Robert Wood Johnson Foundation

JANUARY 2014

Integrating Physical and Behavioral Health

Strategies for Overcoming Legal Barriers to Health Information Exchange

Prepared by Manatt, Phelps & Phillips—Robert Belfort, William Bernstein, and Susan Ingargiola

Executive Summary

This brief explores the strategies states use to address barriers that impede data-sharing efforts among providers to integrate physical and behavioral health care. The first step for states interested in more and better data exchange is to understand legal barriers to sharing such data and to directly confront misperceptions about those barriers with providers, health plans, and other stakeholders.

There is no single obstacle to data-sharing between physical and behavioral health care providers. Federal and state health information privacy laws create a complex network of requirements governing the use and disclosure of health information. The Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule restricts the use and disclosure of protected health information. Due in part to broad exceptions covering disclosures by providers for treatment and related care management activities, HIPAA generally is not an impediment to data-sharing among physical and behavioral health care providers for treatment purposes. However, other laws can-and often do-stand as real obstacles to effective information sharing and care coordination between these two important parts of the health care system. For example, the federal alcohol and drug abuse treatment confidentiality rules, commonly referred to as the "Part 2 regulations," create potential legal obstacles to data-sharing that providers and states must carefully navigate. In addition, individual states have, in some cases, created stringent limitations on sharing behavioral health information across providers and between providers and insurers.

Given the range of state and federal laws governing health information privacy, the nature of the real or perceived legal barriers to data-sharing between physical and behavioral health providers will vary from one situation to another and from one state to another. A state's strategy for reducing barriers to data exchange must be tailored to address the particular obstacles present in that state. Common obstacles to data exchange between and among physical and behavioral health providers, and between plans and providers, include misunderstandings about the law, disagreements over ambiguities in the law, concerns about reliance on the privacy and security practices of other providers, and obstacles to obtaining patient consent. To support care integration efforts, states should work with providers and managed care plans to debunk misconceptions about legal privacy rules which impede data-sharing between physical and behavioral health providers.

In addition to the legal framework in a state, the extent to and the mechanisms by which providers engage in electronic information sharing will affect the feasibility and success of strategies for facilitating robust data-sharing. To effectively reduce barriers, state leaders must understand the nature of data exchange initiatives within their state and develop strategies relevant to electronic and non-electronic communication as appropriate to current data exchange methods and practices. States interested in promoting innovative care delivery models that rely on increased information exchange between physical and behavioral health care providers have several tools at

ABOUT MANATT HEALTH SOLUTIONS

Manatt Health Solutions is an interdisciplinary policy and business advisory division of Manatt, Phelps & Phillips, LLP, one of the nation's premier law and consulting firms. MHS helps clients develop and implement strategies to address their greatest challenges, improve performance and position themselves for long-term sustainability and growth. For more information, visit *www.manatt.com/manatthealthsolutions.aspx.*

ABOUT STATE HEALTH AND VALUE STRATEGIES

State Health and Value Strategies, a program funded by the Robert Wood Johnson Foundation, provides technical assistance to support state efforts to enhance the value of health care by improving population health and reforming the delivery of health care services. The program is directed by Heather Howard at the Woodrow Wilson School of Public and International Affairs at Princeton University.

ABOUT THE ROBERT WOOD JOHNSON FOUNDATION

For more than 40 years the Robert Wood Johnson Foundation has worked to improve the health and health care of all Americans. We are striving to build a national culture of health that will enable all Americans to live longer, healthier lives now and for generations to come. For more information, visit *www.rwjf.org*. Follow the Foundation on Twitter at *www.rwjf.org/twitter* or on Facebook at *www.rwjf.org/facebook*.

their disposal to reduce or eliminate these barriers to data-sharing. States can use the following six strategies to overcome barriers:

- clarify state law through agency guidance;
- enact state legislation or regulations to streamline privacy standards governing exchange;
- create standardized consent forms;
- provide information exchange implementation advice;
- enact immunity laws to protect providers engaging in information exchange; and
- promote technological solutions to data segmentation that would allow health care providers to share some data but not others.

Introduction

Medicaid programs across the country are exploring strategies to better integrate the delivery of physical and behavioral health services. A growing number of Medicaid officials believe that coordinating care across these two historically balkanized sectors of the health care system is critical to improving health outcomes and decreasing costs. However, effective care coordination requires robust data exchange among physical and behavioral health providers and many providers are reluctant to freely share data for fear of violating health information privacy laws.

Legal Framework

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is the legal foundation for health information privacy in the United States. The *HIPAA Privacy Rule*[1] restricts the use and disclosure of "protected health information" maintained by "covered entities," which include most physical and behavioral health providers.

Two elements of HIPAA warrant special attention by states and providers interested in integrating care. First, HIPAA permits covered entities to use and disclose protected health information for treatment, payment, and health care operations without the patient's authorization. These terms are defined as follows:

- *Treatment* is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.
- *Payment* encompasses activities of a health plan to collect premiums, determine, or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual; and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
- *Health care operations* include, among other things, quality assessment and improvement activities, including case management and care coordination; competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; business planning, development, management, and administration; and business management and general administrative activities of the entity, including but not limited to de-identifying protected health information.[2,3]

Under HIPAA, a covered entity may use—and disclose—protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information to another health care provider for its treatment activities; to another covered entity or health care provider for that entity's or provider's payment activities; or to another covered entity for quality improvement and limited other health care operations carried out by that entity if both covered entities have or had a relationship with the patient and the protected health information pertains to the relationship.

