Direct instances implemented by state programs in Alabama, Georgia, Louisiana, South Carolina, Michigan, West Virginia, and Wisconsin. These connections were a result of the experience gained and lessons learned through the Behavioral Health Data Exchange Consortium project. Direct messages can now be sent by providers using these services at any time to facilitate care coordination interstate for real-life patients. Perhaps more importantly, these connections have allowed these states to be much more prepared to share patient information if large numbers of citizens are displacement by a potential hurricane or natural disaster.

In Michigan, MiHIN Shared Services planned to pilot the exchange of behavioral health information with a sub state HIE and behavioral health provider. MiHIN hopes to conduct two small scale pilots related to consent management that will be evaluated and discussed within the behavioral health community before wider adoption. In preparing for the pilot, the MiHIN shared services team met to coordinate their activities with behavioral and mental health providers, representatives from HIEs across Michigan, public health, consumers, FQHCs and behavioral and mental health departments from the Michigan Department of Community Health.

6. RECOMMENDATIONS

The work completed under the Behavioral Health Data Exchange (BHDE) Consortium project took important steps toward demonstrating the ability to exchange behavioral health data across state lines in an electronic environment. These exchanges currently happen in a paper environment, but a number of technical, policy, and educational initiatives need to be advanced in order to realize the vision of including behavioral health data in electronic health information exchange (HIE) activities.

Including Behavioral Health Data Exchange in Discussions about Scalable Trust

Ongoing activities to establish policies and procedures for connecting health information organizations on a large scale to enable a nationwide network of exchange partners do not include specific consideration of specially protected behavioral health information. For example, the Data Use and Reciprocal Support Agreement (DURSA) was established as the trust agreement put forward by the previous Nationwide Health Information Network (NwHIN) initiative of the Office of the National Coordinator for Health IT (ONC) (now the eHealth Exchange, which is operationally supported by Healtheway[10]), but it does not include any language related to the exchange of behavioral health data. Similarly, initiatives working on the governance and certification of exchange partners have yet to include discussions related to policies that may govern the exchange of behavioral health data. For the electronic exchange of health information to become truly standardized, work in this area must include consideration of the additional requirements placed on the exchange of data covered by 42 CFR Part 2.

Increase Functional Understanding of Exchanging Behavioral Health Data

General knowledge regarding disclosure and re-disclosure requirements is essential to establishing broader acceptance of the exchange of behavioral health data. There are still significant cultural barriers to the exchange of these data, both from those who are not aware of the regulations and from those who are aware but are fearful that potential trading partners will mishandle the data. Although the receiving provider is responsible for adhering to storage and consent requirements, both partners should establish a sense of trust so that the giving provider will recognize the receiving provider as an appropriate steward of this specially protected information. There is an urgent need for training within the general health care (or primary care) provider population regarding what is allowable in terms of document storage and appropriate access controls for data flagged with behavioral health information.

[10] http://www.healthewayinc.org/index.php/about

Patients will also have increasing control over their general health data and eventually over their behavioral health data. Because of this, patients will need to be educated on the implications of consenting to share health information in general and behavioral health information in particular. Patients need to know what protections they can expect and demand from providers to increase their comfort with exchange. The state designated entities for HIE could pursue establishing partnerships with large national medical associations, patient advocacy groups, and ONC's eConsent project to develop and test patient education materials to guide their consent choices. This could be a significant step forward for integrating the exchange of behavioral health data into overall exchange activities.

Aligning Policy with Technical Capabilities

While electronic health record (EHR) technical solutions must be put forward that allow for the transfer, acceptance, and storage of this data in a way that is compliant with 42 CFR Part 2, the policies that govern the exchange between partners are complex and must be addressed. Initiatives to establish the technical capacity to segment machine-readable data for purposes of storage and transport will greatly increase the comfort level of providers in exchanging specially protected information. This capacity has the potential to increase the movement of behavioral health information while making it possible to protect the information appropriately. The Substance Abuse and Mental Health Services Administration (SAMHSA), under its Health Information Technology strategic initiative, currently supports a set of pilot projects looking at issues related to common disclosure consent forms, notification of prohibition of re-disclosure and consent management strategies as well as structured data exchange in a more robust HIE framework in which both push and pull options are available for behavioral health data.

Conclusion

This project provides an initial step forward for the exchange of behavioral health data, but more work is needed to realize the full integration of the behavioral health patient and provider network into the broader HIE landscape. Without specific inclusion of the needs and concerns related to the exchange of behavioral health data, it will be difficult for the current HIE framework to provide equitable solutions to those seeking to link behavioral health services with the primary care system, and people with behavioral and substance abuse treatment needs could be left behind by efforts to create nationwide HIE.

ATTACHMENT 1
BEHAVIORAL HEALTH USE CASES

1. Behavioral health provider (provider is a Part 2 program as well as a mental health provider) in one state needs patient information from a behavioral health provider in another state in order to treat the patient

Description:

Patient has temporarily relocated to Florida from Michigan. Patient informs behavioral health center in Florida about prior treatment at behavioral health center in Michigan. Behavioral health center in Florida requests patient information from behavioral health center in Michigan. Behavioral health center in Michigan sends patient treatment records to behavioral health center in Florida via DIRECT messaging.

Sample Flow:

A behavioral health center in Florida is receiving patient's information from a behavioral health center in Michigan via NwHIN DIRECT.

1. Jane Patient temporarily relocates from Michigan to Florida for the winter.
2. Jane Patient informs the Florida Snowbird Community Mental Health Center in Florida that she received treatment from the Michigan Snowflake Community Mental Health Center.
3. The Florida Snowbird Community Mental Health Center has Jane Patient sign a patient consent form[11] to enable it to request her health records from the Michigan Snowflake Community Mental Health Center.
4. The Florida Snowbird Community Mental Health Center scans Jane Patient's signed patient consent form into their computer system.
5. The Florida Snowbird Community Mental Health Center logs into its HISP of choice and looks up the NwHIN DIRECT e-mail address for the Michigan Snowflake Community Mental Health Center.
6. The Florida Snowbird Community Mental Health Center then creates an e-mail, attaching Jane Patient's signed patient consent form, requesting Jane Patient's health records from Michigan Snowflake Community Mental Health Center and sends the secure e-mail through its HISP via DIRECT.
7. The Michigan Snowflake Community Mental Health Center receives the NwHIN DIRECT e-mail.
8. After reviewing the e-mail and attached signed patient consent, the Michigan Snowflake Community Mental Health Center replies to the e-mail using its NwHIN DIRECT HISP attaching Jane Patient's health records requested in the patient consent. Such reply e-mail would also contain the language required on the prohibition against redisclosure.
9. The Florida Snowbird Community Mental Health Center receives and opens the e-mail and attachment.
10. The Michigan Snowflake Community Mental Health Center would receive a return receipt.

[11] "Patient consent form" in these use cases refers to a written form signed by the patient, or the authorized legal representative of the patient, in which the form complies with 42 CFR Part 2 and complies with the particular state's behavioral health law for disclosure of patient health data between treating health care providers for purposes of treating the patient.

2. Behavioral health provider (provider is a Part 2 program as well as a mental health provider) sends patient data to patient's primary care physician upon conclusion of treatment

Description:

Patient is seen for treatment at either an in-patient or out-patient behavioral health facility in New Mexico. Upon completion of the stay/visit, the behavioral health facility asks the patient whether they want the facility to send a summary of the patient's treatment data (e.g., clinical summary and/or care plan) to the patient's primary care physician (or could send to a specialist like a psychiatrist). Patient says "yes" and signs a patient consent form[12]. The facility then sends the patient's data via DIRECT messaging to the patient's primary care physician in Kentucky. Note that the patient had submitted clarifying information to the New Mexico provider for their records.

Sample Flow:

A behavioral health facility pushes a care summary to the patient's PCP upon completion of treatment.

1. Jane Patient is admitted to Sunrise Behavioral Health Center, an in-patient facility, and treated for addiction and mental health issues.
2. Jane Patient submits clarifying information to the Sunrise Behavioral Health Center about her mental health issues that are recorded in the center's records.
3. Jane Patient completes her treatment at Sunrise Behavioral Health Center and is going through the discharge process.
4. The discharge nurse at the Sunrise Behavioral Health Center asks Jane Patient if she wants to send a copy of her clinical records and care plan to Jane's primary care physician in Kentucky.
5. Jane Patient agrees and signs a patient consent form.[13]
6. The Sunrise Behavioral Health Center staff look up Jane's primary care physician DIRECT e-mail address and sends a secure e-mail via its HISP via DIRECT to Jane's primary care physician along with the language required on the prohibition against redisclosure and the patient-submitted clarifying information and related notice.
7. Jane Patient's primary care physician receives and opens the e-mail and attachment.
8. A read receipt is sent to the Sunrise Behavioral Health Center, informing them that their message has been received and opened by Jane Patient's primary care physician in Kentucky.

[12] Id.
[13] Id.

3. Referral from primary care provider to behavioral health provider (behavioral health provider is a Part 2 program as well as a mental health provider)

Description:

Patient is seen by her primary care provider. Primary care provider determines that a referral to a mental health center, specializing in treatment for addiction, is warranted. Primary care physician sends a clinical summary of his/her concerns to the behavioral health provider. The patient presents for treatment at the mental health center.

Sample Flow:

A referral from a primary care physician in Alabama to a behavioral health provider in Florida.

1. Jane Patient is seen by her primary care provider.
2. The primary care provider has concerns about Jane Patient's health and recommends that she see XYZ community health center for treatment for addiction to cocaine and for mental health problems.
3. Jane Patient agrees.[14]
4. The primary care provider looks up the XYZ community health center's DIRECT e-mail address and sends a secure e-mail to accomplish the referral via its DIRECT HISP to XYZ community health center along with a summary of his concerns and a copy of Jane's relevant clinical records.
5. The XYZ community health center receives and opens the e-mail and attachment(s).
6. A read receipt is sent to Jane's primary care provider, informing them that their message has been received and opened by XYZ community health center.
7. Jane Patient arrives at XYZ community health center for treatment.

[14] May or may not need patient consent prior to disclosure. TBD.

OUT OF SCOPE, but by identified by states as an important use of Direct messaging:

Use of Direct messaging for exchanging patient health data and/or submitting periodic reports for purposes of payment and eligibility determinations. Examples include: secure communication between payer and provider to send information that is needed for a determination of medical necessity or for finding a behavioral facility out of state. The group believed that using Direct would be a more secure way to accomplish these administrative tasks than the current method of faxing the relevant documents.

Correlation to ONC DIRECT Use Case Stories (as of Nov. 26, 2011):

BHDE Use Case No.	Description	Related ONC DIRECT Use Case No.	Description
1	Behavioral health provider in one state needs patient information from a behavioral health provider in another state in order to treat the patient	1	Could be related to ONC DIRECT use case #1 "Primary care provider refers patient to specialist including summary care record", except that our scenario does not assume a prior referral, and our actors are two behavioral health providers, rather than a PCP and a specialist. In addition, our scenario has two-way communication (first the request, and second the response with the patient data).
2	Behavioral health provider sends patient data to patient's primary care physician upon conclusion of treatment	2, 11	Could be related to ONC DIRECT use case #2 "Specialist sends summary care information back to referring provider", except that our scenario does not assume a prior referral, and the "specialist" would be the behavioral health provider. Could also be related to ONC DIRECT use case #11 "Hospital sends discharge information to referring provider", except that our scenario does not assume a prior referral, and the "hospital" could be an in-patient behavioral health provider
3	Referral from primary care provider to behavioral health provider	1, 3	Could be related to ONC DIRECT use case #1 "Primary care provider refers patient to specialist including summary care record", except that we are assuming that the specialist is a behavioral health provider. Could be related to ONC DIRECT use case #3 "Primary care provider refers patient to hospital including summary care record", except that our scenario does not specify if the behavioral health provider is an in-patient facility or not.

ATTACHMENT 2
STATE LAW SUMMARY

Behavioral Health Data Exchange Consortium

Summary of State Laws

Question: Does this state's laws require patient consent or authorization to enable disclosure of patient's health data to another treating healthcare provider?[15]

Note: question excludes psychotherapy notes as defined by HIPAA.

