

INCLUSION OF BEHAVIORAL HEALTH INFORMATION IN EXCHANGES: CAN IT BE DONE?¹

The Issue

There is a national push to provide patients with more integrated and coordinated care in order to achieve better outcomes and to provide treatment more efficiently. One way to do this is for providers to share patient health information through health information exchanges ("HIEs").

Efforts are underway to develop HIEs and begin exchanging health information through them. However, concerns have been raised regarding whether behavioral health providers² can legally disclose patient health information to HIEs without violating State and Federal confidentiality laws. The applicable laws, and their impact on the inclusion of behavioral health information in HIEs, are discussed below.

Short Answer

HIPAA permits mental health information to be used and disclosed to HIEs for treatment, payment and healthcare operations among affiliated members of an HIE without express patient consent or authorization. However, 42 CFR Part 2 requires express patient consent for protected substance abuse treatment information to be exchanged on an HIE. The primary Oklahoma law pertaining to the confidentiality of mental health information is consistent with federal law. However, certain professional privilege statutes have not been amended to be consistent with HIPAA and may still require patient consent to disclose PHI to an HIE. Trade groups representing psychiatrists, psychologists and other behavioral health practitioners remain concerned about protecting patient confidentiality and the electronic exchange of behavioral health information and have promulgated codes of ethics and other directives that impact and may limit the electronic exchange of such behavioral health information without patient consent.

Health Insurance Portability and Accountability Act ("HIPAA")³

HIPAA establishes a set of national standards for the protection of health information. It provides a federal floor for medical privacy protection while preserving more stringent state laws. HIPAA addresses the use and disclosure of individuals' health information, referred to as

¹ Prepared by Crowe & Dunlevy, P.C. for the Oklahoma Department of Mental Health and Substance Abuse Services, 2012. This paper is intended for educational purposes only and should not be construed as legal advice.

² As used in this document, the term "behavioral health provider" includes mental health and substance abuse treatment providers.

³ "HIPAA" refers to the Standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 C.F.R. Parts 160 and 164, as amended from time to time including, but not limited to the amendments made by Title XIII of the American Recovery and Reinvestment Act of 2009 called the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

“protected health information” or "PHI"⁴ by organizations subject to HIPAA, which are called “covered entities.”⁵ Health care providers are covered entities. In addition, HIPAA establishes standards for individuals' privacy rights to understand and control how their health information is used and mandates certain administrative requirements.

HIPAA does not distinguish between mental health information and physical health information, with one narrow exception for psychotherapy notes.⁶ Psychotherapy notes are notes recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.⁷

Under HIPAA, a health care provider with a direct treatment relationship with a patient may use or disclose a patient's PHI without obtaining patient authorization for purposes of treatment⁸, payment⁹, and health care operations.¹⁰ For uses and disclosures of PHI *other than* for treatment, payment, and health care operations, a health care provider must obtain the patient's written authorization unless otherwise permitted or required by law.¹¹

⁴ PHI is defined as individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. 45 C.F.R. § 160.103. PHI does not include 'de-identified' health information which is health information that does not identify the patient and in which there is no reasonable basis to believe that the health information can be used to identify the patient.

⁵ Id.

⁶ See, Malke, Linda A., and Brian Krex, "HIPAA and Mental Health Information: Know the Law," *In Confidence* 10:11 (November 2002), pg. 1-2.

⁷ 45 C.F.R. § 164.501. The definition of psychotherapy notes excludes medication prescription and monitoring, counseling sessions 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.

⁸ Treatment is defined as the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another. 45 C.F.R. § 164.501.

⁹ Payment includes various activities of health care providers to obtain payment or reimbursement for his or her services. 45 C.F.R. § 164.501.

¹⁰ Health care operations generally include certain administrative, financial, legal and quality improvement activities necessary to run a health care provider's business. 45 C.F.R. § 164.501.

¹¹ 45 C.F.R. § 164.506. For example, an individual's authorization is required to use PHI for research. Also, authorization is required for fundraising activities, except for limited activities involving only demographic information and date of service, and for marketing activities, except for certain face-to-face encounters and promotional gifts of nominal value.

