INDIVIDUAL CHOICE

This is one of a series of companion documents to *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Privacy and Security Framework). This guidance document provides information regarding the HIPAA Privacy Rule as it relates to the Individual Choice Principle in the Privacy and Security Framework.

INDIVIDUAL CHOICE PRINCIPLE: Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

INDIVIDUAL CHOICE AND THE HIPAA PRIVACY RULE

The Individual Choice principle of the Privacy and Security Framework emphasizes that the opportunity and ability of an individual to make choices with respect to the electronic exchange of their individually identifiable health information is an important aspect of building trust. The Privacy and Security Framework also recognizes that the options for expressing choice and the level of detail for which choice may be made will vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information.

The Privacy Rule provides an individual with several rights intended to empower the individual to be a more active participant in managing his or her health information. These are the right to access certain health information maintained about the individual; the right to have certain health information amended; the right to receive an accounting of certain disclosures; the right to receive a covered entity's notice of privacy practices; the right to agree or object to, or authorize, certain disclosures; the right to request restrictions of certain uses and disclosures; and provisions allowing a covered entity to obtain consent for certain uses and disclosures. See 45 C.F.R. §§ 164.524, 164.526, 164.528, 164.520, 164.510, 164.508, 164.522, and 164.506, respectively. Assuming that a HIPAA covered entity intends to electronically exchange protected health information (PHI) to and through a particular health information organization (HIO), which we will identify as HIO-X here, primarily for the purpose of treatment, as described in the Introduction, the discussion below will focus on how the Privacy Rule's provisions for optional consent and the right to request restrictions on certain uses and disclosures can support and facilitate individual choice with respect to the electronic exchange of health information in a networked environment.

Optional Consent

The Privacy Rule's optional consent provisions offer covered entities the ability to adopt use and disclosure policies that build upon the Privacy Rule's baseline requirements and reflect a covered entity's own professional ethics and best judgment. The Privacy Rule defers to covered entities with regard to the decision of whether to obtain an individual's consent in order to use or disclose PHI for treatment, payment, and health care operations purposes, and with regard to the content of the consent and the manner of obtaining it. 45 C.F.R. § 164.506(b). In addition, the Privacy Rule does not prevent a covered entity from establishing a policy requiring individual consent in order to make certain other disclosures that are otherwise permitted by the Privacy Rule without individual consent or authorization. For example, while the Privacy Rule permits a covered entity to disclose an individual's information to law enforcement under certain conditions, nothing in the Privacy Rule precludes the covered entity from establishing a policy requiring individual consent to make such disclosures. Ultimately, the Privacy Rule allows each covered entity to tailor their consent policies and procedures, if any, according to what works best for their organization and the individuals with whom they interact.

Covered entities may elect to adopt an individual consent policy within an electronic health information exchange environment to accomplish several objectives. Covered entities may, for example, utilize the consent mechanism to obtain an individual's consent prior to making any disclosure of PHI to or through HIO-X. Alternatively, covered entities may obtain consent in a manner that limits electronic health information exchange disclosures on a more granular level. For example, a covered entity could obtain consent for disclosures for certain purposes, for disclosures to certain categories of recipients, or for exchanges of certain types of information (such as information that may be considered particularly sensitive). In addition, consent may be obtained either once or on a regular basis.

A consent regime 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, or based on a unilateral decision of the HIO that such consent is a requirement of participation). Regardless of the selected means, covered entities may utilize, at their discretion, a consent policy to tailor an individual's ability to effectively "opt-in" or "opt-out" of some or all electronic health information exchanges made to or through a HIO and thereby achieve the objectives behind the Individual Choice Principle.

An Individual's Right to Request Restrictions on Uses and Disclosures

The Privacy Rule also provides individuals with a right to request that a covered entity restrict uses or 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. If a covered entity does agree to a restriction, the Privacy Rule requires that the covered entity abide by the agreement, except if the information is needed to provide emergency treatment to the individual, or if the agreement is terminated, either as agreed to by the individual, or by the covered entity (in which case the termination applies only to PHI created or received after the individual is informed of the termination).