Significantly, the HIPAA Privacy Rule usually does not distinguish between general medical information and other, potentially more sensitive types of health information, such as behavioral health data. Thus, as a general matter, the flexible rules described above, which permit information sharing without patient authorization for treatment, payment, care coordination, and other related purposes, will apply to any medical information exchanged between physical and behavioral health providers, as well as to insurance plans and managed behavioral health plans.

The one exception to this general rule applies to psychotherapy notes, which may be disclosed only with the written authorization of the patient, except in very limited circumstances.[4] Psychotherapy notes are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude records of medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.[5] Critically, progress notes or other documentation of counseling sessions that are integrated with the above information are not considered psychotherapy notes under HIPAA because they are not kept separate from the rest of the patient's medical record.

Another HIPAA consideration when exchanging information is the Privacy Rule's "minimum necessary" provision. This provision requires a covered entity to make reasonable efforts

to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. Importantly, though, the minimum necessary requirement does not apply to the use or disclosure of protected health information for treatment purposes.[6,7,8]

HIPAA typically should not serve as a legal impediment to robust health information exchange among physical and behavioral health providers. The HIPAA Privacy Rule has broad exceptions covering disclosures by providers for treatment and related care management activities that apply to all medical information other than psychotherapy notes and are not subject to "minimum necessary" restrictions.

Federal Substance Abuse Treatment Regulations

Unlike HIPAA, the federal alcohol and drug abuse treatment confidentiality rules do create potential legal obstacles to data exchange that must be carefully navigated. The rules, commonly referred to as the "*Part 2 regulations*," based on the section of the federal code where they are located, do not contain broad exceptions for treatment, payment, or health care operations. The only exception in the rules that is likely to be applicable to data exchange in connection with provider integration efforts relates to disclosures for emergency medical care.

While the Part 2 regulations are stringent, they are not applicable to general medical providers who deliver a mix of substance abuse and other health care services. The regulations apply only to the records of "federally assisted alcohol and drug abuse programs," or "Part 2 providers." Under the regulations, an alcohol or drug abuse program is defined as "any person or entity that holds itself out as providing, and actually provides, alcohol or drug abuse diagnosis, treatment, or referral for treatment."[9] Generally, the regulations cover those facilities, programs, or units that are specially licensed to provide substance abuse treatment, or market themselves as offering these services. A general medical facility or office is **not** considered a program; only those identified alcohol or drug abuse units located within the facility qualify as programs. Thus, records relating to substance abuse diagnosis or treatment provided in a general hospital emergency room or inpatient department, in a mental health facility, or in a primary care physician's office, are not subject to the Part 2 regulations.

The Part 2 regulations only apply to those alcohol or drug abuse programs that receive federally assistance. Federal assistance, though, is defined broadly to include, among other things, receipt of Medicare or Medicaid payments, acceptance of grants from federal agencies, registration to dispense controlled substances, and tax exempt status. Thus, the vast majority of specialized substance abuse treatment facilities and programs will meet this test.

As indicated above, except in a medical emergency, the records of Part 2 providers may not be disclosed for treatment, care coordination, or quality improvement purposes without the patient's consent. Consent must be in writing and must include the following elements:

- The name of the program.
- The name of the recipient of the records.
- The name of the patient.
- The purpose of the disclosure.
- A description of the information being disclosed.
- The signature of the patient or a minor patient's parent or guardian.
- The date of the signature.
- A statement that the consent is subject to revocation.
- The date or event upon which the consent expires. The consent may remain in effect no longer than is reasonably necessary to achieve its purpose.[10]

The consent requirements are particularly restrictive in several respects. First, the consent form must specify the particular person or entity receiving the records. A general consent authorizing disclosure to all providers treating the patient is insufficient. Second, consent is usually required for the re-disclosure of records received by a general medical provider from a Part 2 provider, even though the general medical provider is not directly subject to the Part 2 regulations. Third, all disclosures of records protected by the Part 2 regulations must be accompanied by a warning notice indicating the specially protected nature of the records.[11]

The Part 2 regulations are not superseded by HIPAA. Therefore, even though HIPAA provides a relatively flexible legal framework for health information exchange among all physical health and mental health providers, data-sharing arrangements involving Part 2 providers will typically require some type of patient consent process.

State Health Information Privacy Laws

As is the case with the Part 2 regulations, state health information privacy laws are not pre-empted by HIPAA if they are more stringent than the HIPAA Privacy Rule.[12] The nature and scope of these laws varies widely from state to state. Some states have adopted comprehensive laws that are similar in scope to HIPAA and apply to the entire health care industry, while other states have enacted narrower laws that protect specific types of sensitive health information or cover particular types of providers. Examples include:

California Confidentiality of Medical Information Act

An example of a comprehensive state privacy law is the *California Confidentiality of Medical Information Act* (CMIA).[13] The CMIA provides that "no provider of health care shall disclose medical information regarding a patient of the provider without first obtaining an authorization."[14] Exceptions include, but are not limited to, disclosures for purposes of diagnosis and treatment of the patient, or to an insurer, employer, health care service plan, governmental authority, or other entity responsible for

determination of payment. A provider that receives medical information pursuant to an authorization may not further disclose that information except in accordance with a new authorization.[15] Like HIPAA, but unlike the Part 2 regulations, and with the exception of psychotherapy notes[16], the CMIA permits physical and behavioral health providers to share patient information for treatment purposes without the patient's authorization.