Health care providers are also permitted to disclose PHI to "business associates"¹² without a patient's authorization as long as a Business Associate Agreement has been executed pursuant to which the business associate agrees to comply with HIPAA.¹³ The HITECH Act clarified that HIEs can be business associates of covered entities.¹⁴ Although consent or authorization may not always be required, HIPAA requires health care providers, on the first encounter with the patient, to provide patients with notice of the provider's privacy policies and to make a good faith effort to obtain written acknowledgment of the patient's receipt of the notice.¹⁵

In 2008, the Office of the National Coordinator ("ONC")¹⁶ issued *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* ("the Privacy and Security Framework"). In conjunction with the Privacy and Security Framework, the ONC issued a series of fact sheets ("Fact Sheets") to provide guidance intended to address common questions relating to electronic health information exchange. The Fact Sheets refer to HIEs as health information organizations ("HIOs"). The following Frequently Asked Questions are reprinted, verbatim, from the ONC Fact Sheets.

Can a health information organization (HIO), as a business associate, exchange protected health information (PHI) with another HIO acting as a business associate?

Yes, so long as the disclosure of PHI is authorized by the HIO's business associate agreement and the information exchange would be permitted by the HIPAA Privacy Rule. For example, a HIO may disclose, on behalf of a primary care

¹² Business associates are individuals or entities, other than members of the covered entity's workforce, that receive, create, or have access to PHI and perform a function or service on behalf of the covered entity. 45 C.F.R. § 160.103.

¹³ 45 C.F.R. § 164.504(e). The business associate agreement must include provisions such as the following: restrictions on how the business associate may use or disclose the PHI; a promise to protect the information; an obligation to return or destroy the information at the end of the contract; and assurances to make the information available to the covered entity for compliance purposes.

¹⁴ Section 13408 of the HITECH Act adds the following to the definition of business associate: "Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a [business associate agreement]. . .

¹⁵ This notice is referred to as a Notice of Privacy Practices. 45 C.F.R. § 164.520.

¹⁶ The full name of the ONC is the Office of National Coordinator for Health Information Technology. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). ONC is the principal Federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information.

physician, PHI about an individual for treatment purposes in response to a query from another HIO, acting on behalf of a hospital at which the individual is a patient, unless, for instance, the primary care physician has agreed to the patient's request to restrict such disclosures. Similarly, a HIO that is a business associate of two different covered entities may share PHI it receives from one covered entity with the other covered entity as permitted by the Privacy Rule and its business associate agreement, for example, for treatment purposes, subject to any applicable restrictions.¹⁷

How do HIPAA authorizations apply to an electronic health information exchange environment?

The HIPAA Privacy Rule requires the individual's written authorization for any use or disclosure of protected health information (PHI) not otherwise expressly permitted or required by the Privacy Rule. For example, authorizations are not generally required to disclose PHI for treatment, payment, or health care operations purposes because covered entities are permitted to use and disclose PHI for such purposes, with few exceptions. Thus, to the extent the primary purpose of any electronic health information exchange is to exchange clinical information among health care providers for treatment, HIPAA authorizations are unlikely to be a common method of effectuating individual choice for the exchange. However, if the purpose of a covered entity sharing PHI through a health information organization is for a purpose not otherwise permitted by the Privacy Rule, then a HIPAA authorization would be required. In such cases, the Privacy Rule would allow covered entities to disclose PHI pursuant to an electronic copy of a valid and signed authorization. Further, the Privacy Rule allows HIPAA authorizations to be obtained electronically from individuals, provided any electronic signature is valid under applicable law.¹⁸

Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to Opt-In or Opt-Out of electronic health information exchange?

Yes. In particular, the Privacy Rule's provisions for optional consent and the right to request restrictions can support and facilitate individual choice with respect to the electronic exchange of health information through a networked environment, depending on the purposes of the exchange. The Privacy Rule allows covered entities to obtain the individual's consent in order to use or disclose protected health information (PHI) for treatment, payment, and health care operations purposes. If a covered entity chooses to obtain consent, the Privacy Rule provides the covered entity with complete flexibility as to the content and manner of obtaining the consent. 45 C.F.R. § 164.506(b). Similarly, the Privacy Rule also provides individuals with a right to request that a covered entity restrict uses or

¹⁷ ONC Fact Sheet, *Introduction*, pg. 3. The questions and answers are also included as FAQs on the Office of Civil Rights website: <http://www.hhs.gov/ocr/privacy/hipaa/faq>.