State	Substance Abuse Treatment Facilities	Emergency Exception for Substance Abuse?	State Mental Health Law	Emergency Exception for Mental Health?	Consent Elements?	Other
Alabama	Yes, state law defaults to Part 2	Yes, state law defaults to Part 2	No, patient consent is not required (except communications between the psychiatrist or psychologist or psychological technician)	No, patient consent is not required	None specified	—

[15] States use various terms to refer to the concept of obtaining approval from a patient to share health information with an outside party, including "consent," "authorization," and "release." Under the HIPAA Privacy Rule, the terms "consent" and "authorization" mean two different things. The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain a patient "consent" for uses and disclosures of protected health information for treatment, payment, and health care operations. See 45 C.F.R. § 164.506(b). Covered entities that do so have complete discretion to design a process that best suits their needs. By contrast, an "authorization" is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. See 45 C.F.R. § 164.508(a). An authorization is a detailed document that must contain specific elements set forth in the Rule. See 45 C.F.R. § 164.508(c). Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. We use the term consent to refer to this concept generally, unless we are directly quoting a state statute or regulation.

State	Substance Abuse Treatment Facilities	Emergency Exception for Substance Abuse?	State Mental Health Law	Emergency Exception for Mental Health?	Consent Elements?	Other
Florida	Yes, written consent required; references federal law	Yes, disclosure without patient consent permitted "to medical personnel in a medical emergency"	Yes. Cannot disclose unless patient "authorizes the release"	No, disclosure without patient consent permitted: if treating the patient for an emergency medical condition and provider is unable to obtain consent due to patient's condition or the nature of the situation requiring immediate medical attention. "Emergency medical condition" has a detailed definition. Also yes if patient has declared an intention to harm other persons and the disclosure is to provide adequate warning to the person threatened with harm.	None specified, but statute references voluntary universal patient authorization form promulgated by AHCA	—
Kentucky	Yes, state law defaults to Part 2	Yes, state law defaults to Part 2	Yes, patient consent required for disclosure to another treating provider	No provisions specific to mental health emergencies; falls under general waiver of consent for emergency treatment	None specified	Plan to introduce legislation in 2012 session to allow disclosure on mental health records for treatment

State	Substance Abuse Treatment Facilities	Emergency Exception for Substance Abuse?	State Mental Health Law	Emergency Exception for Mental Health?	Consent Elements?	Other
Michigan	Yes, consent required for disclosure to health professionals for the purpose of diagnosis or treatment of the individual.	Yes, disclosure without patient consent "To medical personnel to the extent necessary to meet a bona fide medical emergency."	Yes, patient consent required for disclosure to another mental health treating provider (interpreted as permitting disclosure to other types of treating providers with consent too)	No, disclosure without patient consent "if there is a compelling need for disclosure based upon a substantial probability of harm to the recipient [patient] or other individuals"	For substance abuse, § references federal law	—
New Mexico	Nothing more restrictive than Part 2 found	Nothing more restrictive than Part 2 found	Yes, patient authorization is required, except in limited circumstances to another treating mental health provider	No, disclosure without patient authorization is permitted when such disclosure is necessary to protect against a clear and substantial risk of imminent serious physical injury or death inflicted by the patient on the patient's self or another	For mental health disclosures, consent needs to be in writing and signed, and must contain a statement of the patient's right to examine and copy the info to be disclosed, the name and title of the proposed recipient and a description of the use that may be made of the info	For mental health treatment records, additional requirement of the sending provider to include any clarifying or correcting statements of the patient and other documentation of reasonable length provided by the patient along with the mental health treatment records.

Citations of State Laws

State	Substance Abuse Treatment Facilities	Emergency Exception for Substance Abuse?	State Mental Health Law	Emergency Exception for Mental Health?	Consent Elements?	Other
Alabama	None. Follows federal law	None. Follows federal law	Ala. Code 34-26-2	None. Follows federal law	None specified.	—
Florida	FS §397.501(7)(a)	FS §397.501(7)(a)(1) & (2)	FS §394.4615(2)(a)	FS 408.051(3) and FS 395.002(8) and FS 394.4615(3)(a)	FS 408.051(4) and Florida rules	—
Kentucky	KRS 222.271; 908 KAR 1:320	—	KRS 210.235(1)	None	n/a	SB125 (proposed legislation)
Michigan	MCL 333.6112	MCL 333.6113	MCL 330.1748(1),(6), & (7)	MCL 330.1748(7)	MCL 333.6112	—
New Mexico	n/a	n/a	NMSA 43-1-19	NMSA 43-1-19	NMSA 43-1-19 (C)	NMSA 43-1-19 (D)

ATTACHMENT 3
ANALYSIS OF SECOND SET OF SAMHSA FAQS RELEASED DECEMBER 9, 2011 AS APPLIES TO PROJECT SCOPE

ANALYSIS OF 2ND SET OF SAMHSA FAQS RELEASED DECEMBER 9, 2011 AS APPLIES TO THE SCOPE OF THIS PROJECT

The following is a brief analysis of the second set of FAQs released by SAMHSA on December 9, 2011, as relevant to our project's Draft Policies and Procedures. Each numbered item below corresponds to the FAQ Question and Answer number. This analysis is for informational purposes only and is not meant to provide legal advice. The analysis was conducted by subject matter experts for the Behavioral Health Data Exchange Consortium. The analysis has not been confirmed by the Department of Health and Human Services.

SAMHSA FAQ		SHPC Analysis
Q1.	**When a patient has signed a consent form allowing disclosure to multiple parties, can the patient revoke consent for disclosure to one or more of those parties while leaving the rest of the consent in force?**	Does not directly apply.
A1.	Yes. Under 42 CFR Part 2 (hereafter referred to as "Part 2"), a patient can revoke consent to one or more parties named in a multi-party consent form while leaving the rest of the consent in effect. In a non-Health Information Exchange (HIE)[16] environment, this can be accomplished simply by the Part 2 program indicating on the consent form or in the patient's record that consent has been revoked with respect to one or more named parties. In an HIE environment, the revocation with respect to one or more parties should be clearly communicated to the Health Information Organization (HIO)[17] as well as noted in the patient's record by the Part 2 program. To ensure compliance with consent requirements, an HIO should have policies and procedures in place for implementing patient decisions to give and revoke consent. Once a patient has revoked a Part 2 consent with respect to one or more parties, that revocation should be immediately communicated to the HIO by the entity obtaining the patient's revocation so that it implements the revocation decision and no longer transmits the Part 2 program's protected patient information to those one or more parties. Part 2 permits a patient to revoke consent orally [42 CFR §2.31(a)(8),(c)(8)]. While oral revocations must be honored under Part 2, SAMHSA recommends the entity obtaining the revocation get it in writing and/or document the revocation in the patient's record. Part 2 prohibits a program from making a disclosure on the basis of a consent which it knows has been revoked. A program however is entitled to act in reliance on a signed consent prior to a revocation, and such disclosure would not be improper [42 CFR § 2.31(c)(3) and § 2.31(a)(8)]. SAMHSA recommends that a revocation be communicated as soon as practicable to entities relying on such consent. We note that the requirements of the HIPAA Privacy Rule must also be considered. For information on HIPAA, see the HHS Health Information Privacy website at: http://www.hhs.gov/ocr/privacy/index.html or http://www.samhsa.gov/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf	

[16] Health Information Exchange ("HIE") is a generic term that refers to a number of methods and mechanisms through which information can be exchanged electronically.

[17] As used in these FAQs, the term Health Information Organization "HIO" means an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.

SAMHSA FAQ		SHPC Analysis
Q2.	**Does a consent form allowing for a program to disclose Part 2 information remain in effect when the *disclosing* program merges with another or undergoes corporate restructuring?**	Does not directly apply.
A2.	Whether a consent form remains in effect when a program merges with another program or undergoes corporate restructuring depends on how the entity making the disclosure is identified on the consent form. Under Section 2.31(a)(1), the *disclosing entity* can be listed by "specific name or general designation." If a particular program is designated by specific name as the entity permitted to make the disclosure, then the consent form would no longer be valid if the program's name is changed (following a merger or restructuring or for another reason) since the new entity is not identified as the same one that was listed on the consent form. If the disclosing entity is listed by a general designation, such as "any drug or alcohol treatment program that is affiliated with the XYZ HIO," then that consent would continue to be valid if the program making the disclosure merges or undergoes corporate restructuring, assuming the new merged program is also an HIO-affiliated member. Note that section 2.19 sets forth the requirements when a Part 2 program is discontinued or taken over or acquired by another program, as opposed to just undergoing a name change or restructuring. This section provides that a discontinued program or one acquired by another program must purge patient identifying information from its records or destroy the records unless the patient consents to the transfer of his or her records, except to the extent that there is a legal requirement that records be retained. In cases where a *recipient* organization has undergone a name change, whether or not a new consent form is needed depends upon the specific designation made on the original consent. Section 2.31(a)(2) allows for specification of either the name or title of the individual or the name or the organization to which the disclosure is to be made. Therefore, an organizational name change alone may not necessitate a new consent.	

SAMHSA FAQ	SHPC Analysis
Q3. May a Part 2 program disclose patient information to providers of "on-call coverage" pursuant to a Qualified Service Organization Agreement (QSOA)? **A3.** Yes. 42 CFR § 2.11 defines "Qualified Service Organization (QSO)" and lists the types of services that a QSO provides, and further references Qualified Service Organization Agreements (QSOA). Medical services are included on that list and thus a Part 2 program can enter into a QSOA with providers of "on-call coverage." A QSOA is a two-way agreement between a Part 2 program and the entity providing the service, in this case the provider of on-call coverage. The QSOA authorizes communication between those two parties, however the Part 2 program should only disclose information to the QSO that is necessary for the QSO to perform its duties under the QSOA. Also, the QSOA does not permit a QSO to redisclose information to a third party unless that third party is a contract agent of the QSO, helping them provide services described in the QSOA, and only as long as the agent only further discloses the information back to the QSO or to the Part 2 program from which the information originated. For additional information, see FAQ Number 10 of the 2010 FAQs published by SAMHSA and the ONC at: http://www.samhsa.gov/healthPrivacy/docs/EHR-FAQs.pdf. Thus, if a QSOA exists between a Part 2 program and an HIO for services rendered to the program by the HIO, the QSOA would not allow the HIO to redisclose that information to a third party like providers of "on-call coverage." For an HIO to redisclose Part 2 information to providers of "on-call coverage" that are not part of the Part 2 program, a consent form that allows the HIO to make the redisclosures to the providers of "on-call coverage" would be needed. Since "on-call coverage" arrangements are fluid and the identity of the health care provider who is providing the on-call coverage might not be known, the designation of the recipient could be "the health care provider who is providing on-call coverage for the ABC treatment program." By designating the recipient as the "on-call coverage provider," the requirement that the recipient's name or title be listed would be met. Consent for disclosures to providers of on-call coverage can be included in the same consent form used for other disclosures of patient information if the program so chooses. An HIO can also redisclose Part 2 information without patient consent to providers of "on-call coverage" who are part of the Part 2 program or of an entity having direct administrative control over the program, as long as the on-call providers need the information in connection with their duties that arise out the provision of diagnosis, treatment or referral for treatment services [42 CFR § 2.12(c)(3)].	Our consent forms are consistent with this FAQ#3 regarding providers of on-call coverage for recipients

SAMHSA FAQ	SHPC Analysis
Q4. Can a single Part 2 consent form be used to authorize patient information to be exchanged through an HIO's system for different purposes, such as treatment, payment, disease management and/or quality improvement? **A4.** Yes, Part 2 allows the use of a single consent form authorizing the disclosure of Part 2 patient information to different recipients for different purposes. However, Part 2 also requires a consent form to specify the kind and amount of information that can be disclosed to each of the recipients named in the consent. The amount of information to be disclosed "must be limited to that information which is necessary to carry out the purpose of the disclosure" [42 C.F.R. §2.13(a)]. This will vary depending on the different purposes for which different recipients are being allowed access to the information made available through an HIE. Thus the consent form would have to be structured to make it clear what information may be given to which recipients, and for which purposes. The HIE system must also be designed to limit the different recipients' access through the HIE to only the kind and amount of patient information each needs to fulfill the specific purpose for which they are being allowed access.	Does not directly apply since we are only using the data for treatment
Q5. Does Part 2 permit a healthcare provider to disclose information without consent when there is an immediate threat to the health or safety of an individual or the public? **A5.** Part 2 permits the disclosure of information under certain circumstances without consent during a medical emergency or in other limited situations. If a Part 2 program (or a healthcare provider that has received Part 2 patient information) believes that there is an immediate threat to the health or safety of any individual, there are steps described below that the Part 2 program or healthcare provider can take in such a situation: Notifications to medical personnel in a medical emergency: A Part 2 program can make disclosures to medical personnel if there is a determination that a medical emergency exists, i.e., there is a situation that poses an immediate threat to the health of any individual and requires immediate medical intervention [42 CFR §2.51(a)]. Information disclosed to the medical personnel who are treating such a medical emergency may be redisclosed by such personnel for treatment purposes as needed. For additional information regarding disclosures during a medical emergency, see FAQs Numbered 7, 8, and 9 below. Notifications to law enforcement: Law enforcement agencies can be notified if an immediate threat to the health or safety of an individual exists due to a crime on program premises or against program personnel. A Part 2 program is permitted to report the crime or attempted crime to a law enforcement agency or to seek its assistance [42 CFR §2.12(c)(5)]. Part 2 permits a program to disclose information regarding the circumstances of such incident, including the suspect's name, address, last known whereabouts, and status as a patient in the program.	Does not directly apply because we are not addressing emergency scenario