As with HIPAA, the CMIA provides special protection for psychotherapy notes. Health care providers may not disclose medical information that relates to the patient's participation in outpatient treatment with a psychotherapist unless the person or entity requesting that information submits to the patient and to the provider of health care, health care service plan, or contractor a written request, signed by the person requesting the information, that includes all of the following: the specific information relating to a patient's participation in outpatient treatment with a psychotherapist being requested and its specific intended use or uses; the length of time during which the information will be kept before being destroyed or disposed of; a statement that the information will not be used for any purpose other than its intended use; and a statement that the person or entity requesting the information will destroy or return the information when the specified period has expired.[17]

New York Mental Hygiene Law

New York offers an example of a more narrowly drawn statute. *Section 33.13 of the Mental Hygiene Law* governs the confidentiality of records maintained by facilities licensed or operated by the New York State Office of Mental Health or Office of People With Developmental Disabilities. Significantly, the law does not apply to other medical facilities, such as general hospitals, that may provide mental health treatment or to mental health practitioners practicing outside of licensed mental health facilities.

The statute provides that information maintained by such facilities or programs is confidential and cannot be released to any person without the patient's consent unless an exception applies. One such exception permits sharing of information between "facilities or others providing services for such patients or clients pursuant to an approved local or unified services plan." State officials have interpreted this provision as permitting health information exchange among licensed mental health facilities, but not between such facilities and other health care providers. Another exception allows hospital emergency rooms and mental health programs to share mental health information about a patient. Thus, the New York law falls somewhere between the highly restrictive Part 2 regulations and the more flexible HIPAA and CMIA rules.

Common Obstacles to Data Exchange

Given the patchwork of state and federal laws governing health information privacy, the nature of the real or perceived legal barriers to data exchange between physical and behavioral health providers and insurers will vary from one situation to another. Below are some of the common obstacles to data-sharing that arise in connection with initiatives to integrate physical and behavioral health care.

Misunderstanding the Law

Health care providers are often confused by the complex web of state and federal privacy laws and regulations. In the absence of a single, comprehensive health information privacy legal framework that exclusively governs all data exchange activities, providers are left to figure out how the patchwork of laws applies to their particular activities. Examples of common provider misconceptions about health privacy laws include the following:

Misconception	Actual Legal Rule
HIPAA requires patient authorization for disclosures for treatment purposes.	No patient authorization is required.
HIPAA's minimum necessary provision forces providers to determine which part of the medical record they can share with other providers for treatment purposes.	The minimum necessary rule does not apply to disclosures for treatment purposes.
A provider may not disclose information to another provider for treatment purposes unless the receiving provider has a pre-existing relationship with the patient.	No pre-existing relationship is required to receive information for treatment purposes. (A prior relationship is required to receive information for quality improvement purposes.)
HIPAA's restriction on the disclosure of psychotherapy notes applies to all notes of counseling sessions that are part of the patient's medical record.	A clinician's notes qualify as psychotherapy notes under HIPAA only if they are maintained separately from the patient's medical record.
The Part 2 regulations restrict the disclosure of all substance abuse treatment information.	The Part 2 regulations apply only to specialized substance abuse providers, not general medical providers who deliver substance abuse services.
A consent for the release of a Part 2 provider's records must be a separate document and cannot be combined with any other type of patient consent.	A Part 2 consent can be combined with another patient consent form if the form contains all of the elements required under the Part 2 regulations.

These examples are by no means exhaustive. Provider misconceptions about the restrictions imposed under state and federal laws may stifle data exchange that is legally permissible.

Ambiguities in the Law

In some cases, providers or insurers are concerned about data exchange not because they have misinterpreted a clearly articulated legal provision, but because the law is ambiguous and subject to different interpretations. Ambiguity is a particular problem with respect to state privacy laws. The HIPAA Privacy Rule contains a detailed set of standards governing the use and disclosure of information, which are further clarified by extensive written guidance issued by regulators. In contrast, many state privacy laws contain general language on the need to protect confidentiality, without providing a specific set of restrictions and exceptions. Even when the law includes more detailed standards, the application of those standards to the dynamic world of electronic data exchange is often unclear as state regulators often provide far less interpretive guidance than their federal counterparts. As a result, the insurer's or provider community's understanding of the law may be based on informal guidance from state agencies, local practice customs, or other factors that make it difficult to achieve community-wide consensus on relevant legal requirements. In this environment, multiprovider collaborations tend to devolve to the lowest common denominator, where the most restrictive interpretation of the law becomes the standard for sharing, or not sharing, data.