¹⁸ ONC Fact Sheet, *Individual Choice*, pg. 4-5.

disclosures of PHI about the individual for treatment, payment, or health care operations purposes. *See*, 45 C.F.R. § 164.522(a). While covered entities are not required to agree to an individual's request for a restriction, they are required to have policies in place by which to accept or deny such requests.¹⁹ Thus, covered entities may use either the Privacy Rule's provisions for consent or right to request restrictions to facilitate individual choice with respect to electronic health information exchange.

Further, given the Privacy Rule's flexibility, covered entities could design processes that apply on a more global level (e.g., by requiring an individual's consent prior to making any disclosure of PHI to or through a health information organization (HIO), or granting restrictions only in which none of the individual's information is to be exchanged to or through the HIO) or at a more granular level (such as by type of information, potential recipients, or the purposes for which a disclosure may be made). Whatever the policy, such decisions may be implemented on an organization-wide level, or across a HIO's health information exchange (such as based on the consensus of the health information exchange participants).²⁰

Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to decide whether sensitive information about them may be disclosed to or through a health information organization (HIO)?

Yes. To the extent a covered entity is using a process either to obtain consent or act on an individual's right to request restrictions under the Privacy Rule as a method for effectuating individual choice, policies can be developed for obtaining consent or honoring restrictions on a granular level, based on the type of information involved. For example, specific consent and restriction policies could be developed, either on an organization level or HIO level, for HIV/AIDS, **mental health**, genetic, and/or **substance abuse information**. In addition, there may be other Federal and State laws that will affect a covered entity's exchange of this sensitive information to or through a HIO, and covered entities should consider these other laws when developing individual choice policies. . . (Emphasis added.)²¹

Does the HIPAA Privacy Rule permit a covered entity to disclose psychotherapy notes to or through a health information organization (HIO)?

¹⁹ The HITECH Act changed this in one regard. Now, a covered entity **must** comply with the requested restriction if (a) the patient requests restriction on disclosure of PHI to a health plan for purposes of carrying out payment or health care operations (and not for purpose of carrying out treatment), except as otherwise required by law; and (b) the PHI pertains solely to a health care item or service for which OMH or other health care provider involved has been paid by the patient in full and no payment is sought from any third party.

²⁰ ONC Fact Sheet, *Individual Choice*.

²¹ *Id.*, pg. 5.

Yes, provided the covered entity has obtained the individual's written authorization in accordance with 45 C.F.R. § 164.508. . . With few exceptions, the Privacy Rule requires a covered entity to obtain individual authorization prior to a disclosure of psychotherapy notes, even for a disclosure to a health care provider other than the originator of the notes, for treatment purposes. For covered entities operating in an electronic environment, the Privacy Rule does, however, allow covered entities to disclose protected health information pursuant to an electronic copy of a valid and signed authorization, as well as to obtain HIPAA authorizations electronically from individuals, provided any electronic signature is valid under applicable law.²²

Substance Abuse Information, 42 C.F.R. Part 2 ("Part 2")

Federal statutes mandate special treatment for alcohol and drug abuse patient records, collectively referred to as substance abuse treatment records.²³ In addition to this statute, the accompanying federal regulations concerning confidentiality of these records provide guidance in even greater detail.²⁴

Records of the "identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research" are confidential and can be disclosed only under the circumstances authorized by 42 U.S.C. § 290dd-2 or the accompanying regulations.²⁵ These requirements apply to any records of a program which is "federally assisted."²⁶ This means any "program" that is funded directly or indirectly by a federal agency, including Medicare, and any facility licensed or certified as a Medicare provider or registered to dispense controlled substances for treatment of alcohol or drug abuse.²⁷ A "program" is defined in 45 C.F.R. § 2.11 as:

1. An individual or entity (other than a general medical care facility) who holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment; or
2. An identified unit within a general medical facility which holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment; or

²² *Id*, pg. 6.