SAMHSA FAQ	SHPC Analysis
A.5. Continued Immediate threats to health or safety that do not involve medical emergencies or crimes on programs premises or against program personnel: Part 2 programs and health care providers and HIOs who have received Part 2 patient information, can make reports to law enforcement about an immediate threat to the health or safety of an individual or the public *if patient-identifying information is not disclosed*. Immediate threats to health or safety that do not involve a medical emergency or crimes (e.g., a fire) are not addressed in the regulations. Programs should evaluate those circumstances individually. Reports of child abuse and neglect: The restrictions on disclosure do not apply to the reporting under State law of incidents of suspected child abuse and neglect to the appropriate State or local authorities. However, Part 2 restrictions continue to apply to the original alcohol or drug abuse patient records maintained by the program including their disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect [42 CFR § 2.12(c)(6)]. Also, a court order under Part 2 may authorize disclosure of confidential communications made by a patient to a program in the course of diagnosis, treatment, or referral for treatment if, among other reasons, the disclosure is necessary to protect against an existing threat of life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect [42 CFR § 2.63(a)(1)]. Court ordered disclosures: Under the regulations, Part 2 programs or "any person having a legally recognized interest in the disclosure which is sought" may apply to a court for an order authorizing disclosure of protected patient information [42 CFR § 2.64]. Thus, if there is an existing threat to life or serious bodily injury, a Part 2 program or "any person having a legally recognized interest in the disclosure which is sought" can apply for a court order to disclose information.	

SAMHSA FAQ	SHPC Analysis
Q6. Under what circumstances can information disclosed pursuant to Part 2 be redisclosed? **A6.** Once Part 2 information has been initially disclosed (with or without patient consent), no redisclosure is permitted without the patient's express consent to redisclose or unless otherwise permitted under Part 2. Disclosures made *with* patient consent must be accompanied by a statement notifying the recipient that Part 2 redisclosure is prohibited, unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by Part 2 (42 CFR § 2.32). When disclosures are made *without* patient consent under the following circumstances, limited redisclosures without obtaining the patient's consent: are permitted, such as medical emergencies [42 CFR § 2.51], child abuse reporting [42 CFR § 2.12(c)(6)], crimes on program premises or against program personnel [42 CFR § 2.12(c)(5)], and court ordered disclosures when procedures and criteria are met [42 CFR §§ 2.61-2.67]. When disclosures are made under the following circumstances the recipient is prohibited from redisclosing the information without consent, except under the following restricted circumstances: Research: Researchers who receive patient identifying information are prohibited from redisclosing the patient-identifying information to anyone except back to the program [42 CFR § 2.52(b)]. Audits and Evaluations: Part 2 permits disclosures to persons and organizations authorized to conduct audits and evaluation activities, but imposes limitations by requiring any person or organization conducting the audit or evaluation to agree in writing that it will redisclose patient identifying information only (1) back to the program, or (2) pursuant to a court order to investigate or prosecute the program (not a patient), or (3) to a government agency that is overseeing a Medicare or Medicaid audit or evaluation [42 CFR § 2.53(c)(d)]. Qualified Service Organization Agreements (QSOAs): Part 2 requires the QSO to agree in writing that in receiving, storing, processing, or otherwise dealing with any information from the program about patients, it is fully bound by Part 2, it will resist, in judicial proceedings if necessary, any efforts to obtain access to information pertaining to patients except as permitted by Part 2, and will use appropriate safeguards to prevent the unauthorized use or disclosure of the protected information [42 CFR § 2.11]. In addition, QSOAs may allow disclosure in certain circumstances. Authorizing Court Orders: When information is disclosed pursuant to an authorizing court order, Part 2 requires that steps be taken to protect patient confidentiality. In a civil case, Part 2 requires that the court order authorizing a disclosure include measures necessary to limit disclosure for the patient's protection, which could include sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered [42 CFR § 2.64(e)(3)]. In a criminal case, such order must limit disclosure to those law enforcement and prosecutorial officials who are responsible for or are conducting the investigation or prosecution, and must limit their use of the record to cases involving extremely serious crimes or suspected crimes. For additional information regarding the contents of court orders authorizing disclosure, see 42 CFR § 2.65(e).	This is consistent with our Policy #5 & 7 on redisclosure and the sample QSOA language

SAMHSA FAQ		SHPC Analysis
Q7.	**How can a Part 2 program ensure that it will be notified that a health care provider invoked the medical emergency exception and gained access to protected Part 2 information?**	Does not directly apply because we are not addressing emergency scenario
A7.	The Part 2 regulations at 42 CFR §2.51 specify that when a disclosure is made in connection with a medical emergency, the *Part 2 program* must document in the patient's record the name and affiliation of the recipient of the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency [42 CFR § 2.51(c)]. See previous FAQs, and specifically, Number 30 of the 2010 FAQs. SAMHSA recommends that HIE data systems be designed to ensure that the Part 2 program is notified when a disclosure occurs and Part 2 records are released pursuant to a medical emergency. To promote compliance, SAMHSA recommends that the notification include all the information that the Part 2 program is required to document in the patient's records (e.g., date and time of disclosure, the nature of the emergency, etc.). Similarly, SAMHSA recommends that the information about emergency disclosures be kept in the HIO's electronic system and protected using appropriate safeguards. Before a Part 2 program enters into an affiliation with an HIO, it should consider whether the HIO system has the capability to comply with all Part 2 requirements, including the capacity to notify the Part 2 program when its records have been disclosed pursuant to a medical emergency. For additional information regarding disclosures during a medical emergency, see the FAQs Numbered 5, 8, and 9.	
Q8.	**What categories of health care professionals are considered "medical personnel" for the purpose of obtaining information during a medical emergency?**	Does not directly apply because we are not addressing emergency scenario
A8.	Part 2 allows patient identifying information to be disclosed to medical personnel in a medical emergency [42 CFR § 2.51]. Part 2 does not define the term "medical personnel" but merely provides that information can be given to medical personnel who have a need for information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention. It is up to the health care provider or facility treating the emergency to determine the existence of a medical emergency and which personnel are needed to address the medical emergency. The name of the medical personnel to whom the disclosure was made, their affiliation with any health care facility, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the medical emergency must be documented in the patient's records by the Part 2 program disclosing them [42 CFR §2.51(c)]. Additional information about disclosures in medical emergencies is found in FAQs Numbered 5, 7, and 9.	

SAMHSA FAQ		SHPC Analysis
Q9.	**Can the Part 2 medical emergency exception be invoked to head off a potential medical emergency such as a potential drug interaction?**	Does not directly apply because we are not addressing emergency scenario
A9.	If a health care provider treating an individual determines that a medical emergency exists as defined in Part 2, i.e., "a condition which poses an immediate threat to the health of any individual [not just the patient], and which requires immediate medical intervention," and in treating the medical emergency the health care provider needs information about potential drug interactions, then that information and any other information contained in the Part 2 record that the treating health care provider determines he or she needs to treat the medical emergency can be disclosed. If no such determination exists, SAMHSA recommends trying to obtain consent from the patient. If a health care provider is treating a patient in a non-emergency situation and the health care provider is concerned about a potential drug interaction, in an HIE environment, an HIO may only disclose a Part 2 program patient's records to a health care provider if the patient signs a consent form releasing the Part 2 record to the health care provider. Such a consent form may already exist if the patient previously signed a Part 2 consent form allowing the HIO to disclose Part 2 information to HIO affiliated health care providers and the provider seeking access is listed as a recipient on that form. A health care provider who is concerned about a potential drug interaction and treating a patient in a non-emergency situation can also gain access to a Part 2 program patient's record if the health care provider has signed a QSOA with the patient's Part 2 program (and the information is limited to what is needed for the provider to provide services to the Part 2 program) or obtains patient consent. In a non-emergency situation, if the health care provider concerned about a potential drug interaction is part of the Part 2 program (or of an entity that has direct administrative control over the program), he or she can gain access to the Part 2 patient's record without consent if the health care provider needs the information to treat the patient. 42 CFR § 2.12(c)(3) does not restrict communications between and among such personnel who have a need for the information in connection with their duties arising out of the provision of diagnosis, treatment or referral for treatment services. It should be noted that concern alone about potential drug interaction may not be sufficient to meet the standard of a medical emergency. Thus, based on the circumstances of the presenting situation, SAMHSA recommends that health care providers should obtain consent from the patient where feasible.	

SAMHSA FAQ	SHPC Analysis
Q10. Do all primary care providers who prescribe controlled substances to treat substance use disorders meet the definition of a "program" under Part 2? **A10.** No. Not every primary care provider who prescribes controlled substances meets the definition of a "program" or part of a "program" under Part 2. For providers to be considered "programs" covered by the Part 2 regulations, they must be both "federally-assisted" and meet the definition of a program under 42 CFR § 2.11. Physicians who prescribe controlled substances to treat substance use disorders are DEA-licensed and thus meet the test for federal assistance [42 CFR § 2.12(b)(2)]. Nevertheless, the regulations establish additional criteria to meet the definition of a "program": 1. If a provider is *not* a general medical care facility, then the provider meets Part 2's definition of a "program" if it is an individual or entity that holds itself out as providing, *and* provides alcohol or drug abuse diagnosis, treatment or referral for treatment. 2. If the provider is an identified unit within a general medical care facility, it is a "program" if it holds itself out as providing, *and* provides, alcohol or drug abuse diagnosis, treatment or referral for treatment. 3. If the provider consists of medical personnel or other staff in a general medical care facility, it is a program if its primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment *and* is identified as such specialized medical personnel or other staff within the general medical care facility. In addition, in explaining Part 2's applicability and coverage, § 2.12(e)(1) states that "coverage includes, but is not limited to, employee assistance programs, programs within general hospitals, school-based programs and private practitioners who hold themselves out as providing, and provide alcohol or drug abuse diagnosis, treatment or referral for treatment" [42 CFR § 2.12(e)(1)].	Does not directly apply

SAMHSA FAQ	SHPC Analysis
A.10. Continued Accordingly, primary care providers who do not work in general medical care facilities meet Part 2's definition of a program if their principal practice consists of providing alcohol or drug abuse diagnosis, treatment or referral for treatment, *and* they hold themselves out as providing the same. If their principal practice consists of providing alcohol or drug abuse diagnosis, treatment or referral for treatment, but they do not hold themselves out as providing those services, then it is likely that they would not meet the definition of a program. The phrase "holds itself out" is not defined in the regulations, but could mean a number of things, including but not limited to state licensing procedures, advertising or the posting of notices in the offices, certifications in addiction medicine, listings in registries, internet statements, consultation activities for non-"program" practitioners, information presented to patients or their families, or any activity that would lead one to reasonably conclude that the provider is providing or provides alcohol or drug abuse diagnosis, treatment or referral for treatment. Further, while the term "general medical care facility" is not defined in the definitions section of 42 CFR 2.11, hospitals, trauma centers, or federally qualified health centers would generally be considered "general medical care" facilities. Therefore, primary care providers who work in such facilities would only meet Part 2's definition of a program if 1) they work in an identified unit within such general medical care facility that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment, or 2) the primary function of the provider is alcohol or drug abuse diagnosis, treatment or referral for treatment and they are identified as providers of such services. In order for a program in a general medical care facility to share information with other parts or units within the general medical care facility, administrative controls must be in place to protect Part 2 information if it is shared. In addition, a practice comprised of primary care providers could be considered a "general medical facility." As such, only an identified unit within that general medical care facility which holds itself out as providing *and* provides alcohol or drug abuse diagnosis, treatment or referral for treatment would be considered a "program" under the definition in the Part 2 regulations. Medical personnel or staff within that facility whose primary function is the provision of those services and who are identified as such providers would also qualify as a "program" under the definition in the Part 2 regulations. Other units or practitioners within that general medical care facility would not meet the definition of a Part 2 program unless such units or practitioners also hold themselves out as providing *and* provide alcohol or drug abuse diagnosis, treatment or referral for treatment	

