COLLECTION, USE, AND DISCLOSURE LIMITATION

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 Collection, Use, and Disclosure Limitation Principle in the Privacy and Security Framework.

COLLECTION, USE, AND DISCLOSURE LIMITATION PRINCIPLE:

Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

COLLECTION, USE, AND DISCLOSURE LIMITATION AND THE HIPAA PRIVACY RULE

The Collection, Use, and Disclosure Limitation Principle in the Privacy and Security Framework emphasizes that appropriate limits should be set on the type and amount of information collected, used, and disclosed, and that authorized persons and entities should only collect, use, and disclose information necessary to accomplish a specified purpose. The Privacy Rule is consistent with the Collection, Use, and Disclosure Limitation Principle and supports adherence to the principle by covered entities that participate in electronic health information exchange in a networked environment. In particular, the Privacy Rule:

1) Generally requires covered entities to limit uses, disclosures, and requests of protected health information (PHI) to the minimum necessary; and
2) Defines and limits the uses and disclosures covered entities may make without an individual's authorization.

The Minimum Necessary Standard

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule also requires covered entities to take reasonable steps to limit any requests for PHI to the minimum necessary, when requesting such information from other covered entities. In some cases, the Privacy Rule does not require that the minimum necessary standard be applied, such as, for example, to disclosures to or requests by a health care provider for treatment purposes,

or to disclosures to the individual who is the subject of the information. See 45 C.F.R. §§ 164.502(b), 164.514(d).

For routine or recurring requests and disclosures, covered entities must implement reasonable policies and procedures (which may be standard protocols) to limit the information disclosed or requested. For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to the minimum necessary for the intended purpose, and review and limit each disclosure or request on an individual basis in accordance with these criteria. For certain disclosures, the Privacy Rule permits a covered entity to rely, if reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose, such as when the information is requested by another covered entity. 45 C.F.R. § 164.514(d)(3).

Further, a covered entity's contract with a business associate must limit the business associate's uses and disclosures of, as well as requests for, PHI to be consistent with the covered entity's minimum necessary policies and procedures, since a business associate contract may not authorize the business associate to use or further disclose the information in a manner that would violate the Privacy Rule. See 45 C.F.R. § 164.504(e)(2)(i).

Depending on the type of disclosure or request, it may be that some or many of the requests or disclosures to or through a health information organization (HIO) by a covered entity may not be subject to the Privacy Rule's minimum necessary standard. This would be true in the HIO-X case, for example, as described in the Introduction, whose primary purpose is to exchange electronic PHI between and among several hospitals, doctors, pharmacies, and other health care providers for treatment. However, even though the Privacy Rule does not require that the minimum necessary standard be applied to electronic health information exchanges for treatment purposes, covered entities engaging in electronic health information exchange and HIO-X are free to apply minimum necessary concepts to develop policies that limit the information they include and exchange, even for treatment purposes. For routine exchanges of information for treatment purposes, for example, the covered entities and HIO-X can come up with a standard set of information that should be included in an exchange and that would be considered minimally necessary for the purpose. Doing so would be consistent with the Collection, Use, and Disclosure Limitation Principle, and may help foster increased trust in electronic health information exchange.

For electronic health information exchanges by a covered entity to and through a HIO that are subject to the minimum necessary standard, such as for a payment or health care operations purpose, the Privacy Rule would require that the minimum necessary standard be applied to that exchange and that the business associate agreement limit the HIO's disclosures of, and requests for, PHI accordingly.

Defining and Limiting Uses and Disclosures

The Privacy Rule defines and limits the uses and disclosures of PHI a covered entity may make without the individual's authorization. In doing so, and consistent with the Collection, Use, and Disclosure Limitation Principle, the Privacy Rule defines the permitted uses and disclosures based on the purpose of the use or disclosure, and attaches conditions accordingly. For example, the Privacy Rule generally permits covered entities to disclose PHI for the core health care functions of treatment, payment for care, and health care operations, with few exceptions and limitations. In addition, in recognition of the important uses made of health information outside of the health care context, the Privacy Rule permits uses and disclosures for a number of additional public policy and benefit purposes, such as research or public health, without the individual's authorization. However, specific conditions or limitations apply to uses and disclosures by a covered entity for these purposes, to strike an appropriate balance between the individual's privacy interests and the public interest need for this information.