²³ 42 U.S.C. §290dd-2.

²⁴ These regulations are found at 42 C.F.R. Part 2.

²⁵ 42 U.S.C. § 290dd-2(a).

²⁶ 42 C.F.R. § 2.3.

²⁷ 42 C.F.R. § 2.12(b). Clinicians who use controlled substance (e.g., benzodiazepines or methadone) for detoxification or maintenance treatment of a substance use disorder require a federal DEA registration and become subject to Part 2 through the DEA license.

3. Medical personnel or other staff in a general medical care facility whose primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment and who are identified as such providers.²⁸

Importantly, to the extent applicable, this federal law protects all medical information in a patient's record maintained by a program, including those records unrelated to the substance abuse treatment, according to at least one state supreme court.²⁹ At the time of the patient's admission or as soon as the patient is capable of communication, the patient must be given the notice of confidentiality set forth at 42 C.F.R. § 2.22(d).

Both the statute and the regulations specify that when records are released with the patient's consent, specific guidelines must be followed. The requirements for patient consent concerning these records are unique in that the consent form must describe the purpose for the disclosure; the specific name of the facility or program permitted to make the disclosure and to which disclosure is to be made; and the date on which the consent was signed and on which it will expire.³⁰ If no date is stated, the authorization expires in six (6) months.

Substance abuse records disclosed pursuant to the patient's written consent must be accompanied by the following specific statement:

This information has been disclosed to you from records protected by Federal confidentiality rules (42 C.F.R. 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 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules

²⁸ General medical hospitals that do not have identified substance abuse units and do not otherwise fall within this definition of a program, are not subject to these federal regulations. Further, in the case of *Center for Legal Advocacy v. Earnest*, 320 F.3d 1107 (10th Cir. 2003), the court held that a hospital's emergency department did not constitute a "program" subject to the regulations, in light of the fact that (i) the primary function of emergency room personnel was not the provision of alcohol or drug abuse diagnosis, treatment or referral; and (ii) the emergency department of the hospital did not promote itself to the community as a provider of substance abuse services. The court reached this conclusion even though the hospital did have a substance abuse program within the hospital and the evidence showed substantial integration of the emergency room records and records of program participants.

²⁹ See, *Jane H. v. Rothe*, 488 N.W.2d 879 (N.D. 1992) and *In re R. O.*, 631 N.W. 2d 159 (N.D. 2001).

³⁰ A Part 2 consent form must include the following elements: (a) Name or general designation of the program or person permitted to make the disclosure; (b) Name or title of the individual or name of the organization to which disclosure is to be made; (c) Name of the patient; (d) Purpose of the disclosure; (e) How much and what kind of information is to be disclosed; (f) Signature of patient (and, if applicable, a parent or guardian); (g) Date on which consent is signed; (h) Statement that the consent is subject to revocation at any time except to the extent that the program has already acted on it; and (i) Date, event, or condition upon which consent will expire if not previously revoked.

restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

In light of these significant limitations regarding the release of substance abuse information, authorizations for the release of PHI should specifically restrict redisclosure of substance abuse information maintained by a program, even to persons or entities who are not subject to the HIPAA.

Disclosure of substance abuse patient records may be made without the patient's consent under the following circumstances:

1. to medical personnel as needed in a medical emergency;
2. to qualified personnel for scientific research, financial audits or program evaluation so long as patient identities are not disclosed in reports resulting from these activities;
3. pursuant to a court order which contains all of the required information described in the regulations and after the court determines there is good cause for the release.³¹

The differences between the disclosure provisions of HIPAA and 42 C.F.R Part 2 are summarized in the following table.³²

42 C.F.R. Part 2	HIPAA Privacy Rule
<p>Programs may not use or disclose any information about any patient unless the patient has consent in writing (on a form that meets the requirements established by the regulations) or unless another very limited exception specified in the regulations applies. Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure.</p>	<p>HIPAA permits uses and disclosures for "treatment, payment and health care operations" as well as certain other disclosures without the individual's prior written authorization. Disclosures not otherwise specifically permitted or required by the Privacy Rule must have an authorization that meets certain requirements. With certain exceptions, HIPAA generally requires that uses and disclosures of PHI be the minimum necessary for the intended purpose of the use or disclosure.</p>

On June 17, 2010, the Substance Abuse and Mental Health Services Administration ("SAMHSA") and the Office of the National Coordinator ("ONC") for Health Information Technology released *Frequently Asked Questions ("SAMHSA FAQs") for Applying the Substance*

³¹ 42 U.S.C. § 290dd-2(b)(2).