Concerns About Reliance on Other Providers

Providers and insurers engaged in health information exchange are, to some degree, placing their trust in one another. If one provider engages in inappropriate conduct or employs lax privacy safeguards, other providers and involved insurers could face liability or negative publicity.

For example, if Provider A submits a patient consent form authorizing Provider A to access Provider B's records, Provider B must rely on the fact that Provider A's form meets all applicable legal requirements. Provider B may be concerned about relying on Provider A's compliance because Provider B is the party making the disclosure and will likely be held responsible if the disclosure is legally impermissible. If Provider B is unsure about whether the consent form is valid, Provider B can reject the request and require Provider A to obtain a new consent using Provider B's form. By that time, Provider A may face difficulties obtaining the patient's consent. The lack of standardization fuels uncertainty and mistrust.

A similar dynamic may arise with respect to collaborating providers' security practices. If Provider B grants Provider A access to Provider B's records, Provider B may be concerned that Provider A's data security safeguards are less robust than Provider B's. Provider B may fear that if there is a breach involving Provider A's record system, Provider B will be held responsible because it shared data with Provider A. Because Provider B may not have the capacity or the resources to effectively assess Provider A's security practices, Provider B may make the risk averse decision to not share data.

Finally, providers may be concerned about the accuracy or completeness of other providers' records. While providers have always shared medical records with one another, more extensive electronic data exchange arrangements may facilitate access to the records of many more providers, some of whom the accessing provider does not know well. There may be a lower level of trust among providers in these circumstances, and a heightened concern of malpractice liability if records used for treatment purposes are inaccurate or incomplete.

Obstacles to Obtaining Patient Consent

In certain cases, providers and insurers seeking to integrate physical and behavioral health care may all agree that patient consent is necessary for certain types of data exchange. They may also agree on the type of consent form that must be used for the intended purposes of the collaboration. But some or all of the providers or involved entities may believe that obtaining consent is operationally infeasible or unduly burdensome. They may feel that the consent management process requires new, costly workflows for educating patients about their rights, obtaining signatures on consent forms, and tracking consents both internally and across the multiprovider collaboration. Providers and insurers may also be skeptical about whether patients will take the time to read and sign the consent forms. While providers may be prepared to comply with an "opt out" process where information sharing is permissible unless a patient objects, applicable law does not permit this type of process for some or all of the data being exchanged.

Some of the factors that may contribute to the resistance of physical and behavioral health providers or plans to manage a patient consent process include the following:

- **Obtaining patient consent may be time consuming and costly.** Private practitioners, in particular, may be especially resistant to implementing new workflows to manage patient consent. While hospitals and other institutional providers may already operate a patient registration process administered by dedicated administrative staff, private medical offices often do not have specialized personnel who can easily take on additional patient education responsibilities. Practitioners may view consent management as a new cost center for which there is no offsetting reimbursement.

- **Providers may be reluctant to make intensive efforts to obtain patient consent when there is no immediate clinical benefit to them in doing so.** In a data exchange model in which each provider obtains the consent of its patients to upload information to a Health Information Exchange (HIE), a provider's failure to get consent does not prevent the provider from accessing information that has been made available by other providers. A "moral" obligation to seek patient consent for the collective benefit of all participating providers may not be powerful enough to influence providers' behavior.

- **Lackluster efforts by providers to obtain patient consent may create a cycle of non-participation.** If few records are available in an HIE due to the absence of patient consent, providers will stop checking the HIE and gradually opt out of participating in the data exchange collaboration.

The difficulties in obtaining patient consent may be exacerbated by the lack of technical means to segregate sensitive health information from other information. Given the variety of state and federal laws, potentially burdensome patient consent requirements may apply only to a small portion of the data being exchanged by providers and plans.

Operational burdens associated with consent management could be minimized if providers seek consent only for those disclosures where it is legally required. In order to avoid obtaining consent where it is not legally mandated, however, providers may need to tag or filter the sensitive data that is subject to the consent requirement. In addition, providers may lack the operational and/or technical capacity to tag or filter sensitive data. This potential barrier to data-sharing is less of a problem when all of a provider's data is governed by the same privacy standard. For instance, a Part 2 provider knows that it must obtain consent for the disclosure of all of its records, except in a medical emergency. In contrast, if a state privacy law governs certain types of data rather than certain types of providers, a provider that delivers a variety of services may maintain some information that can be disclosed without patient consent and other information that cannot. For example, a hospital that utilizes a single, integrated record system may be permitted to disclose general medical information, but not mental health information, contained in that system. If the hospital cannot distinguish between the two types of information electronically on an automated basis, it may feel compelled to obtain patient consent for all disclosures, even if the vast majority of disclosures do not require consent.

Strategies for Overcoming Barriers to Information Sharing

As previously indicated, there is no single obstacle to data-sharing between physical and behavioral health care providers or plans. The nature of the barriers will vary from one setting to another, depending on multiple factors such as the scope and stringency of state privacy laws, the legal sophistication and risk tolerance of participating providers, and the role of state government and other stakeholders (such as trade or professional associations) in clarifying applicable law and promoting the adoption of industry-wide best practices. As a result, a state's strategy for reducing barriers to data exchange must be tailored to address the particular obstacles present in that state.