SAMHSA FAQ	SHPC Analysis
Q11. Is information generated by the provision of SBIRT (Screening, Brief Intervention and Referral to Treatment) services covered by Part 2? **A11.** Screening, Brief Intervention and Referral to Treatment (SBIRT) is a cluster of activities designed to identify people who engage in risky substance use or who might meet the criteria for a formal substance use disorder. Clinical findings indicate that the overwhelming majority of individuals screened in a general medical setting do not have a substance use disorder and do not need substance use disorder treatment. The determination whether patient information acquired when conducting SBIRT services is subject to Part 2 depends on whether the entity conducting the SBIRT activities is a federally-assisted "program" as defined in the regulations. If the entity conducting SBIRT services is not a federally-assisted program, then the SBIRT services and patient records generated by such services would not be covered under 42 CFR Part 2, although HIPAA and state laws may apply. However, if the entity or unit within a general medical care facility conducting the SBIRT services is a federally-assisted program under Part 2, then the SBIRT patient records would be subject to Part 2 regulations. See FAQ Number 10 of these FAQs for a discussion of the definition of a program under 42 CFR Part 2.	Does not directly apply
Q12. What is Part 2's relationship to State laws? **A12.** 42 CFR § 2.20, states that "no State law may authorize or compel any disclosure prohibited by these [Part 2] regulations." However, States may impose additional confidentiality protections. Thus, § 2.20 provides that, "If a disclosure permitted under these regulations is prohibited under State law, neither these regulations nor the authorizing statutes may be construed to authorize any violation of that State law."	Our Policies & Procedures and sample consent forms are consistent with this interpretation. In particular, they acknowledge the fact that the states may have additional requirements for mental health
Q. 13. Would a logon or splash page notification on an HIO's portal that contains the Part 2 notice prohibiting redisclosure be sufficient to meet Part 2's requirement that disclosures made with patient consent be accompanied by such a statement? **A13.** No. Part 2 requires each disclosure made with written patient consent to be accompanied by a written statement that the information disclosed is protected by federal law and that the recipient cannot make any further disclosure of it unless permitted by the regulations (42 CFR § 2.32). A logon page is the page where a user logs onto a computer system; a splash page is an introductory page to a web site. A logon or splash page notification on a HIO's portal including the statement as required by § 2.32 would not be sufficient notification regarding prohibitions on redisclosure since it would not accompany a specific disclosure. The notification must be tied to the Part 2 information being disclosed in order to ensure that the recipient of that information knows that specific information is protected by Part 2 and cannot be redisclosed except as authorized by the express written consent of the person to whom it pertains or as otherwise permitted by Part 2.	This FAQ is consistent with our Policy #5 & 7.

SAMHSA FAQ	SHPC Analysis
Q 14. If a Part 2 program has signed QSOAs with two service providers, can those services providers redisclose Part 2 information to each other? **A14.** No. A QSOA is a two-way agreement between a Part 2 program and the entity providing the service, for example a lab. The QSOA authorizes communication only between the Part 2 program and QSO. The QSO, in this case the lab, would not be allowed to redisclose lab results about the Part 2 program's patient to another QSO such as an HIO, even if the HIO has also signed a QSOA with the Part 2 program. In order for the lab to redisclose Part 2 patient information to the HIO, it would need the patient's signed Part 2 consent or be otherwise permitted by Part 2. One consent form could both authorize the Part 2 program to disclose information to the lab, and authorize the lab to redisclose Part 2 information to the HIO. Once the HIO obtains the lab results it could, through the QSOA it signed with the Part 2 program, send those results to the Part 2 program, assuming that was a service described in the QSOA.	Our Policies & Procedures are consistent with this FAQ, because it is the consent form, rather than the QSOA, that authorizes the disclosure between HISPs who may be QSOAs of the sender and recipient.

SAMHSA FAQ	SHPC Analysis
Q15. If an HIO has a QSOA with a Part 2 program and a patient signs a consent allowing a HIO affiliated provider to gain access to the patient's records through the HIO, does that patient consent allow the HIO to disclose the Part 2 information? **A15.** Yes, as long the consent form signed conforms to the requirements of Part 2. (See previously issued FAQ Number 11 published by SAMHSA and ONC in 2010 for a list of the required elements of a patient consent under Part 2: http://www.samhsa.gov/healthprivacy/docs/EHR-FAQs.pdf). A QSOA does not allow a QSO such as an HIO to redisclose Part 2 information to a third party, except to a contract agent of the HIO if it needs to do so in order to provide the service(s) described in the QSO. However, if a patient signs a consent form authorizing the HIO, which has received the disclosed information from the Part 2 program, to redisclose the Part 2 information to a HIO affiliated member, then the Part 2 information can be redisclosed by the HIO. Part 2's consent provision requires that a consent form include the "specific name or general designation of the program or person permitted to make the disclosure" [42 CFR Part 2, § 2.31(a)(1)]. In the case where Part 2 information is made available to an HIO, whether through a QSOA or written patient consent, the consent form allowing the HIO to redisclose the Part 2 information must identify by name or general designation the Part 2 program(s) as the entity permitted to make the disclosure of the Part 2 information. This is because, while the HIO is redisclosing the Part 2 information, the disclosing entity remains the Part 2 program. The consent can also name the HIO as a redisclosing party. As noted above, the disclosing Part 2 program may be identified either by its specific name or by "general designation." Language such as "all programs in which the patient has been enrolled as an alcohol or drug abuse patient" would be an acceptable general designation.	Our Policies & Procedures are consistent with FAQ #15 & 16. Our Policies & Procedures and sample consent forms *do* name the recipient specifically. Consent Form A specifically names the disclosing party, while Consent Form B includes a general designation of the disclosing party that complies with this FAQ explanation of "general designation." The FAQ #15 provides acceptable sample language for "general designation" as follows: "all programs in which the patient has been enrolled as an alcohol or drug abuse patient". Our Consent Form B does not use this exact language, but it does specifically name "substance abuse treatment programs." This language should be equivalent and also acceptable, but Consortium members should advise whether they would like to change Consent Form B to include the exact sample language from the last paragraph of FAQ #15.

SAMHSA FAQ	SHPC Analysis
Q16. Under Part 2, can an HIO or HIO affiliated member use a consent form that generally designates the entities permitted to make disclosures of Part 2 information, and refers to the HIO's website for a list of those disclosing entities? **A16.** Yes, the consent form can refer to the HIO's website for the list of entities permitted to make disclosures if the *disclosing entity* is identified by a "general designation" in the consent form as permitted under Part 2. Part 2's consent provisions allow either the "name or general designation of the program or person permitted to make the disclosure" to be specified on the consent form. Because a general designation is permitted, if such general designation is used, then the specific names of those disclosing entities do not need to be included on the consent form and patients can be referred to the HIO's website for a list of those entities. This is in contrast to Part 2's consent provision regarding *recipients* of Part 2 data. 42 CFR §2.31(a)(2) requires that a consent form include "the name or title of the individual or the name of the organization to which disclosure is to be made." Thus, as was previously noted in previously issued FAQ Number 18 published by SAMHSA and ONC in 2010 (http://www.samhsa.gov/healthPrivacy/docs/EHR-FAQs.pdf), Part 2 consents cannot refer patients to the HIO's website for a list of potential recipients of their data but rather must identify within the consent all the HIO affiliated members by name or title that are potential recipients of the Part 2 data. Therefore, a new consent form (e.g. by the additional Part 2 program or the HIO) would be required when a new recipient of the information is added.	Our Policies & Procedures are consistent with this FAQ, because our Policies & Procedures and sample consent forms do not permit disclosure to future, unnamed recipients.

ATTACHMENT 4
BEHAVIORAL HEALTH DATA EXCHANGE CONSORTIUM FINAL POLICIES AND PROCEDURES

BEHAVIORAL HEALTH DATA EXCHANGE CONSORTIUM

1. INTRODUCTION

The draft policies and procedures set out in this document are intended to facilitate the exchange of patient health data between behavioral health providers (substance abuse treatment and/or mental health providers) and other providers for the purposes of treating the patient. These policies and procedures are designed to be flexible and replicable in other states.

These draft policies and procedures are limited in scope to the Behavioral Health Data Exchange Consortium project scope: policies and procedures to enable behavioral health providers to participate in interstate health information exchange for patient treatment purposes using the push transaction model via NwHIN DIRECT protocols. Specifically excluded from the scope of this project are the exchange of psychotherapy notes (as defined in the HIPAA Privacy Rule); laws specific to minors; the exchange of other sensitive data such as HIV, STDs, family planning, etc.; and data from educational institutions. Also, the team decided not to address disclosure in emergency situations.

The team was guided by the following principles when developing these draft policies and procedures:

- Limit policies and procedures to the scope of the project
- All HIEs, are HIPAA business associates, and therefore are bound by their Business Associate Agreements which set requirements under which they must comply with and are directly liable for violations of the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule, our focus should be on issues unique to behavioral health.
- Focus on meeting minimum requirements of federal and state law; anticipate future influencing factors balanced with scope limits
- Focus on policies and procedures that are feasible and practical for providers to implement
- Policies and procedures can provide more than one option to choose from on how to implement
    - Should state the legal requirement (bottom line rules) and then be flexible in how to implement the requirements.
- Review existing materials
- Consensus approach to drafting policies and procedures

This Version 2 Draft Policies and Procedures is intended to be used in the participating states' internal review process and pilot planning purposes. Ms. Prescott and LAC have incorporated comments from the December 13, 2011 in-person meeting. An analysis was completed of the newly released second set of Frequently Asked Questions (FAQs) from SAMHSA regarding 42 CFR Part 2 and health information exchange. Thus, we believe this version 2 Draft Policies and Procedures is consistent with both the first and second set of FAQs from SAMHSA.

2. DISCLAIMER

The authors have attempted to assure that the information presented is accurate as of January 1, 2012. The information in this document is intended to provide a basis for minimum policies and procedures that would be used in pilot demonstrations with test data and would be in addition to other policies and procedures that the organizations would have in place (e.g., HIPAA Privacy and Security Rules). Sample policies and/or forms provided are not meant to guarantee compliance with applicable law or regulations. They should not be used as a substitute for legal or other expert advice. Statements in the document should not be construed as an endorsement by the U.S. Department of Health and Human Services. This report does not contain any individually identifiable information.

3. ASSUMPTIONS

1. The sender and receiver have other policies and procedures in place covering other requirements, such as HIPAA Privacy and Security Rules.
2. The sending and receiving parties are capable of operationalizing these basic minimum policy requirements below.
3. The sender and recipient of the patient request and patient data are both utilizing the DIRECT protocols and complying with all DIRECT policies and procedures (e.g., the DIRECT end user must not permit other unauthorized persons to logon to, or otherwise access, his/her/its DIRECT email account; audit trails are kept; acknowledgement of message receipt is implemented).
4. The DIRECT protocol and how the sender and receiver have established their DIRECT interconnection handles proper authentication of the DIRECT end users.
5. Both the sender and the receiver are or have been in a treatment relationship with the patient who is the subject of the requested disclosure (as Treatment is defined in the HIPAA Privacy Rule).
6. States use various terms to refer to the concept of obtaining approval from a patient to share health information with an outside party, including "consent," "authorization," and "release." Under the HIPAA Privacy Rule, the terms "consent" and "authorization" mean two different things. The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain a patient "consent" for uses and disclosures of protected health information for treatment, payment, and health care operations. See 45 C.F.R. § 164.506(b). Covered entities that do so have complete discretion to design a process that best suits their needs. By contrast, an "authorization" is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. See 45 C.F.R. § 164.508(a). An authorization is a detailed document that must contain specific elements set forth in the Rule. See 45 C.F.R. § 164.508(c). Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. We use the term consent to refer to this concept generally, unless we are directly quoting a state statute or regulation.
7. The patient data being requested or sent in the DIRECT message is behavioral health data.
8. Disclosures for emergency medical treatment are **not** addressed in these policies and procedures.

9. The sending healthcare provider may utilize a HISP or a HIO. A HISP is a Health Information Service Provider. A HIO is a Health Information Organization. In this document, HISP and HIO will be used interchangeably to refer to a third party legal entity that is performing a service on behalf of the health care provider, such as routing the DIRECT message to the recipient.
10. The receiving healthcare provider may utilize a HISP or a HIO.
11. There could be more than two HISPs or HIOs involved in the activities of sending and receiving DIRECT messages.

4. DRAFT POLICIES AND PROCEDURES

The following policies and procedures represent minimum policies that apply to behavioral health data disclosure only. **Note that compliance with ALL of these policies would be required at a minimum**. Participation/subscription agreements[18] utilized by the pilot sites may be used to implement minimum policies and procedures, or the pilot site may use other methods for operationalizing the policies and procedures.