³² Reprinted from *The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs*, U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration ("SAMHSA"), 2004.

*Abuse Confidentiality Regulations to Health Information Exchange (HIE).*³³ The SAMHSA FAQs set forth the general provisions of Part 2, provide guidance on the application of Part 2 to electronic health records (EHRs), and identify methods for including substance abuse patient record information into health information exchanges that are consistent with the Federal statute.³⁴ Several of the more pertinent SAMHSA FAQs are reprinted, verbatim, below.³⁵

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

A1 Yes. The federal confidentiality law and regulations (codified at 42 U.S.C. § 290dd-2 and 42 CFR Part 2 ("Part 2")), enacted almost three decades ago after Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, has been a cornerstone practice for substance abuse treatment programs across the country. Part 2 permits patient information to be disclosed to Health Information Organizations (HIOs) and other health information exchange (HIE) systems; however, the regulation contains certain requirements for the disclosure of information by substance abuse treatment programs; most notably, patient consent is required for disclosures, with some exceptions.

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

A4. No. HIOs may take any number of forms and perform a variety of functions on behalf of the health care providers and other entities participating in the HIO network. Regardless of the functions performed by the HIO, 42 CFR Part 2 still applies. . . [*Remainder of answer omitted.*]

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

A5. Unlike HIPAA, which generally permits the disclosure of protected health information without patient consent or authorization for the purposes of treatment, payment, or health care operations, Part 2, with limited exceptions (i.e., medical emergencies and audits and evaluations), requires patient consent for such disclosures (42 CFR §§ 2.3, 2.12, 2.13). Some types of exchange, however, may take place without patient consent when a qualified service organization agreement ("QSOA") exists or when exchange takes place between a Part 2

³³ The stated purpose of the FAQs is for SAMHSA and ONC to provide constituents with "every tool and resource possible to enable a more complete understanding of these federal regulations which were enacted in 1972 and in 1975 [42 CFR Part 2]."

³⁴ <http://www.samhsa.gov/HealthPrivacy/docs/EHR-FAQs.pdf>

³⁵ There are 37 questions and answers contained in the SAMHSA FAQs.

program and an entity with administrative control over that program.³⁶ .
.[Remainder of answer omitted.]

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

A6. Yes. A QSOA under Part 2, which is similar but not identical to a business associate agreement under §§ 164.314(a) and 164.504(e) of the HIPAA Security and Privacy Rules, is a mechanism that allows for disclosure of information between a Part 2 program and an organization that provides services to the program, such as an HIO. Examples of services that an HIO might provide include holding and storing patient data, receiving and reviewing requests for disclosures to third parties, and facilitating the electronic exchange of patients' information through the HIO network.

Before a Part 2 program can communicate with a Qualified Services Organization – in this case the HIO – it must enter into a two-way written agreement with the HIO. Once a QSOA is in place, Part 2 permits the program to freely communicate information from patients' records to the HIO as long as it is limited to that information needed by the HIO to provide services to the program. The HIO may also communicate with the Part 2 program and share information it receives from the program back with the program. Patient consent is not needed to authorize such communication between the HIO and Part 2 program when a QSOA is in place between the two.

Q7. May information protected by Part 2 be made available to an HIO for electronic exchange?

A7. Information protected by 42 CFR Part 2 may only be made available to an HIO for exchange if:

- 1) a patient signs a Part 2-compliant consent form authorizing the Part 2 program to disclose the information to the HIO; *OR*
- 2) A Qualified Service Organization Agreement ("QSOA") is in place between the Part 2 program and the HIO.

³⁶ A qualified service organization ("QSO") means a person or organization that: (1) provides services to a [Part 2] program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting or other professional services or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and (2) has entered into a written agreement with a program under which that person (a) acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the programs, it is fully bound by these regulations; and (b) if necessary, will resist in judicial proceedings any efforts to obtain access to patient records, except as permitted by these regulations.