Crafting the most effective strategy for reducing barriers requires a sophisticated understanding of the nature of the data exchange initiatives within the state. Some of the relevant questions states may need to ask include the following:

- **Which providers are included in the data exchange system?** Are Part 2 providers participating? Are other providers subject to stringent state privacy laws involved? If such providers are participating, is their full participation critical to the initiative's success?
- **What type of data is being exchanged?** Is all of the data coded or structured, or does the exchange include free text? Can elements of the data sets be effectively filtered or segregated?
- **Is data being accessed in hospital emergency rooms or in other settings where immediate access to records without advance notice is essential?**
- **Are providers accessing records in situations or settings where obtaining patient consent is feasible?**
- **Have all of the relevant state privacy laws been catalogued and analyzed?**
- **Is there a consensus among and between providers and insurers on the applicable legal requirements?**

Another important question for states to consider relates to the manner in which health care providers are exchanging information. In the years since enactment of the *Health Information Technology for Economic and Clinical Health Act*, the tools available for electronic health information sharing have evolved significantly. While efforts to encourage electronic HIE were once focused on complex, regional, or national data exchange models, they are now increasingly targeted to more nimble, tactical models of exchange facilitated by smaller groups of providers in a community (e.g., a hospital and the physicians in its community, or an accountable care organization). In addition to the legal framework governing health information exchange, the mechanisms by which providers engage in electronic information sharing will affect the effectiveness and feasibility of different strategies for facilitating more robust data exchange.

Below are six strategies states may utilize to address the varied causes of data illiquidity:

- Clarification of state law through agency guidance;
- Enactment of state legislation or regulations to streamline privacy standards governing exchange;
- Creation of standardized consent forms;
- Provision of information exchange implementation advice;
- Enactment of immunity laws to protect providers engaging in information exchange; and
- Promotion of technological solutions to data segmentation allowing health care providers to share some data but not others.

While some of these strategies have been focused on promoting electronic health information exchange, they are generally

applicable to information sharing through other means such as paper, fax, or telephone.

Clarification of State Law Through Agency Guidance

As mentioned previously, providers and insurers may be reluctant to exchange information because they misunderstand applicable privacy law or the law is too ambiguous to interpret with confidence. This type of obstacle to data-sharing represents the "low hanging fruit" that states can address through the issuance of interpretive agency guidance.

A good example of the kind guidance that can effectively clarify the legal landscape is the U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration (SAMHSA)'s *Frequently Asked Questions Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*[18]. While the SAMHSA guidance did not relieve Part 2 providers of the obligation to obtain patient consent for most disclosures, it did interpret the Part 2 regulations in several ways that provided comfort to Part 2 providers interested in participating in electronic data exchange initiatives. Among other things, the guidance stated that:

- **Part 2 providers may upload patient information to a centralized health information exchange for storage without patient consent under a "Qualified Service Organization Agreement," which is similar to a business associate contract under HIPAA.** As a result, Part 2 providers have been able to upload records to an HIE, where the records can be accessed by hospital emergency rooms without patient consent or by other providers with patient consent at the point of care. Absent advance uploading, it might be impossible for other providers to obtain Part 2 records on a timely basis.
- **A single consent form may be used to authorize disclosure of records from a Part 2 provider to multiple providers participating in an HIE or other data-sharing arrangement.** In addition, the same consent form can authorize successive disclosures and re-disclosures. This regulatory flexibility can simplify the consent process.
- **Electronic patient signatures may be used to satisfy the Part 2 regulations' consent requirements.** As a result, an online consent process is feasible.
- **"Treatment" is a sufficient description of the purpose of a disclosure under the Part 2 regulations.** A broad description of the purposes of a disclosure in the consent form can minimize the need for obtaining consent repeatedly as treatment progresses.
- **While a consent form must state a specific expiration date or an event upon which the consent expires, there is no maximum period during which the consent may be valid.** Setting a far off expiration date or event can obviate the need to renew the consent.

While SAMHSA may have offered informal advice to Part 2 providers on some of these issues previously, the issuance of a formal, written guidance document to the public gave far greater comfort to the industry and allowed collaborating clinicians to operate under a universally agreed upon set of principles. State agencies may be in a similar position to correct misconceptions or eliminate ambiguities regarding the meaning of state mental health or other privacy laws, clearing the way for providers to exchange data without fear of regulatory enforcement.

State agencies should take care to craft their guidance in a way that addresses the full range of questions that physical and behavioral providers may have about the application of state law to information exchange. Questions to consider in advance of issuing any guidance may include:

- Which type of information is being shared?
- Which types of providers are sharing this information?
- Under which laws are these providers licensed?
- Is information being shared for medical treatment only or for other purposes such as quality improvement studies?
- Through what technical means are providers exchanging information? Are providers using an outside vendor to facilitate exchange?
- How are providers interfacing with patients?

To anticipate all of the relevant questions, state officials should discuss the real or perceived obstacles to data exchange with providers in advance of issuing any guidance.

State Legislation to Streamline Privacy Standards

While providing interpretive guidance on existing privacy laws and operating data exchange initiatives within the parameters of these newly clarified statutes is often helpful, in some cases, physical and behavioral health providers and plans may feel strongly that existing privacy laws–even if clarified–are simply too restrictive for efficient, cost-effective information sharing. In particular, providers may believe that obtaining patient consent for the day-to-day disclosure of information for treatment purposes is too costly and operationally complex.