1. **MINIMUM POLICY REQUIREMENT**: If a third party HISP is used for transfer of the DIRECT message that contains patient data covered by 42 CFR Part 2 (substance abuse treatment data), then the following analysis must take place to determine whether a QSOA (Qualified Services Organization Agreement[19]) must be put in place between a Part 2 program who is a DIRECT message sender and its HISP providing the service to transport the DIRECT message[20]:

    a. Background: If a third party (e.g., a HISP or a HIO) is performing a service on behalf of a Part 2 program that involves access to patient health data, then the third party may not have access to the data unless one of the following occurs:

        i. The third party has entered into a Qualified Services Organization Agreement (QSOA) with the Part 2 program for which it provides DIRECT messaging services, OR

        ii. The third party could only have access to the patient data protected by Part 2 with a specific patient consent naming the third party (e.g., a consent naming a HIO and permitting it to have access to the patient data for certain purposes specified in the consent form).

[18] Participation/subscription agreements refer to the legal contracts between the entity providing the DIRECT messaging service and the participating healthcare providers who are DIRECT users.
[19] A QSO is similar to a HIPAA Business Associate (and could be a business associate as well), where the QSO performs services on behalf of the Part 2 program and is also required to fully comply with 42 CFR Part 2. A QSO is defined in 42 CFR §2.11 as: a person – i.e., an individual, partnership, corporation, federal, state or local government agency, or any other legal entity – that "provides services to a [Part 2] program, such as data processing, …" and "has entered into a written agreement with a [Part 2] program." The written agreement must include an acknowledgement that in receiving, storing, processing, or otherwise dealing with any patient records from the program, the person is fully bound by Part 2 and, if necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part 2 regulations. Sample QSOA language is included in the last section of this document.
[20] A QSOA is not necessary between the sending Part 2 program and "downstream" HISPs, other than its own HISP.

b. Specific Application (HISP as mere transport): If the third party HISP merely serves as the transport mechanism for the encrypted DIRECT message that contains the Part 2 patient data, and cannot open or unencrypt such DIRECT message, and does not have access to the contents of the DIRECT message, and does not host an email client for the DIRECT user (e.g., does not provide a web portal with email capability), and does not exercise control over or govern the exchange of data, then the HISP would not need to enter into a QSOA with each Part 2 program DIRECT user because the HISP's role would be similar to the post office or FedEx courier function.

c. Specific Application (HISP providing more than mere transport): If the third party HISP provides more than mere transport of encrypted data as mentioned above, then the HISP must :

   i. Enter into a Qualified Services Organization Agreement (QSOA) with the DIRECT healthcare provider who is the sender or receiver of DIRECT message(s) containing Part 2 data, OR

   ii. Obtain written patient consent form, compliant with 42 CFR Part 2, that authorizes the Part 2 program to disclose the patient's information to the HISP. In other words, there would be a consent signed naming the HISP as being authorized to have access to the patient data.

   Note: The above only authorizes the message transmission between the Part 2 provider DIRECT user and its HISP. In order for the Part 2 program's HISP to be authorized to make further disclosure, there must be a written, signed Part 2-compliant consent form naming the recipient provider (which is discussed in Minimum Policy Requirement #2 below).

2. **MINIMUM POLICY REQUIREMENT**: Behavioral health data that requires special protection and patient consent under federal or state law will only be exchanged after an appropriate written patient consent form has been signed.

   a. Specific Application (Part 2 consent form elements): The patient consent form must meet the 42 C.F.R. Part 2 requirements if patient data to be requested or shared comes from a program that is subject to 42 CFR Part 2 (certain federally funded drug and alcohol treatment programs). To be compliant with 42 CFR Part 2, the written consent form must contain the following 9 elements:

      i. The specific name or general designation of the program or person permitted to make the disclosure;

      ii. The name or title of the individual or the name of the organization to which disclosure is to be made;

      iii. The name of the patient;

      iv. The purpose of the disclosure;

      v. How much and what kind of information to be disclosed;

vi. The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under §2.15 in lieu of the patient;

vii. The date on which the consent is signed;

viii. 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 disclosure information to a third party payer; and

ix. The date, event or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

b. Specific Application (consent form elements for disclosure of mental health data): The patient consent form must meet any applicable state law requirements (such as mental health law) if any patient data to be requested or shared is subject to special protection under state law. For our participating states:

i. All of the participating states, except one (Alabama), required patient consent prior to disclosure of mental health treatment records.

ii. Only one of the participating states specified certain elements for a patient consent [21]for the disclosure of mental health treatment records: New Mexico required that the patient consent be 1) in writing and signed, and 2) contain a statement of the patient's right to examine and copy the information to be disclosed, the name and title of the proposed recipient of the information and a description of the use that may be made of the information.

iii. One state, New Mexico, also gave the patient a right to submit (to the mental health provider who is the source of the record) clarifying or correcting statements and other documentation of reasonable length for inclusion with the confidential mental health treatment records. Any disclosure of the mental health treatment records would also have to have such patient-supplied information accompanying it.

[21] Some statutes (like 42 CFR Part 2) refer to the document that the patient signs giving their permission to disclose their health data a "consent," while some other statutes (e.g., Florida's) may refer to such document as an "authorization" or other state statutes (e.g., New Mexico's) use both terms "consent" and "authorization."

iv. One state, Florida, has a standard form for patient authorization[22] (consent) that can be used on a voluntary basis. Use of the form does provide some immunity protections.

c. Specific Application (consent form scope to include recipient's HISP): If the sender (the entity making the disclosure) is a Part 2 program, and the consent form lists the recipient provider (but does not list the recipient provider's HISP by name), then the consent form should specify that disclosure is permitted to the recipient or the recipient's agents, QSOs, business associates, medical staff, etc. of such recipient. See examples of consent forms in Attachment A and B to this document and as further explained below.

d. Specific Application (no prescribed consent form): The FAQs released by SAMHSA in June 2010 (Set One FAQs) and the second set of FAQs released by SAMHSA in December 2011 (Set Two) provide additional guidance on different approaches for the consent form. Several different formats for a consent form can be used, as long as the minimum elements are included. None of the participating states required use of any particular state consent form. Thus, there are several different options for a consent form that senders and recipient DIRECT users could employ to transfer behavioral health patient data for treatment purposes. Some sample patient consent forms are provided as Attachment A and B to this document, as explained further below.

e. Specific Application (multiple disclosures under one consent form): SAMHSA Set One FAQ #21 and Set Two FAQ #1 confirm that under a Part 2 patient consent, patient health data may be disclosed multiple times, as long as the consent has not yet expired and the entities to whom the information is to be disclosed are the same recipients named in the consent, the nature of the information, and the purpose for the disclosure specified in the consent form are still the same. A separate consent form does not need to be obtained each time a disclosure of Part 2 records is made.

f. Specific Application (consent form not permitted to reference website for list of recipients): SAMHSA Set One FAQ #18 and Set Two FAQ #16 confirm that to be a Part 2-compliant consent form, it may not simply reference a website for a list of providers who are authorized to be recipients of a patient's health data covered by Part 2. Similarly, Set One FAQ #19 and Set Two FAQ #16 say that it is not acceptable to include future unnamed affiliated providers as potential recipients to whom the disclosure of the Part 2 data is to be made.

g. Specific Application (e-consent): SAMHSA Set One FAQ #15 confirms that an electronically signed consent form would also be allowable, provided it is valid under applicable law. In our DIRECT messaging case, the applicable law would likely be the sender's state law and the recipient's state law.

h. Specific Application ("original" signature not required): SAMHSA Set One FAQ #15 confirms that Part 2 does not require a patient's "original" signed consent form to be in the possession of the sender or recipient in order to make a

disclosure of Part 2 patient data. A sender or recipient may accept a copy of a signed consent form.

3. **MINIMUM POLICY REQUIREMENT**: Access to the patient's specially-protected health data is only permitted by recipients authorized in the patient consent form.

    a. Specific Application (matching DIRECT email address to recipient authorized in the consent form): The sender of the patient health data should verify that the DIRECT email address they are sending such data to belongs to the treating provider named in the consent form. This premise is already part of the national DIRECT policies, but it is particularly important in the context of behavioral health data.

        i. Organization-level vs. Individual-level DIRECT address. Care must be taken by the sender to correctly select the DIRECT email address to direct the message to. Consideration should be given to whether an entity-level DIRECT email address or an individual-level DIRECT email address matches the recipient named on the patient consent form.

        ii. Scope of Consent and Persons Authorized to Open DIRECT Email. The recipient DIRECT end user who opens the DIRECT message containing patient data being disclosed pursuant to a patient's consent must be a person authorized in the written patient consent form. As mentioned in Section 2.c above, the consent form may or may not be worded to permit access by persons on the medical staff or third party agents, QSOs or HIPAA business associates of the recipient provider.

        iii. Reply-to DIRECT address. If the sender of a patient's behavioral health data is replying to a DIRECT email message sent by the requesting provider, and the requesting provider is named in the patient consent form, then the sender can simply "reply-to" the requestor, unless otherwise directed in the message from the requestor.

    b. Optional (inclusion of DIRECT address on consent form): One could include the recipient provider's DIRECT secure email address on the patient consent form (similar to many forms that include fax number today). This may help reduce the chance of the message being directed to the wrong recipient DIRECT email address.

4. **MINIMUM POLICY REQUIREMENT**: Senders of a patient's specially-protected health data pursuant to a patient consent form must ensure that the other aspects of the disclosure comply with the specifications of the consent form, namely:

    a. Specific Application (limitations on data disclosed): The sender (discloser) of the patient data must only send the data that matches how much and what type of data is to be disclosed specified in the patient consent. Exceeding the amount or type of data specified in the consent form would likely be a violation of applicable law which could subject the sender to civil or criminal consequences.

    b. Specific Application (consent expiration): The sender (discloser) of the patient data must ensure that the patient consent has not expired prior to disclosing

the patient's data. The consent form terms will indicate expiration date, event or condition.

c. Specific Application (consent revoked): The sender (discloser) of the patient data must ensure that the patient consent has not been revoked prior to disclosing the patient's data. Revocation could occur in a number of ways, depending on what the consent form terms are for revocation and/or the notice to the patient about methods of revocation.

d. Specific Application (purpose): The recipient of the patient data pursuant to a consent form must ensure that the patient data received from the sender is only used for the purposes specified in the written consent form. For this project, the purpose of the disclosure is for treating the patient.[23]

e. Specific Application (subject line): The subject line in a DIRECT message is unencrypted, and therefore the subject line should not directly or indirectly identify the patient as a drug or alcohol abuse patient. The patient can be named in the subject line, as long as he/she is not identified as a drug or alcohol abuse patient.

5. **MINIMUM POLICY REQUIREMENT**: Recipients of a patient's specially-protected health data must be put on notice of the prohibition against re-disclosure required by 42 CFR Part 2 and some state laws.

a. Background: Part 2 requires each disclosure made with written patient consent to be accompanied by a written statement that the information disclosed is protected by federal law and that the recipient cannot make any further disclosure of it unless permitted by the regulations. Thus, when information is disclosed electronically, an accompanying notice explaining the prohibition on redisclosure must also be electronically sent. Under 42 CFR § 2.32, the statement must read:

> "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 abuse patient."[24]

b. Specific Application (electronic implementation of notice): This notice of prohibition against redisclosure (the "notice") could be implemented in a number of ways with the DIRECT protocol. For example, the Part 2 program sender could choose to:

[23] 42 CFR Part 2 allows patient data to be disclosed without consent in certain other circumstances not applicable here.

[24] See Question and Answer #12 of the SAMHSA FAQs, June 2010.

i. Separate Attached Document Containing the Notice: Include the notice in a separate document (e.g., Word, PDF, or text format) as an attachment to the DIRECT message it is sending.

ii. Notice within the Attached Patient Data Document: Include the notice within the document that contains the patient data that the sender attaches to the DIRECT message.

1. Attached File Type (non-discrete data[25]): The notice could be placed inside the document that contains the non-discrete patient data. Examples include a Word document, a PDF or other image document, or a text document.

2. Attached File Type (discrete data[26]): As the use of DIRECT moves more toward EHR-based message initiation and receipt, fields in a file containing discrete patient data could be utilized for providing the notice (e.g., in an HL7 segment).

3. Note on HISP-Imposed Constraints: DIRECT does not limit the type of file that can be attached to a DIRECT email message. Some HISP vendors may limit the size or type of files that can be attached, depending on the contract with such HISP vendor.

iii. Notice in the Body of Email Itself: The sender could include the notice in the DIRECT message email itself, either in the body of the email or as a notice after the sender's signature.

iv. Other: The sender could utilize other means to include the notice with the patient data, as long as it met the statute's "accompanying" requirement.