In an electronic health information exchange environment, a covered entity's disclosures of PHI to or through a HIO likely will be limited to only certain discrete purposes, such as in the case of HIO-X, for primarily treatment purposes. Many of the other purposes for which the Privacy Rule permits a covered entity to disclose PHI, such as, for example, to report suspected child abuse or to report a crime on the premises of the covered entity, by their nature may not lend themselves to an electronic health information exchange environment. Regardless of the scope of the purposes for the electronic health information exchange environment, any disclosures by a HIPAA covered entity to or through a HIO must be in accordance with the Privacy Rule. Also, as described in the Introduction, covered entities participating in a HIO must have a business associate agreement with the HIO that defines the uses and disclosures the HIO is permitted to make with PHI on a covered entity's behalf.

In addition to the Privacy Rule's use and disclosure limitations, covered entities engaging in electronic health information exchange need to be cognizant of States with more stringent privacy laws, as well as other Federal laws that may apply, which will affect the exchange of electronic health information.

FREQUENTLY ASKED QUESTIONS

Q1: **Under the HIPAA Privacy Rule, may a covered health care provider disclose electronic protected health information (PHI) through a health information organization (HIO) to another health care provider for treatment?**

A1: Yes. The Privacy Rule permits a covered entity to disclose PHI to another health care provider for treatment purposes. See 45 C.F.R. § 164.506. Further, a covered entity may use a HIO to facilitate the exchange of such information for treatment purposes, provided it has a business associate agreement with the HIO that requires the HIO to protect the information. See 45 C.F.R. §§ 164.502(e), 164.504(e).

Q2: **May a health information organization (HIO) manage a master patient index on behalf of multiple HIPAA covered entities?**

A2: Yes. A HIO may receive protected health information from multiple covered entities, and manage, as a business associate on their behalf, a master patient index for purposes of identifying and linking all information about a particular individual. Disclosures to, and use of, a HIO for such purposes is permitted as part of the participating covered entities' health care operations under the HIPAA Privacy Rule, to the extent the purpose of the master patient index is to facilitate the exchange of health information by those covered entities for purposes otherwise permitted by the Privacy Rule, such as treatment.

Q3: **What may a HIPAA covered entity's business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?**

A3: A business associate agreement may authorize a business associate to make uses and disclosures of PHI the covered entity itself is permitted by the HIPAA Privacy Rule to make. See 45 C.F.R. § 164.504(e). In addition, the Privacy Rule permits a business associate agreement to authorize a business associate (e.g., a HIO) to: (1) use and disclose PHI for the proper management and administration of the business associate, in accordance with 45 C.F.R. § 164.504(e)(4); and (2) to provide data aggregation services related to the health care operations of the covered entities for which it has agreements. In most cases, the permitted uses and disclosures established by a business associate agreement will vary based on the particular functions or services the business associate is to provide the covered entity. Similarly, a covered entity's business associate agreement with a HIO will vary depending on a number of factors, such as the electronic health information exchange purpose which the HIO is to manage, the particular functions or services the HIO is to

perform for the covered entity, and any other legal obligations a HIO may have with respect to the PHI. For example, the business associate agreements between covered entities and a HIO may authorize the HIO to:

- Manage authorized requests for, and disclosures of, PHI among participants in the network;
- Create and maintain a master patient index;
- Provide a record locater or patient matching service;
- Standardize data formats;
- Implement business rules to assist in the automation of data exchange;
- Facilitate the identification and correction of errors in health information records; and
- Aggregate data on behalf of multiple covered entities.