A few states have attempted to minimize this burden on providers by enacting legislation that establishes a streamlined patient consent process for data-sharing within a state-recognized HIE framework. The goal of these legislative efforts is to replace the patchwork of state privacy laws with a single, more flexible set of requirements for electronic information sharing.

A primary example of this type of approach is the *North Carolina Health Information Exchange Act*, or NCHIE Act, which authorizes the creation and operation of a voluntary, statewide electronic health information exchange network, or *NC Network*. The NCHIE Act supersedes other state privacy laws with respect to information sharing within the NC Network. In place of the patchwork of state laws that impose various requirements on different types of information and providers,

the NCHIE Act authorizes the exchange of all data within the NC Network in accordance with HIPAA standards. Because HIPAA permits the disclosure of protected health information for treatment, payment, and health care operations without patient authorization, affirmative patient consent is generally not required for data exchange within the NC Network. The NCHIE Act does grant patients the right to opt out of the NC Network (except for exchange of their information in a medical emergency) by completing a form at their provider's office.[19] But providers view the obligation to accept a limited number of opt-out requests as far less burdensome than administering an affirmative consent process for all of their patients.

Nevada has adopted a similar approach. Under the *Nevada Public Health and Safety Code*,[20] if a HIPAA-covered entity complies with HIPAA when electronically transmitting individually identifiable health information, the covered entity is exempt from complying with any state health information privacy law that is more stringent than HIPAA. The Nevada law also requires a covered entity participating in an electronic data exchange arrangement to allow a patient to opt out of having his or her health information disclosed electronically to other covered entities, though this right is not afforded to Medicaid and SCHIP enrollees or when the information sharing is required by either HIPAA or state law. *Ohio* has also adopted a similar approach.[21]

The new North Carolina, Nevada, and Ohio laws cannot legally pre-empt the more stringent Part 2 regulations, which are established at the federal level. Thus, Part 2 providers must continue to comply with the affirmative written consent requirements of the Part 2 regulations. However, most physical and behavioral health providers can exchange information under the far more flexible HIPAA standards. Given the fact that most Part 2 providers have their own record systems that are not integrated with the record systems of other medical providers, limiting an affirmative patient consent requirement to Part 2 providers without having to filter out or segregate substance abuse treatment information from other health information is possible.

Standardized Consent Forms

Even if patient consent is required for some or all of the information sharing between physical and behavioral health providers and plans, there may still be opportunities for states to simplify the consent management process. New York, which has some of the most stringent state privacy laws in the nation, provides a good example of this type of initiative.

New York is in the process of developing the *Statewide Health Information of New York* (SHIN-NY), a statewide electronic network of networks that connects physical and behavioral health providers. The SHIN-NY will enable providers across the state to share patient health information in real time at the point of care for treatment purposes, engage in quality improvement activities, and perform public health reporting. The state created a "*statewide collaboration process,*" or SCP, to develop privacy and security policies governing access to health information through the SHIN-NY. The SCP involves broad participation by a diverse set of health care stakeholders, including representatives of hospitals, physicians, behavioral health providers, health plans, state agencies, consumer groups, and privacy advocates. The SCP is overseen by the New York eHealth Collaborative, a not-for-profit organization charged by the state with directing the development of the SHIN-NY.

The SCP developed a *standard consent form* that covers all information exchanged by physical and behavioral providers, including mental health, substance abuse, and HIV-related records. The form has been approved by state regulatory agencies and has been carefully crafted to comply with the SAMHSA guidance on HIEs discussed above. The use of a standard consent form approved by the state eliminates concerns about whether potentially disparate forms used by the wide array of providers exchanging information through the SHIN-NY are legally valid. The form also allows providers to obtain a one-time consent for the exchange of all physical and behavioral health information, obviating the need for seeking multiple consents covering different types of information. Finally, the standard form can be used as a multiprovider consent. A group of collaborating providers may use a consent form that covers all of the providers in the network, enabling one provider to obtain patient consent for all participants. While the development of the standardized consent form has not eliminated the need to obtain patient consent, it has simplified the process, minimized the burden, and promoted mutual trust.

The standardization of consent forms does not necessarily have to occur in connection with a statewide electronic health information exchange initiative such as the SHIN-NY. The state, either on its own or through a delegation to a multistakeholder, nonprofit organization, can develop similarly streamlined standards for narrower data-sharing arrangements such as health homes, care coordination networks, and pilot programs designed to test new ways of integrating physical and behavioral health.

Implementation Advice

In addition to streamlining patient consent, states may be able to help health care providers and plans simplify their implementation of health information sharing initiatives in other ways, such as developing standardized industry-wide privacy practices that create greater comfort among providers and plans that all participants in a data exchange arrangement are taking their privacy responsibilities to one another seriously. Most states that are operating or creating a statewide health information exchange network have developed standardized practices. The *State HIE Cooperative Agreement Program*, which was authorized by the Health Information Technology for Economic and Clinical Health Act and which provided states or "state-designated entities" with funds to develop and operate statewide HIE networks, required it. State officials interested in this approach should determine whether standardized privacy practices have already been developed in their states for electronic

information sharing. If not, states may model standard privacy practices on those developed in other states.