6. **MINIMUM POLICY REQUIREMENT**: Any state law requirements for items or notices to be included with the patient data being disclosed must also be met. For our participating states, any message sent by a New Mexico provider that includes a patient's mental health treatment records must be accompanied by any patient-supplied clarifying or correcting statements and other documentation of reasonable length (if any is supplied by the patient). Methods of "accompaniment" would be the same as in the prior section, unless otherwise specified by the particular state law or regulation.

7. **MINIMUM POLICY REQUIREMENT**: The recipient of the specially-protected patient data is forbidden from redisclosing such data to any third party, unless further disclosure is expressly permitted by the written consent of the patient (or as otherwise permitted by 42 CFR Part 2[27]).

---

[25] Discrete data is data that is provided in separate, structured elements that can be used for computation, or are coded to enable automatic manipulation and/or computation, etc. Non-discrete data would be the opposite; an example would be text in an unstructured format or a simple image.

[26] Id.

[27] 42 CFR Part 2 allows patient data to be redisclosed without consent in certain other circumstances not applicable here.

a. Specific Application (agreement not to redisclose): Any recipient must agree to abide by this requirement.[28]

b. Specific Application (technical capability regarding segregation from redisclosure): Any recipient of patient health data that falls under this prohibition against redisclosure must ensure that his/her/its procedures and/or system can segregate and/or flag such non-redisclosable patient data such that the notice of prohibition of redisclosure stays with and/or applies to all the data elements of such non-redisclosable data.

   i. Scope of prohibition on redisclosure. Part 2 prohibits revealing any information that would identify the person, either directly or indirectly, as having a current or past drug or alcohol problem or as being a patient in a Part 2 program.[29]

c. Specific Application (technical capability regarding accompanying information): For New Mexico, and perhaps other states, if any mental health treatment records from New Mexico contain patient-submitted clarifying or correcting statements and other documentation, then the recipient must keep such patient-supplied information with such patient data.[30]

5. SAMPLE PATIENT CONSENT FORM ANALYSIS[31]

6. SAMPLE QSOA LANGUAGE

The following is sample language that can be used as an additional section in a participation/subscription agreement between the DIRECT subscriber (called "Participant" in the excerpt below) and a HISP or HIO (called "Vendor" in the excerpt below) who is performing DIRECT messaging services on behalf of the DIRECT subscriber.

Excerpt of Language for QSO:

1. **Qualified Service Organization Provisions**. This Section ___ shall only apply in the event that a Participant is or has a program subject to 42 CFR Part 2 or transmits Health Data[32] from or other data about clients in a program subject to 42 CFR Part 2.

   a. **Vendor's Role.** Vendor is a Qualified Service Organization or QSO of Participant for the purpose of providing the services specified in this Agreement for Participant, which include but are not limited to[33] data processing, holding and

[28] Id.

[29] See 42 CFR §2.11 & §2.13, and SAMHSA FAQ #16.

[30] Note: Some state laws may not impose a prohibition against further redisclosures on recipient providers located outside of its state's borders.

[31] The sample consent forms are not included in the final version of the report. Therefore the analysis of the consent forms has been redacted.

[32] Health Data was defined elsewhere in the Agreement, but generally refers to health information about an identified client/patient of the Participant.

[33] The activities listed here would vary depending on what services the Vendor would be providing for the DIRECT subscriber.

storing information about Part 2 program clients, receiving and reviewing requests for disclosures to third parties for Permitted Purposes[34] under this Agreement, and/or facilitating the electronic exchange of Part 2 clients' information through the Network,[35] as applicable for the particular service to which Participant is subscribed.

b. **Limits on Use and Disclosure**.

i. The QSO shall only access Health Data or other data about clients of Participant's Part 2 program to the extent needed by the QSO to provide services to the Part 2 program described in this Agreement.

ii. The QSO agrees not to use or further disclose any Health Data or other Part 2 program client information other than as specified in this Agreement.

iii. The QSO acknowledges that in receiving, storing, processing, or otherwise using any information from the Part 2 program about the clients in the program, it is fully bound by the provisions of the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2.

iv. The QSO undertakes to resist in judicial proceedings any effort to obtain access to information pertaining to Part 2 program clients otherwise than as expressly provided for in 42 CFR Part 2, and the QSO shall notify the appropriate Participant.

[34] Permitted Purposes would be defined elsewhere in the Agreement. Example Permitted Purposes could include Treatment, Payment and/or Healthcare Operations (as defined in HIPAA), public health reporting, etc.

[35] Network would be defined elsewhere in the Agreement and would refer to the system that is provided by the Vendor and used by the Participant.

ATTACHMENT 4.1: BASIC CONSENT FORM

[Note: This project involved a sample consent form which will not be included in the final version of this report.]

ATTACHMENT 4.2: MULTISTATE CONSENT FORM

[Note: This project involved a sample consent form which will not be included in the final version of this report.]

ATTACHMENT 5
SUMMARY OF STATE PLANS TO REVIEW POLICIES AND PROCEDURES

State	Description of Method for Obtaining Legal Review	Description of Method for Obtaining Feasibility Review (Clinical and Technical)	Anticipated Time Frame Needed to Complete Review Process
Alabama	• Review will be done by the Alabama One Health Record Legal Team that consists of Legal advisors and attorneys that represent our stake holders. • Review is also done by the Alabama Medicaid Agency's Office of General Counsel in collaboration with our contracted Legal Counsel for the Alabama One Health Record. • Review will also be done by Clay Gaddis, Medicaid HIPAA Privacy and Security Officer.	• Our Business Policy and Workflow subgroup reviews and identifies P&P issues for both HIPAA and 42 CFR Part 2 regarding daily practice management. • Will review with our State HIE vendor and One Health Record HISP provider, Thomson-Reuters.	4-5 weeks
Florida	• Review will be done by the Florida Dept of Health (DOH) General Counsel, who is also the DOH Privacy Officer. • Review will also done by Carolyn Dudley, Assistant Staff Director for Civil Rights, Department of Children and Families (DCF), Office of Civil Rights. • Review will also be done by John Collins, the HIPAA Privacy & Security Officer for AHCA, Office of the Inspector General, HIPAA Compliance Office. • Will also send P&P to Florida's Legal Work Group (LWG) to review. • Do not plan to request an AG opinion.	• Florida Council for Community Health will review. • Will review with State HIE vendor, Harris Corp.	3-4 weeks
Kentucky	• Review will be done with Office of the Inspector General (OIG), Cabinet for Health and Family Services. Our preliminary discussions with state officials have identified OIG as the entity with responsibility for this type of determination. Should OIG identify issues that require further review (at the Attorney General level), appropriate steps will be taken to assure compliance with all applicable statutes and regulations.	• Will work through the Kentucky Association of Regional Programs, the state comprehensive care group. • May also review with the state National Alliance on Mental Illness (NAMI) chapter. • Will work with both our State HIE and HealthBridge (large RHIO in Cincinnati area) for RHIO input.	3-4 weeks

State	Description of Method for Obtaining Legal Review	Description of Method for Obtaining Feasibility Review (Clinical and Technical)	Anticipated Time Frame Needed to Complete Review Process
Michigan	• Review will be completed by Michigan's Legal Work Group and stakeholders. • Will send to the MDCH Privacy and Security Officers for review • Will send to MIHIN Executive Director for review • Planning on sending to the Michigan chapter of the National Alliance on Mental Illness for review and comment • May present to Michigan's HIT Commission for review	• Will work with the MiHIN- the coordinating body for all of Michigan's HIEs. • Will work with vendor(s) in Michigan – Axolotl and possibly Covisint.	4-5 weeks
New Mexico	• Use best efforts to secure review by New Mexico Attorney General's office or by counsel to New Mexico Department of Health	• Will work with the State HIE Vendor (LCF Research) and the New Mexico Health Information Collaborative • Review by the State Health IT Coordinator • Review by the State of New Mexico Interagency Behavioral Health Purchasing Collaborative • Review by other NM project defined stakeholders	3-4 weeks

ATTACHMENT 6
CHECKLIST FOR MAKING REQUEST

[NOTE: THIS CHECKLIST HAS BEEN SLIGHTLY MODIFIED FROM THE CHECKLIST USED IN THE PILOT]

State Health Policy Consortium, Behavioral Health Data Exchange Consortium, Pilot Component

If I make a request for disclosure of data that falls under the definition of health information which is specially protected under Federal regulation CFR 42, part 2 or additional State/local laws related to the exchange of behavioral health data and I intend to receive the information from the disclosing provide by using Direct secure messaging (DSM) capabilities, I agree that I understand the procedures outlined below.[36]

I also understand that the provider that is receiving the request and will disclose the data has been provided a similar checklist outlining his/her responsibility about appropriate transmission and disclosure of the data.

Provider/Entity:	Date:	Phone:	Direct e-mail:

Identity Confirmation (if patient is presenting to you for the first time)

☐ *	Establish the patient relationship/confirm the patient's identity.
☐ *	Confirm with patient the location(s) of relevant patient records and identities of treating providers (Responding/Disclosing Provider).

Consent Confirmation

☐ *	If the patient has presented to you, obtain written consent from patient to contact each specific Responding/Disclosing Provider for the purpose of requesting treatment records.

Contacting Provider(s) and submitting request

☐	Consider contacting (telephone/fax/) Responding/Disclosing provider to establish existence of access to DSM and accurate Direct address. This should be done before disclosing the identity of the patient.
☐	Consider scope of information request for your purposes and limit scope to the extent reasonable.
☐ *	If the patient has presented to you, obtain written consent from patient authorizing disclosure of patient information to you. (Responding/Disclosing provider may accept your form of consent or may require that you have the patient sign a consent provided by Responding/ Disclosing provider). If patient is not present, confirm that the Responding/Disclosing provider has obtained the consent necessary for the disclosure.
☐ *	Submit electronic copy of patient's signed written consent to Responding/Disclosing provider utilizing Responding/Disclosing provider's DSM e-mail address.
☐	If no response within 24 hours, follow up contact may be appropriate

After Receipt

☐ *	Upon receipt of information from Responding/Disclosing provider, review and determine appropriate levels of privacy protection required for information, i.e., is the information subject to prohibitions on redisclosure?

[36] This attachment, *Checklist for Making Request*, does not satisfy the requirement to obtain a valid authorization pursuant to the HIPAA Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule, including uses and disclosures of psychotherapy notes.

☐	Consider acknowledging an understanding of the redisclosure statement
☐ *	Implement appropriate level of privacy protection for information received, including but not limited to electronically sequestering the information received to make sure it is not redisclosed. (If EHR system functionality allows record to be segmented or flagged as sensitive data, add to the system. If not, keep the information separate from the system to prevent unauthorized access or redisclosure).

* These steps are required in order to comply with the regulations for sending/receiving behavioral health data, or with the exchange of information using Direct secure messaging. The steps not marked with an asterisk are encouraged to promote trust between exchanging providers, but are not required for compliance.

ATTACHMENT 7
CHECKLIST FOR RESPONDING TO A REQUEST

[NOTE: THIS CHECKLIST HAS BEEN SLIGHTLY MODIFIED FROM THE CHECKLIST USED IN THE PILOT]

State Health Policy Consortium, Behavioral Health Data Exchange Consortium, Pilot Component

If I receive a request to disclose data that falls under the definition of health information which is specially protected under Federal regulation 42CFR Part 2 or additional State/local laws related to the exchange of behavioral health data and I intend to respond to the request using Direct secure messaging (DSM) capabilities, I agree that I understand the procedures outlined below.[37]

I also understand that the provider that sent the request and will receive the data has been provided a similar checklist outlining his/her responsibility about storing and disclosure of the data.

Provider/Entity:	Date:	Phone:	Direct e-mail:

Identity Confirmation

☐	When the request for disclosure is received from an unknown provider, call to confirm the identity and to verify their DSM e-mail address. If possible, do not use the phone number provided by the participant. This verification is best accomplished by calling the medical records department of the organization using the organization's phone number. Look up the phone number through an independent source such as a state licensure database, or locate the participant's organization online if it is a large organization such as a hospital or health plan.
☐ *	When an initial request for disclosure is received from a known provider, call the provider to verify their DSM e-mail address if you have not previously exchanged information using DMS.
☐	If possible, incorporate the DSM e-mail address of the provider (Requesting/Receiving Provider) in your address book upon confirmation.

Consent Confirmation

☐ *	If consent is required for the disclosure and patient is present, ask them to fill out the appropriate consent forms. If patient is with the Requesting/Receiving provider, submit a copy of your consent form for the patient to fill out and return (this can be done via DSM or using the typical procedures followed for establishing appropriate consent Alternatively, a standard consent form can be used if both parties agree.