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

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

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

A9. HIOs have adopted a number of different policies for making general clinical information available to participating members. Some HIOs have adopted a "no consent" model, under which a patient's health information may be disclosed to an HIO and subsequently disclosed by the HIO to its affiliated members for specified purposes without obtaining the patient's consent. Other HIOs have adopted an "opt in" model, in which the patient's information is disclosed to the HIO and subsequently disclosed by the HIO to affiliated members for specified purposes only if the patient has affirmatively agreed to such disclosures. Yet other HIOs have adopted an "opt out" model, in which the patient's information is disclosed to the HIO and subsequently disclosed by the HIO to affiliated members for specified purposes unless the patient has affirmatively declined to participate in such exchange.³⁷

Regardless of which model the HIO adopts for exchanging general clinical information, the HIO must still comply with the requirements of 42 CFR Part 2 with respect to Part 2 information. This means that even if an HIO adopts a "no consent" model for other information, the patient's Part-2 compliant consent must be obtained to disclose Part 2 information to or through the HIO. On the other hand, the HIO may impose requirements in addition to 42 CFR Part 2. For example, because an "opt in" model requires affirmative patient consent to participate in the HIO, a Part 2 program may need to obtain patient consent to disclose Part 2 information to an HIO even if the Part 2 program has a QSOA with the HIO.

³⁷ This discussion of patient choice models relies upon definitions presented in "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" found on the ONC web page. There are variations on these general models; however, the principles with respect to 42 CFR Part 2 apply to all models.

Oklahoma Law

The primary Oklahoma statute pertaining to the confidentiality of behavioral health information is 43A O.S. § 1-109 ("Section 1-109").³⁸ At one time, Section 1-109 was inconsistent with HIPAA as it related to the confidentiality of mental health information. Section 1-109 required patient consent, even for disclosures for treatment, payment or healthcare operations. However, Section 1-109 has been amended over the years and now appears to be generally consistent with HIPAA in its treatment of mental health information. Substance abuse information continues to be afforded higher protection pursuant to Part 2 and Section 1-109 is consistent with Part 2.

Specifically, in regard to uses and disclosures for treatment, payment and health care operations, the language that most directly impacts disclosures to HIEs, Section 1-109 provides:

E. An authorization shall not be required for the following uses and disclosures, but information disclosed pursuant to one of these exceptions must be limited to the minimum amount of information necessary:

1. Disclosure by health care provider of mental health information necessary to carry out another provider's own treatment, payment, or health care operations. Such disclosures shall be limited to mental health information and shall not include substance abuse information. . . .³⁹

Section 1-109 is not the only Oklahoma statute pertaining to the confidentiality of PHI. There are numerous professional privilege statutes that provide protection for health information created and maintained in the treatment context. One example is the Oklahoma Patient-Physician Privilege.⁴⁰ At one time, the Oklahoma Patient-Physician privilege was more stringent than HIPAA and was not preempted because it limited a physician's ability to disclose PHI without patient consent.

Fortunately, the Oklahoma Patient-Physician Privilege has been amended to clarify that it is a testimonial privilege only and that it does not make communications confidential when state and federal privacy laws would otherwise permit disclosures. Therefore, since HIPAA does not require patient consent for disclosures for treatment, payment and healthcare operations, neither does the Oklahoma Patient-Physician Privilege. This is significant because if the Oklahoma Patient-Physician Privilege had not been amended, express patient consent would have been

³⁸ The HIPAA regulations discussed above were adopted, in part, to create a uniform, national system for the use and disclosure of medical records and other PHI. These regulations provide that they will preempt, or take precedence over, any state laws that are contrary to the provisions of the HIPAA Privacy and Security Regulations. 45 CFR §160.202. However, a state law that is "more stringent" than HIPAA will be saved from preemption. 45 CFR § 160.203. Because 43A O.S. § 1-109 was deemed to be "more stringent" in the protections it afforded patients, it was not pre-empted.

³⁹ 43A O.S. § 1-109 E.1.