One example of this approach is the New York SCP's development of *Privacy and Security Policy and Procedures*, or SCP Policies, which set forth minimum standards for exchanging data through the SHIN-NY. The SCP Policies' "consent to access" model allows providers seeking access to information to obtain patient consent at the point of care on behalf of other providers whose information has been uploaded to the SHIN-NY and is being disclosed. This model vests responsibility with the provider most motivated to obtain consent, or the provider that needs the information at that moment to deliver services. The model also enables information to be uploaded for storage in the SHIN-NY before patient consent has been provided, which allows emergency medical providers to "break the glass" and access information in an emergency. The SCP Policies also establish a range of standards on key data security issues, such as user authorization and authentication, access controls, and breach notification. By requiring all providers participating in the SHIN-NY to follow the SCP Policies, the state has created greater comfort among providers that reasonable safeguards are in place throughout the system.

States can also help health care providers and plans formulate a strategy for obtaining patient consent in a manner that minimizes operational burdens. For example, if information sharing is occurring as part of a targeted care management program, states can encourage participating providers to obtain patient consent as part of program enrollment. Consent for the disclosure of health information can be provided by patients as part of their consent to participate in the program generally, in much the same way providers obtain consent to disclose information when they get informed consent from patients to participate in a clinical trial. This approach eliminates the need for additional workflows. The consent can cover exchange among all providers in the program, minimizing the need for duplicative efforts by multiple providers and plans.

Finally, states help providers understand that health information sharing does not have to be undertaken on a regional or national level right out of the gate. Starting small and sharing information among a targeted set of providers for a discreet group of patients participating in a targeted initiative (e.g., a care management program) will often yield quicker results. In this way, states can minimize some of the obstacles that often plague complex forms of community-wide health information sharing and providers can hit the ground running with data-sharing approaches, albeit on a smaller scale.

State Immunity Laws

To address concerns about malpractice liability based on a provider's reliance on the inaccurate or incomplete medical records of another provider, several states have enacted immunity laws designed to promote electronic health information exchange. Examples of such laws include:

- The NCHIE Act, which provides immunity for any health care provider who, in treating a patient, in good faith relies upon information provided through the HIE Network.
- *The Illinois Health Information Exchange and Technology Act,*[22] which provides that any health care provider who relies in good faith upon any information provided through the statewide health information network in treating a patient, is immune from criminal or civil liability arising from any damages caused by such good faith reliance. The immunity does not apply to acts or omissions constituting gross negligence or reckless, wanton, or intentional misconduct.

Promoting Technological Solutions to Data Segmentation

As discussed, one of the challenges in minimizing the burden of consent management is tagging or segregating the subset of data that cannot be disclosed without patient consent and allowing other data to flow between providers. If the sensitive data cannot be targeted, providers may need to obtain patient consent for all disclosures, even if most disclosures do not require consent.

Applying different disclosure rules within an exchange environment is easier when the rules are provider or facility-based. For example, more stringent rules can be applied to Part 2 providers than other providers. But the challenge is far greater when different disclosure rules apply to data that is comingled in the medical records of a single provider.

For example, if a state law applies more restrictive disclosure rules to the mental health information maintained by a general hospital or medical group, a single rule cannot be applied to all of the data held by those providers. Restrictions on the improper re-disclosure of sensitive information without patient consent may create the same challenge. For instance, information received by a general medical provider from a Part 2 provider may not be re-disclosed by the general medical provider, except as permitted by the Part 2 regulations. Thus, if information subject to Part 2 is mixed with other health information by a general medical provider, the re-disclosure of the provider's entire medical record through a data exchange without patient consent is problematic. In these more difficult situations, data segmentation may provide a solution.

Data segmentation is defined as "the process of sequestering from capture, access, or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share."[23] Data segmentation could allow health care providers to separate sensitive health information that is subject to more stringent legal privacy protection from other less restrictively regulated data; and withhold the more stringently protected information from exchange until patient consent has been obtained.

But there are a number of technical challenges to data segmentation. To be segmented, electronic health information

must be structured and coded so that computers can distinguish between different types of health information and consistently treat them separately. Today, much electronic health information is unstructured, having been entered into electronic systems using free-text fields that computers cannot easily segment. Further, while some electronic health record products are capable of segmenting information at the health care encounter level, they may not be able to segment ancillary services, such as prescriptions and laboratory results.

A recent *pilot program* sponsored by the federal Office of the National Coordinator involving the University of Texas, Conernaugh Health System, and Jericho Systems Corporation showed some promising results regarding the ability of providers to filter parts of a patient's medical record in an electronic exchange environment. State governments could participate in or sponsor similar pilots. In addition, states may be in a position to move the health information technology marketplace by creating incentives or mandates for providers to adopt electronic health record systems that incorporate data filtering capacity.