Q4: May a health information organization (HIO), acting as a business associate of a HIPAA covered entity, de-identify information and then use it for its own purposes?

A4: A HIO, as a business associate, may only use or disclose protected health information (PHI) as authorized by its business associate agreement with the covered entity. See 45 C.F.R. § 164.504(e). The process of de-identifying PHI constitutes a use of PHI. Thus, a HIO may only de-identify PHI it has on behalf of a covered entity to the extent that the business associate agreement authorizes the HIO to do so. However, once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or HIO for any purpose (subject to any other applicable laws).

Q5: How may the HIPAA Privacy Rule's minimum necessary standard apply to electronic health information exchange through a networked environment?

A5: The Privacy Rule generally requires covered entities to take reasonable steps to limit uses, disclosures, or requests (if the request is to another covered entity) of protected health information (PHI) to the minimum necessary to accomplish the intended purpose. However, in some cases, the Privacy Rule does not require that the minimum necessary standard be applied, such as, for example, to disclosures to or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information. For routine requests and disclosures, standard protocols may be used to apply the minimum necessary standard, and individual review of each request or disclosure is not required. For non-routine requests and disclosures, the Privacy Rule requires that criteria be developed for purposes of applying the minimum necessary standard on an individual basis to each request or disclosure. For requests for PHI by another covered entity, the disclosing covered entity may rely, if reasonable under the circumstances, on the requested disclosure as the minimum necessary. See 45 C.F.R. §§ 164.502(b), 164.514(d).

Depending on the type of request or disclosure, it may be that some or many of the requests or disclosures to or through the health information organization (HIO) by a covered entity may not be subject to the Privacy Rule's minimum necessary standard. This would be true in the case of a HIO whose primary purpose is to exchange electronic PHI between and among several hospitals, doctors, pharmacies, and other health care providers for treatment. However, even though the Privacy Rule does not require that the minimum necessary standard be applied to electronic health information exchanges for treatment purposes, the covered entities participating in the electronic networked environment and the HIO are free to apply the concepts of the minimum necessary standard to develop policies that limit the information they include and exchange, even for treatment purposes. For electronic health information exchanges by a covered entity to and through a HIO that are subject to the minimum necessary standard, such as for a payment or health care operations purpose, the Privacy Rule would require that the minimum necessary standard be applied to that exchange and that the business associate agreement limit the HIO's disclosures of, and requests for, PHI accordingly. However, as one covered entity may rely, if reasonable, on another covered entity's request as being the minimum necessary amount of PHI, the HIO's business associate agreement similarly can authorize and instruct the HIO to rely on the requests of covered entities as the minimum necessary, where appropriate, to help facilitate disclosures between covered entities.

When the minimum necessary standard is required by the Privacy Rule, or the policies of the HIO and participating covered entities, to be applied to certain exchanges of electronic health information, the application of the minimum necessary standard can be automated by the HIO for routine disclosures and requests through the use of standard protocols, business rules, and standardization of data. More complex or non-routine disclosures and requests may not lend themselves to automation, and may require individual review under the Privacy Rule, to the extent the Privacy Rule otherwise applied to the disclosure or request.

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.

Q7: **To what extent does the HIPAA Privacy Rule allow third parties to access protected health information (PHI) through a health information organization (HIO) for purposes other than treatment, payment, and health care operations?**

A7: The Privacy Rule would permit a HIO, acting as a business associate of one or more covered entities, to make any disclosure the covered entities are permitted by the Privacy Rule to make, provided the HIO's business associate agreement(s) authorizes the disclosure. See 45 C.F.R. § 164.504(e). For example, the Privacy Rule permits a covered entity to make disclosures of PHI for public health and research purposes, provided certain conditions are met. Such disclosures may be made by a HIO, on behalf of one or more covered entities, provided the covered entities or HIO satisfy all of the Privacy Rule's applicable conditions, and the business associate agreement(s) with the HIO authorize the HIO to make the disclosure.