Establish Data to be sent

☐	Once identity is confirmed, discuss (either via phone or DSM) what documents will be exchanged, the preferred format for the documents, which other individuals in the organization should receive the information via DSM and their DSM e-mail addresses, expectations for response times, and other preferences as mutually agreed upon

Sending Data via DSM

☐ *	In the text of the DSM, include your practice's legally required statement of prohibition on re-disclosure which complies with 42 CFR Part 2.
☐	Consider enabling delivery-receipt to confirm that data has been successfully transmitted.

* These steps are required in order to comply with the regulations for sending/receiving behavioral health data, or with the exchange of information using Direct secure messaging. The steps not

[37] This attachment, *Checklist for Responding to a Request*, does not satisfy the requirement to obtain a valid authorization pursuant to the HIPAA Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule, including uses and disclosures of psychotherapy notes.

marked with an asterisk are encouraged to promote trust between exchanging providers, but are not required for compliance.

ATTACHMENT 8
BEHAVIORAL HEALTH DATA EXCHANGE PILOT PROJECT
PROVIDER NOTEBOOK

LCF RESEARCH

Reviewer's Package for Behavioral Health Information, Forms and Direct Secure Messaging User Guide

Behavioral Health Data Exchange
Pilot Component Package for Review

Table of Contents

* These forms are used for DSM for all patients, not just behavioral health patients.

LCF RESEARCH

Introduction and Instructions for Transmission of Protected Health Information via DSM

Introduction

LCF Research is engaged in an exciting project to help set national policy and improve patient care, particularly for behavioral health patients. We are part of a six-state consortium funded by Health and Human Services, Office of National Coordinator, to conduct a test pilot of Direct Secure Messaging (DSM) through New Mexico's Health Information Exchange (HIE). DSM is designed to deliver encrypted emails securely from one provider to another.

We'd like you to be part of this exciting project to help set National standards in the transmission of behavioral health protected health information (PHI). Your perspective on the development and testing of this process is vital to its success.

Many local and state HIEs have chosen not to include the electronic exchange of behavioral health patient data due to the sensitive nature of the data, the additional complexities and ambiguities of federal and state laws, and the penalties associated with failure to comply with those laws. Patients with behavioral health issues are particularly vulnerable to harm from data breaches because of the stigma associated with such conditions, yet they may not receive appropriate care if their physicians are not aware of ongoing behavioral health issues. It is the hope of this project that DSM will provide a solution acceptable to providers and patients that allows patient level information to be electronically transferred safely from one provider to another.

A behavioral health provider and a primary care provider will be asked to assist with the pilot project. Each provider will receive an educational 'notebook' about how DSM works and what is required to participate. 'Test data' will be substituted for actual patient data.

The two providers will be asked to assess and critique the DSM documents in the 'notebook.' They will then be asked for their assessment of the lessons learned from the pilot, including their understanding of DSM, the DSM certification process, provider use of the consent/authorization form for the DSM process, and whether an actual transmission of 'test data' was successful.

The educational notebook includes information on the following topics:

- DSM Fact Sheet – The DSM Fact Sheet provides a brief overview of DSM and questions other providers have had about using DSM.
- DSM Privacy Fact Sheet – The DSM Privacy Fact Sheet offers a tangible summary as to why 42 CFR part 2 regulations are important and how to monitor whether your organization is compliant with this regulation.

LCF RESEARCH

- The Issues with Redisclosure of a Patient's Behavioral Health Information – Redisclosure of information that addresses identity, diagnosis, prognosis, or treatment of patients who are being treated for behavioral health issues are subject to confidentiality regulations. These regulations generally prohibit redisclosure of a patient's health information. This form walks the provider through what is and is not acceptable for redisclosure.
- Protected Health Information Request Form – The Protected Health Information Request Form assists a provider in organizing the required tasks for the exchange of a behavioral health patient's information through DSM.
- Patient Authorization Form – The Patient Authorization Form is used by all patients whose information is either accessed through the Health Information Exchange (HIE) or sent through the DSM, regardless of whether they are a behavioral health or medical patient.
- Checklist for Making a DSM Request from Another Provider – The Making a Request Checklist was developed to assist providers in the process of requesting a patient's PHI through DSM from a provider outside of their organization.
- Checklist for Responding to a DSM Request from Another Provider – Responding to a request from a provider outside of the provider's organization can be an onerous task. The checklist was developed to assist a provider in completing the request.
- NMHIC DSM User Guide – The DSM User Guide provides a step by step process on how to connect to DSM.
- NMHIC DSM User Setup – The DSM User Setup is a form that providers complete and submit to NMHIC in order to initiate the DSM process through NMHIC.
- Contact Information for DSM – Should a provider have any questions about DSM the contact information gives the provider a resource to contact.

New Mexico's Health Information Exchange – How the DSM pilot will occur.

New Mexico Health Information Collaborative (NMHIC) is the name of New Mexico's health information exchange network. Its goal is to improve healthcare quality and efficiency through the creation of a statewide HIE network that is trusted and valued by all stakeholders (employees/patients, employers, physicians, health systems and health plans). One of NMHIC's options is a DSM capability for providers to transmit secure emails from one provider/organization to another. NMHIC will work with providers to help them sign on to and follow through with the DSM process.

Providers participating in the DSM pilot will sign a Subscription Agreement (to authenticate the provider and authorize users) with NMHIC for DSM services. NMHIC will establish the DSM service connection, create an account, create a test message, enable the exchange of information, and monitor and verify the successful transfer of information. Providers will be able to access their DSM account to transfer information to another DSM provider after the completion of the DSM project.

Introduction and Instructions for Transmission of Protected Health Information via DSM (continued)

Final Steps in the DSM Project

Providers participating in the DSM pilot will sign a Subscription Agreement with NMHIC for DSM services. The subscription agreement authenticates the provider and approves the user's access to DSM. NMHIC will create the DSM user account for each provider. For the DSM behavioral health pilot, the provider will create a test message, attach the Patient Authorization Form and send the message and attachment to the other participating provider. The receiving provider will need to reply that the message was received to verify the successful transmission of information.

LCF's goal is to complete the review of educational materials and the piloting of DSM between the two providers by the end of October, 2012.

The two participating providers will be asked to assess and critique the DSM documents in the "notebook", and identify lessons learned from the pilot, including their understanding of DSM, the DSM certification process, provider use of the consent/authorization form for the DSM process, and whether an actual transmission of "test data" was successful.

LCF Research will complete the Behavioral Health DSM pilot project with a status report on the notebook's completeness and ease of use and the success of the DSM pilot implementation. The report will be submitted to ONC, the project's two participating providers, the New Mexico Compliance Officer's Forum that represents health care compliance and privacy and security officers from throughout the State of New Mexico, and members of the six-state consortium. The report will include suggested revisions to New Mexico's DSM educational notebook, procedural updates for transmission of behavioral health information via DSM, and the suggested revised patient authorization form.

Direct Secure Messaging Fact Sheet

The following are some frequently asked questions about Direct Secure Messaging. Should you have additional questions, please contact help@nmhic.org.

Q: What is Direct Secure Messaging?

A: Direct Secure Messaging (DSM) is a secure email service offered to health care providers who are authorized to access protected health information (PHI). Through DSM information is securely transmitted from one provider or organization to another provider or organization.

Q: How is DSM different than a fax or an email?

A: DSM replaces less secure communication methods, such as fax machines and regular courier mail. It is an encrypted email that is sent to and received from two known providers/organizations.

Q: Is DSM easy to do and as fast as a fax or regular e-mail?

A: Yes! DSM is simple, fast, inexpensive, and allows you to exchange notes, referrals, continuity of care documents (CCDs), diagnostic images, and summary of care records. DSM can minimize the steps in exchanging information that are often considered time-consuming, expensive and inconvenient. DSM is a secure method of transmitting PHI.

Q: How does DSM address the privacy and security of PHI?

A: Covered entities are required under the HIPAA Regulations to adopt and adhere to policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to PHI. DSM is designed and operated to insure that messages go where they are meant to, are not altered during transmission, and are not seen by anyone for whom they are not intended. This is accomplished in the following manner:

- DSM will be designed and operated in accordance with national standards for the security of DSM messaging.
- DSM will provide identity assurance and authentication of policies for senders and recipients.
- DSM will provide a means of auditing the transmission of messages.
- DSM messages will be encrypted so that it can be read only by those with the proper authorization.

Q: Does DSM just encrypt my email message?

A: DSM encrypts your message and your attachments. It securely routes your message to the intended recipient, eliminating the risk of information being compromised during transmission.

Q: Does DSM help with Stage 1 of Meaningful Use?

A: DSM helps achieve Stage 1 Meaningful Use for the electronic exchange of information when used to transport content exported from an EHR. DSM encourages efficient exchange of patient health information that can lead to better care and less redundancy (e.g., decreasing the number of duplicate tests and exams).

Q: Can I submit a patient's consent to release PHI through DSM?

A: DSM is ideal for exchanging a patient's consent of their health information from one provider/organization to another.

Disclosure & Redisclosure of Behavioral Health PHI: Your responsibilities when receiving or disclosing PHI

Adapted in part from AHIMA "Redisclosure of Patient Health Information (Updated)" *Journal of AHIMA* 80, no.2 (February 2009): 51-54.

Substance Abuse Patient Records

Federal confidentiality laws and regulations (codified as 42 U.S.C. § 290dd-2 and 42 C.F.R. Part 2) recognizes that the stigma associated with substance abuse and fear of prosecution deters people from obtaining treatment.

The Confidentiality of Alcohol and Drug Abuse Patient Records regulations at 42 C.F.R. Part 2 apply to records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with the performance of drug abuse prevention functions conducted, regulated, or directly or indirectly assisted by any department or agency of the US government. **The rules generally prohibit the disclosure and redisclosure of health information without patient consent.** In fact, the rules require that a notice accompany each disclosure made with a patient's written consent. The notice must state:

> *The 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 abuse patient.*

The federal regulations do not prohibit disclosure or redisclosure:

- To medical personnel to the extent necessary to address a genuine medical emergency.
- If authorized by an appropriate court order of competent jurisdiction granted after an application showing good cause. However, the court is expected to impose appropriate safeguards against unauthorized disclosure.

Redisclosure Q&A

Q: Can we redisclose behavioral health records received from another healthcare provider to a new healthcare provider treating the patient?

A: Redisclosure is generally prohibited. The Confidentiality of Alcohol and Drug Abuse Patient Records rules (42 CFR, part 2), which apply to records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with the performance of drug abuse prevention functions conducted, regulated, or directly or indirectly assisted by any department or agency of the US government, generally prohibit redisclosure of health information. There may be certain exceptions which allow for redisclosure, such as state preemption issues for behavioral health, alcohol/drug abuse, or other restricted health information, which must be taken into consideration.
Reference: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

LCF RESEARCH

7

Q: A patient has authorized disclosure of all of his health records related to treatment in our alcoholic rehabilitation center. We received records from the patient's previous encounters that are now included with our record. Can we redisclose this information as part of our records?

A: No. The patient should be referred back to the healthcare provider that originated the health records. *This means that the information must be able to be segmented and/or redacted from the health record whenever a disclosure is made.* Before incorporating this information into your record (paper or electronic) you must ensure it can be marked as inappropriate for redisclosure.

For additional information see: http://www.samhsa.gov

Protected Health Information (PHI) Request Form

Purpose. This request form can be used in connection with *Patient Authorization and Consent Form for Disclosure of Health Information for Treatment* to enable the exchange of consent and the disclosure of health information between trusted parties for treatment. The form can be designed and completed on the requesting provider's EHR or some other computer system, such as Word. The form can be attached, by the requesting provider, to the DSM.

Instructions. For a provider to request disclosure of heath information from the clinic, the clinic staff or the treating provider should:

1. Provide education to the patient about the need for the Release of Information for treatment purposes.
2. Request that the patient complete the *Patient Authorization and Consent Form for Disclosure of Health Information for Treatment.*
3. Complete the Health Information Request Form below.
4. Use the Direct Secure Messaging Request Form to transmit the Health Information, along with the *Patient Authorization and Consent Form for Disclosure,* by attaching the documents and sending them to the disclosing provider via DSM.

Requesting Provider Information

Person/Org. Name: _____
Phone: _____
Fax: _____
Address: _____
Email Address: _____

Patient Information

Name (First Middle Last) _____
Gender: ___ Male ___ Female
Date of Birth: _____
Address: _____
City / State: _____
Zip: _____

Patient Information Requested

Continuity of Care Document (CCD), consisting of the following kinds of information:

☐ Problems	☐ Vital Signs	☐ Alerts	☐ Immunizations
☐ Procedures	☐ Results	☐ Payers	☐ Medical Equipment
☐ Social History	☐ Medications	☐ Functional Stats	☐ Advanced Directives
☐ Family History	☐ Plan of Care	☐ Encounters	☐ eBHIN Shared Record
			☐ Referral Document

☐ Other: _____

LCF RESEARCH

[Note: This page contained a sample project consent form and has been intentionally removed.]