The Privacy Rule's right to request restrictions would naturally extend to electronic health information exchange environments and may similarly be utilized by covered entities as a mechanism to facilitate individual choice. Covered entities that choose to exchange PHI to or through a HIO may, therefore, want to consider their policies with respect to the right to request restrictions, and how they might respond to such requests in a manner that recognizes the importance of individual choice in building trust in such exchanges.

As with consent, the Privacy Rule does not prevent covered entities from establishing a policy for granting restrictions for certain other disclosures that are otherwise permitted by the Privacy Rule. Also, like consent, the Privacy Rule's right to request restrictions can be applied on a more global level (e.g., the covered entity can choose only to grant restrictions in which none of the individual's information is to be exchanged to or through the HIO) or the covered entity can choose to grant restrictions at a more granular level (such as by type of information to be restricted, potential recipients, or the purposes for which a disclosure may be made). Similarly, restriction policies that are tailored to an individual's preferences may be implemented at the covered entity level, or HIO level.

Covered entities that develop and implement restriction policies focused on giving individuals choices, including the ability to "opt-out" of or "opt-in" to an electronic health information exchange environment completely or selectively, may help build trust and confidence in the use of electronic exchange. Such efforts, thus, support the objectives underlying the Individual Choice Principle and are consistent with the Privacy Rule.

FREQUENTLY ASKED QUESTIONS

Q1: Does the HIPAA Privacy Rule inhibit electronic health information exchange across different states or jurisdictions?

A1: No. The Privacy Rule establishes a federal baseline of privacy protections and rights, which applies to covered entities consistently across state borders. The Privacy Rule, however, as required by HIPAA, does not preempt State laws that provide greater privacy protections and rights. Thus, as with covered entities that conduct business today on paper in a multi-jurisdictional environment, covered entities participating in electronic health information exchange need to be cognizant of States with more stringent privacy laws that will affect the exchange of electronic health information across State lines. In addition, other Federal laws also may apply more stringent or different requirements to such exchanges depending on the circumstances. Covered entities and health information

organizations (acting as their business associates) which participate in multi-jurisdictional electronic health information exchange should establish privacy policies for the network that accommodate these variances.

Q2: How do HIPAA authorizations apply to an electronic health information exchange environment?

A2: 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.

Q3: 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?

A3: 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 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. 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).

Q4: Who has the right to consent or the right to request restrictions with respect to whether a covered entity may electronically exchange a minor's protected health information to or through a health information organization (HIO)?

A4: As with a minor's paper medical record, generally a parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor is the personal representative of the minor under the HIPAA Privacy Rule and, thus, is able to exercise all of the HIPAA rights with respect to the minor's health information. Thus, a parent, guardian, or other person acting *in loco parentis* who is a personal representative would be able to consent to, if the covered entity has adopted a consent process under the Privacy Rule, or to request restrictions on, disclosures of the minor's health information to or through a HIO for treatment or other certain purposes. However, there are a few exceptions when the parent, guardian, or other person acting *in loco parentis* is not the personal representative of the minor child, such as:

(1) when State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service;

(2) when a court determines or other law authorizes someone other than the parent, guardian, or person acting *in loco parentis* to make treatment decisions for a minor; and

(3) when a parent, guardian, or person acting *in loco parentis* agrees to a confidential relationship between the minor and a health care provider. In such cases, it is only the minor, and not the parent(s), who may exercise the HIPAA rights with respect to the minor's health information.

Q5: 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)?

A5: 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. For example, such

laws may prescribe the form of consent that is required or create other requirements for the disclosure of information based on the type of information or the intended recipient.

Q6: Does the HIPAA Privacy Rule permit a covered entity to disclose psychotherapy notes to or through a health information organization (HIO)?

A6: Yes, provided the covered entity has obtained the individual's written authorization in accordance with 45 C.F.R. § 164.508. See 45 C.F.R. § 164.501 for the definition of "psychotherapy notes." 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.