⁴⁰ 12 O.S. §2503.

required to use and disclose PHI for treatment, payment and health care operations, including disclosures to an HIE for such purposes.

The Oklahoma Patient-Psychologist Privilege⁴¹ contains a cross-reference to the Oklahoma Patient-Physician Privilege. Therefore, even though the Patient-Psychologist Privilege also includes a provision requiring patient consent to disclose PHI, presumably a disclosure for treatment, payment and health care operations is permissible because it is permissible under the Patient-Physician Privilege. Specifically, the pertinent part of the Patient-Psychologist Privilege provides as follows:

All communications between a licensed psychologist and the individual with whom the psychologist engages in the practice of psychology are confidential. At the initiation of the professional relationship the psychologist shall inform the patient of the following limitations to the confidentiality of their communications. No psychologist, colleague, agent or employee of any psychologist, whether professional, clerical, academic or therapeutic, shall disclose any information acquired or revealed in the course of or in connection with the performance of the psychologist's professional services, including the fact, circumstances, findings or records of such services, except under the following circumstances:

1. Pursuant to the provisions of Section 2503 of Title 12 of the Oklahoma Statutes [Patient-Physician Privilege] or where otherwise provided by law;
2. Upon express, written consent of the patient . . .⁴²

Unfortunately, there are other Oklahoma professional privilege laws pertaining to behavioral health providers that appear to provide more protection for PHI and will not be preempted unless amended to be consistent with the Patient-Physician Privilege. Thus, patient consent may still be required before these professionals can disclose patient PHI for treatment, payment and health care operations. For example, the Patient-Licensed Professional Counselor Privilege⁴³ does not cross-reference the Patient-Physician Privilege or other state or federal laws that permit uses and disclosure in certain circumstances without patient consent. The pertinent part of the Patient-Licensed Professional Counselor Privilege provides:

A. No person licensed pursuant to the provisions of the Licensed Professional Counselors Act shall knowingly and willfully disclose any information the licensee may have acquired from persons consulting the licensee in his professional capacity as a professional counselor or be compelled to disclose such information except:

1. With the written consent of the client, or in the case of death or disability of the client, the consent of his personal representative or other person authorized to sue

⁴¹ 59 O.S. §1376.

⁴² *Id.*

⁴³ 59 O.S. § 1910.

or the beneficiary of any insurance policy on his life, health or physical condition.

. . .⁴⁴

The privilege applicable to licensed marital and family therapists⁴⁵ is worded a little differently from the other professional privilege statutes; it focuses on situations in which a therapist may be required to disclose PHI. Specifically, the Licensed Marital and Family Therapist Privilege provides, in pertinent part:

A. No person licensed pursuant to the provisions of the Marital and Family Therapist Licensure Act as a marital and family therapist, nor any of his employees or associates, shall be required to disclose any information which he may have acquired in rendering marital and family therapy services, except when:

1. Authorized by other state laws;

. . .

5. A patient agrees to waiver of the privilege accorded by this section, in the case of death or disability of the patient, the consent of his personal representative or other person authorized to sue or the beneficiary of any insurance policy on his life, health or physical condition. In circumstances where more than one person in a family is receiving therapy, each such family member must agree to the waiver. Absent such a waiver from each family member, a marital and family therapist shall not disclose information received from any family member.⁴⁶

Because of the unique wording of the Licensed Marital and Family Therapist Privilege, it is unclear if a therapist may use and disclose PHI without patient consent. Nevertheless, in light of the ambiguity of the statute and the professional ethics below, all behavioral health providers, whether permitted by State and Federal laws, may want to obtain some type of patient consent to use and disclose PHI for treatment, payment and health care operations, including disclosure to an HIE for such purposes.

Professional Ethics

Professional codes of ethics establish requirements for patient confidentiality. For example, the *Ethical Principles of Psychologists and Code of Conduct* ("Principles") provides that "[p]sychologists have a primary obligation and [must] take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be required by law or established by institutional rules or professional or scientific relationship."⁴⁷ The Principles indicate that psychologists should discuss the relevant limits of confidentiality and foreseeable uses of the information generated through treatment.⁴⁸ The Principles provide that psychologists may disclose confidential

⁴⁴

Id.