[Note: This page contained a sample checklist for making a request to transmit behavioral health PHI using Direct. However, since the form was slightly changed during the editing process, it has been removed from the final report to avoid confusion. Instead, see the checklist included in Sections 6 & 7.]

New Mexico
Health Information Collaborative (NMHIC)
Direct Secure Messaging (DSM)

User Guide

DRAFT

May 2012

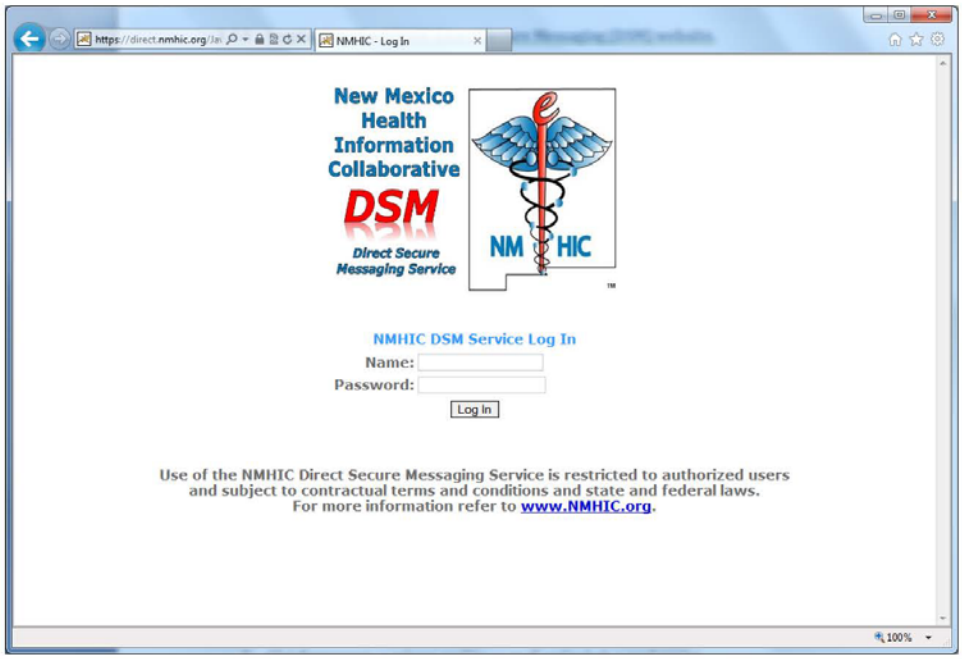
14

1. Accessing the NMHIC Direct Secure Messaging (DSM) website:

1.1. In order to access the NMHIC DSM Web Portal, go to the following URL:

https://direct.nmhic.org

1.2. Or, from the NMHIC.org home page, click on the "DSM Login" button.



NMHIC DSM Log-in page

2. Logging into the NMHIC DSM website:

2.1. Enter the Name and Password supplied by your DSM administrator and click **Log In.**

2.2. When you log in for the first time, you will see a message indicating that your "Password has Expired" and that you will need to change your password.

2.3. The Password requirements are:

2.3.1. Minimum password length is 8 characters, and must contain:

2.3.1.1. English uppercase characters (A through Z)

2.3.1.2. English lowercase characters (a through z)

2.3.1.3. Numerals (0 through 9)

2.3.1.4. Non-alphabetic characters (such as !, $, #, %)

2.4. Once you successfully change your password you will need to click on "**Go back to the login page**" and log in with your new password.

2.5. After you log in, you will be brought to the "**Inbox**" page.

2.6. If you have received a secure message, you would see it listed here.

2.7. To open a message in your Inbox, click on the "**Subject**" of the message.

2.8. If your message includes an attachment, you can download the attachment to your computer or appropriate network location.

NMHIC DSM Inbox page

3. Composing and Sending a secure message:

3.1. To send a "Direct Secure Message" to another Provider, click on the "**Compose**" function, which will bring you to the Compose message page.

3.2. Next, click on the "**Addresses**" button to look up the Provider to send the message to. Note that currently, a Provider can ONLY send a Direct Secure Message to another Provider that has already been set up in the NMHIC DSM system.

3.3. Next, type the subject and the message, and then you can attach any clinical document, (e.g. a referral letter, a clinical note, a Continuity of Care Document, etc.)

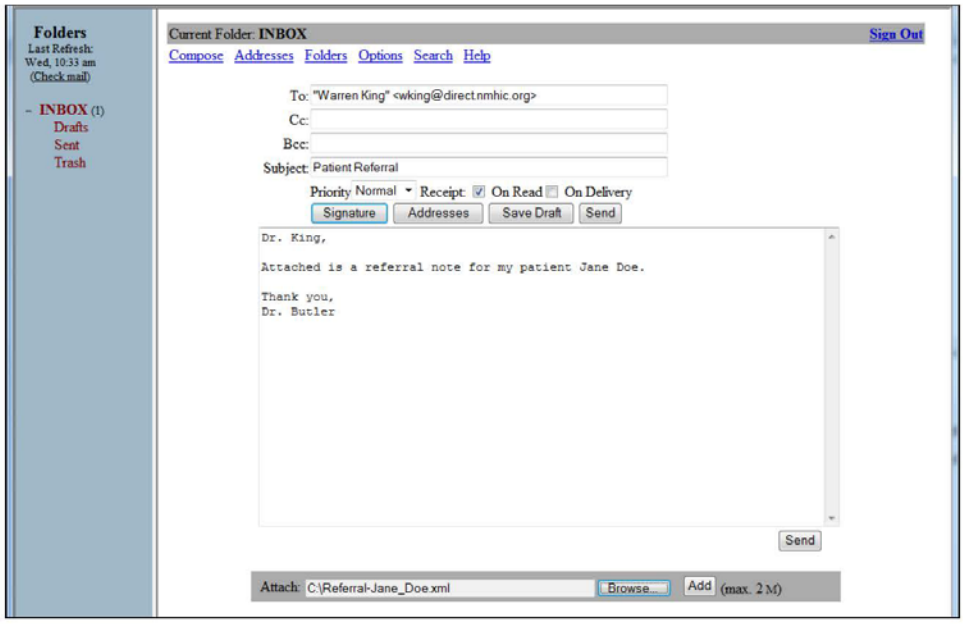
3.4. You can indicate the "**Priority**" of the message, and you can 'check' if you want a "**Receipt**" of the message. Note that "On Read Receipt" is checked by default.

3.5. You can add your "**Signature**" to the message. (See "Options" section below for setting up your Signature.)

3.6. Lastly, click the "**Send**" button to send the message.

Note that the current version of NMHIC DSM does not automatically notify the recipient that they have received a message. You must notify them by other means (e.g. phone or external email).

3.7. You can also click on the "**Save Draft**" button which will save the message in the "Drafts" folder, so you can finish the message and send later.



4. Addresses:

4.1. To view the list of NMHIC DSM users, click on the "**Addresses**" function, which will bring you to the Global Address page.

4.2. You can add NMHIC DSM users to your Personal Address Book.

5. Folders:

5.1. To manage your mail Folders, click on the "**Folders**" function, which will bring you to the Folders page.

5.2. You can create subfolders in order to store messages in different folders.

6. Options:

6.1. To manage your mail Options, click on the "**Options**" function, which will bring you to the Options page.

6.2. You can manage your Personal Information, including setting up a Signature.

6.3. You can change your NMHIC DSM password.

7. Help:

7.1. At anytime you can click on the "**Help**" function, which will provide you with instructions regarding the current NMHIC DSM function you are viewing.

7.2. For additional Help, please contact the NMHIC HIE Help Desk at **Help@NMHIC.org** or **(505) 938-9999**

8. Information about NMHIC DSM:

8.1. Users are prompted to change their password every 90 days.

8.2. Follow the steps in section 2 above for resetting an expired password.

NMHIC Direct Secure Messaging (DSM) Pilot

This form is for setting up a new user in the NMHIC Direct Secure Messaging Pilot Program.

Setting up a new NMHIC DSM user:

1. Complete the following user information:

   First Name: _____ Last Name: _____ Suffix: _____

   Address: _____

   City: _____ State: _____ Zip: _____

   Email Address: _____

   Phone Number: _____

   Name of Practice or Organization: _____

   Signature: _____

2. Submit the User Set-up Form and the completed DSM Agreement to the NMHIC Help Desk at **Help@NMHIC.org** or Fax to **(505) 938-9940**.

   Submitted by:

   Name: _____ Date: _____

   The user's credentials (user name and temporary password) will be communicated to the participating provider.

For internal NMHIC use:

Received by: _____ Date: _____

Set up by: _____ Date: _____

Credentials communicated to: _____ Date: _____

Contact Information

For DSM information contact Help@NMHIC.org or (505) 938-9999

LCF Research
2309 Renard Place SE, Suite 103
Albuquerque, NM 87106-4264
(505) 938-9900
www.LCFresearch.org

DSM Participant Response Form

Thank you for participation in the Behavioral Health DSM Pilot project. In order to improve the DSM Provider Notebook and the DSM process, we would like to know your thoughts, impressions and lessons learned during the process of critiquing the documents and actually transmitting "test patient" information. Your feedback will help us make the DSM process practical and efficient for providers exchanging behavioral health information.

Name_____

Date _____

Please answer each of the following questions and provide a written statement (if appropriate). Feel free to elaborate in your responses.

From your review and use of the DSM Provider Notebook

1. As a new DSM user, did you find the Introduction and Instructions beneficial?
   YES____ NO_____
   a. If no, can you elaborate what was missing or confusing?

2. Was the DSM Fact Sheet helpful?
   YES____ NO_____
   a. If no, what was not helpful?

   b. Are there other questions we should address in the DSM Fact Sheet?
   YES____ NO_____
   If yes, state those questions.

3. Was the Privacy Fact Sheet helpful?
   YES____ NO_____
   a. If no, tell us what was not helpful.

   b. Are there other questions we should address in the Privacy Fact Sheet?
   YES____ NO_____
   If yes, state those questions.

4. The Re-disclosure of Behavioral Health PHI and Your Responsibility. Did this document increase your knowledge about privacy, re-disclosure and the transmission of behavioral health patient information?

   YES____ NO_____

   a. If no, can you suggest a better way of improving this information?

   b. Did the information assist you in meeting legal and internal policy requirements for practices caring for patients with behavioral health, substance abuse or alcohol concerns?

      YES____ NO_____

      If no, can you state what would be beneficial?

   c. Did this information help reduce your concern of legal ambiguity?

      YES____ NO_____

      If no, can you state what information would enhance your understanding?

5. Was the Protected Health Information Request Form clear and concise?

   YES____ NO_____

   a. If no, please elaborate.

   b. Was it helpful?

      YES____ NO_____

      If no, please elaborate.

   c. Do you have a better understanding of what information is necessary for requesting providers?

      YES____ NO_____

      If no, please elaborate.

   d. Is there other information that should be addressed on this form?

      YES____ NO_____

      If yes, state what other information you feel should be addressed.

6. Was the Checklist for Making a Request clear regarding what you need to do or not do?
   YES____ NO_____
   a. If no, can you make a suggestion on how to improve the information?

7. Was the Checklist for Responding to a Request clear regarding what you need to do or not do?
   YES____ NO_____
   a. If no, can you make a suggestion on how to improve the information?

8. Did both of the checklists fit well with your workflow?
   YES____ NO_____
   a. If no, what areas are problematic?

9. Was the Patient Authorization/Consent Form practical, clear and user friendly for you and, from your perspective, for the patient?
   YES____ NO_____
   a. If no, what about the form is problematic?

10. Was the DSM User Guide easy to use?
    YES____ NO_____
    a. If no, what is confusing about the User Guide?

Your Review of the DSM Implementation Process

1. When you attempted to become an authorized DSM user, was the process easy?
   YES____ NO_____
   a. If no, what issues did you experience?

2. Was it easy to send text and documents using DSM?
   YES____ NO_____
   a. If no, what made it difficult?

3. Was it easy to verify receipt that the document(s) were sent?
   YES____ NO_____
   a. If no, please explain.

4. Was it easy to receive and use the text and documents sent to you using DSM?
   YES____ NO_____
   a. If no, please explain.

General Ease of Use and Understanding of the DSM Process

1. NMHIC is interested in how we can improve a provider's understanding and use of the DSM implementation process. Besides the comments you have already made, do you have any additional comments that would help us better understand a provider's need in their use of the Provider Notebook and DSM?

Behavioral Health and Patient Privacy

1. With respect to behavioral health and primary care providers, do you have any additional comments regarding their use of DSM and patient privacy?