Conclusion

Since there is no single obstacle to data-sharing between physical and behavioral health care providers and stakeholders, states should engage in a variety of strategies to address privacy concerns that limit data-sharing and impede efforts to integrate physical and behavioral health care. States will need to employ several tools to reduce or eliminate barriers to data-sharing while working within the patchwork of applicable federal and state privacy laws. States can and should use different tools and approaches depending on the specific situation, service, or state in question. To improve integration between medical and behavioral health care, it is also imperative for states to foster a dialogue on actual versus perceived barriers to data-sharing and to address misperceptions. Furthermore, states must understand the nature of data exchange initiatives within their state and develop strategies relevant to for electronic and non-electronic communication as appropriate to current data exchange methods and practices. The critical step for states is to get started. The sooner states develop and engage in a strategy to facilitate robust data-sharing to support care integration, the more productive electronic data exchange can occur, and the earlier quality of care for patients will be improved.

Endnotes

1. *The Health Insurance Portability and Accountability Act, Standards for Privacy of Individually Identifiable Health Information*, 45 CFR 160, 164 (a)(e), US Dept of Health and Human Services (August 14, 2002) US Government Printing Office.
2. *The Health Insurance Portability and Accountability Act, Privacy of Individually Identifiable Health Information, Definitions*, 45 CFR 164.501, US Dept of Health and Human Services (February 20, 2013) US Government Printing Office.
3. *The Health Insurance Portability and Accountability Act, Privacy of Individually Identifiable Health Information, Uses and Disclosures to Carry Out Treatment, Payment, Or Health Care Operations*, 45 CFR 164.506(c), US Dept of Health and Human Services (January 25, 2013) US Government Printing Office.
4. *The Health Insurance Portability and Accountability Act, Privacy of Individually Identifiable Health Information, Uses and Disclosures for Which an Authorization is Required*, 45 CFR 164.508(a)(2), US Dept of Health and Human Services (January 25, 2013) US Government Printing Office.
5. *The Health Insurance Portability and Accountability Act, Definitions*, 45 CFR 164.501.
6. *The Health Insurance Portability and Accountability Act, Uses and Disclosures of Protected Health Information: General Rules*,45 CFR 164.502(b)(2), US Dept of Health and Human Services (January 25, 2013) US Government Printing Office.
7. *The Health Insurance Portability and Accountability Act, Other Requirements Relating to Uses and Disclosures of Protected Health Information*, 45 CFR 164.514(d), US Dept of Health and Human Services (June 7, 2013) US Government Printing Office.
8. *The American Recovery and Reinvestment Act of 2009, The Health Information Technology for Economic and Clinical Health Act*, Pub. L. No. 111-5, 111th Cong., 1st. Sess. (February 13, 2009) Congress.gov.
9. US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Substance Abuse Treatment. *The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs.* Washington: US Department of Health and Human Services; 2004. *http://www.samhsa.gov/healthprivacy/docs/samhsapart2-hipaacomparison2004.pdf* (accessed December 1, 2013).
10. *Confidentiality of Alcohol and Drug Abuse Patient Records, Form of Written Consent*, 42 CFR 2.31, US Dept of Health and Human Services (October 1, 2013) US Government Printing Office.
11. *Confidentiality of Alcohol and Drug Abuse Patient Records, Prohibition on Redisclosure*, 42 CFR 2.32, US Dept of Health and Human Services (October 1, 2013).
12. *Administrative Data Standards and Related Requirements, General Administrative Requirements, Preemption of State Law, Definitions*, 45 CFR 160.202-203, US Dept of Health and Human Services (January 25, 2013).

13. Individual's Rights to Medical Information Privacy—FAQs. State of California Office of Health Information Integrity, Sacramento: State of California, 2012, *http://www.ohii.ca.gov/calohi/MedicalPrivacyEnforcement/ReportingViolation/FAQs.aspx*.

14. *Confidentiality of Medical Information Act*, Cal. Civ. Code 56 et seq., State of California (September 9, 2013).

15. *Confidentiality of Medical Information Act*, Cal. Civ. Code §§ 56.10, 11 & 13.

16. *Confidentiality of Medical Information Act*, Cal. Civ. Code § 56.05(f).

17. *Confidentiality of Medical Information Act*, Cal. Civ. Code § 56.104.

18. *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE).* Washington: the Legal Action Center for the Substance Abuse and Mental Health Services Administration, US Department of Health and Human Services, *http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf* (no publish date given) (accessed December 1, 2013).

19. North Carolina Health Information Exchange. Raleigh, N.C.; North Carolina Health Information Exchange, 2014, *http://nchie.org/* (accessed December 1, 2013).

20. *Nevada Revised Statutes, Administration of Public Health, Miscellaneous Provisions*, Nev. Rev. Stat. 439.538 (2007) *https://www.leg.state.nv.us/NRS/NRS-439.html#NRS439Sec538*

21. Protected Health Information, Civil or Criminal Liability, Ohio Rev. Code. Ann. §3798.08, 129th Ohio General Assembly (September 10, 2012) *http://codes.ohio.gov/orc/3798*.

22. Illinois Health Information Exchange and Technology Act, Public Act 96-1331 codified at 20 Ill. Comp. Stat. 3860/40, Illinois General Assembly (July 27, 2010) Legislative Information System.

23. Goldstein M and Rein A, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis.* Washington: Office of the National Coordinator for Health IT, 2010. *http://www.healthit.gov/sites/default/files/gwu-data-segmentation-final.pdf*