⁴⁵

59 O.S. § 1925.11.

⁴⁶

Id.

⁴⁷

Ethical Principles of Psychologists and Code of Conduct, Standard 4.01, amended 2010.

⁴⁸

Id., Standard 4.02.

information *without* the consent of the patient "only as mandated by law, or where permitted by law for a valid purpose such as to (1) provide needed professional services; (2) obtain appropriate professional consultations; (3) protect the client/patient, psychologist, or others from harm; or (4) obtain payment for services from a client/patient, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose."⁴⁹

The American Psychiatric Association's ("APA") position on patient confidentiality is stringent. Section 4, paragraph 1 of *The Principles of Medical Ethics* provides:

Psychiatric records, including even the identification of a person as a patient, must be protected with extreme care. Confidentiality is essential to psychiatric treatment. This is based in part on the special nature of psychiatric therapy as well as on the traditional ethical relationship between physician and patient. Growing concern regarding the civil rights of patients and the possible adverse effects of computerization, duplication equipment and data banks makes the dissemination of confidential information an increasing hazard. Because of the sensitive and private nature of the information with which the psychiatrist deals, he or she must be circumspect in the information that he or she chooses to disclose to others about a patient. The welfare of the patient must be a continuing consideration.⁵⁰

Section 4, paragraph 2 of *The Principles of Medical Ethics* further states as follows:

A psychiatrist may release confidential information only with the authorization of the patient or under proper legal compulsion. The continuing duty of the psychiatrist to protect the patient includes fully apprising him/her of the connotations of waiving the privilege of privacy. . .⁵¹

The APA issued a Position Statement on Confidentiality of Computerized Records in 2010 ("Position Statement")⁵² that reinforces its concerns over PHI stored electronically. Although the Position Statement does not expressly address HIE, it is instructional. It provides as follows:

Patients should be able to benefit from the potential improvements in the delivery and quality of care with electronic health records, without being forced to relinquish the privacy and confidentiality of their personal health-related information. Approaches to electronic health record access should consider the diverse settings in which electronic health records will be used, including their use in emergency and other acute settings where rapid access to medically necessary information is essential. Such approaches should also consider that patients have a broad range of needs, preferences and abilities to provide

⁴⁹ *Id.*, Standard 4.05.

⁵⁰ *The Principles of Medical Ethics*, 2010 Edition.

⁵¹ *Id.*

⁵² The 2010 Position Statement revised a prior statement issued in 1997.

informed consent about the implications of electronic record access. At the very least, computerized records should give patients as much control over their information as they have with paper-based records. In addition, computerized records should not force patients to choose between either making all or none of their information available. Electronic health record design and implementation should leverage technology to give more flexible approaches to access for sensitive information. As health information technology continues to advance and evolve, the complexities and potential consequences of computerized records make it essential for psychiatrists to be aware of the implications for their patients and advocate for a culture of confidentiality and respect for patients.

Summary- Key Points

1. Patients should be informed of the potential uses and disclosures of their PHI, including the fact that it may be disclosed to an HIE and exchanged with affiliated members of the HIE. At a minimum, this information should be included in the NPP.
2. Mental health information is treated like general health information under HIPAA, with the exception of psychotherapy notes. Pursuant to HIPAA, mental health information (except for psychotherapy notes) can be used and disclosed by and through HIEs for treatment, payment and healthcare operations without patient consent or authorization. The primary Oklahoma law pertaining to the confidentiality of mental health information is consistent with federal law. However, certain professional privilege statutes have not been amended to be consistent with HIPAA and may still require patient consent to disclose PHI to an HIE.
3. Substance abuse information created and maintained by a federally assisted substance abuse treatment program is subject to heightened requirements under Part 2. Written patient consent is required to exchange information covered under Part 2 by and among HIE affiliated members.
4. Professional codes of ethics generally indicate that mental health treatment providers have an obligation to maintain the confidentiality of patient information. Therefore, even in situations in which state and federal law permit disclosure to HIEs, providers should obtain some form of consent or "opt-in" to ensure patients are fully informed regarding disclosures of their PHI for such sensitive matters. Trade groups representing mental health treatment providers need to provide direction on the extent to which such providers can participate in HIEs.