INTRODUCTION

This guidance is composed of a series of fact sheets that clarify how the HIPAA Privacy Rule applies to, and can be used to help structure the privacy policies behind, electronic health information exchange in a networked environment. The guidance illustrates how HIPAA covered entities may utilize the Privacy Rule's established baseline of privacy protections and individual rights with respect to individually identifiable health information to elicit greater consumer confidence, trust, and participation, in electronic health information exchange.

The fact sheets that compose this guidance are intended to be companion documents to *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (the Privacy and Security Framework) and provide information regarding the Privacy Rule as it relates to the following select principles in the Privacy and Security Framework: Correction; Openness and Transparency; Individual Choice; Collection, Use, and Disclosure Limitation; Safeguards; and Accountability. This guidance is limited to addressing common questions relating to electronic health information exchange in a networked environment, and, thus, is not intended to address electronic exchanges of health information occurring within an organization. Moreover, specific questions related to electronic access by an individual to his or her protected health information (PHI) held by a HIPAA covered entity, or questions related to consumer-oriented health information technologies, such as personal health records (PHRs), are addressed in separate guidance documents issued concurrently with this guidance.

This guidance answers some of the most common and fundamental questions a HIPAA covered entity may have with respect to participating in an electronically networked environment and disclosing PHI to and through separate legal entities called Health Information Organizations (HIOs). There is no universal definition of a HIO; however, for purposes of this guidance, a HIO is "an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards," as defined in The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology.[1] In addition, because HIOs may take any number of forms and support any number of functions, for clarity and simplicity, the guidance is written with the following fictional HIO ("HIO-X") in mind:

> HIO-X facilitates the exchange of electronic PHI primarily for treatment purposes between and among several health care providers (e.g., hospitals, doctors, and pharmacies), many of which are HIPAA covered entities. For the purposes of this guidance, HIO-X is not a data repository for PHI.

[1] Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, The National Alliance for Health Information Technology Report to the Office of the National Coordinator For Health Information Technology: Defining Key Health Information Terms, Pg. 24 (2008).

THE HIPAA PRIVACY RULE AS A FOUNDATION FOR ELECTRONIC HEALTH INFORMATION EXCHANGE

The Privacy Rule applies to health plans, health care clearinghouses, and those health care providers who conduct electronically certain financial and administrative transactions that are subject to the transactions standards adopted by HHS. See 45 C.F.R. § 160.103 (definition of "covered entity"). The Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and by setting limits and conditions on the uses and disclosures that may be made of such information. The Privacy Rule also gives individuals certain rights with respect to their health information.

The Privacy Rule provides a strong foundation for developing electronic health information exchange relationships and business models. Its underlying policies and provisions reflect the careful balance between protecting the privacy of individuals' PHI and assuring that such health information is available to those who need access to it to provide health care, payment for care, and for other important purposes. The Privacy Rule's provisions also provide considerable flexibility to accommodate covered entities' utilization of HIOs and networked environments.

In that regard, the Privacy Rule expressly permits a covered entity to disclose PHI to a business associate, or allow a business associate to create or receive PHI on its behalf, so long as the covered entity obtains satisfactory assurances in the form of a contract or other agreement that the business associate will appropriately safeguard the information. See 45 C.F.R. §§ 164.502(e), 164.504(e). A business associate is a person (other than a workforce member) or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides certain services to, a covered entity. See 45 C.F.R. § 160.103 (definition of "business associate"). The Privacy Rule's business associate provisions can encompass a covered entity's utilization of a HIO to provide services or functions on its behalf. Such activities may include but are not limited to: matching individuals to their PHI across different jurisdictions (e.g., a record locator service); providing the infrastructure to exchange information among entities participating in the HIO network; and managing individuals' privacy preferences with respect to their health information in the network.

The contract between a covered entity and its business associate must establish the permitted and required uses and disclosures of PHI by the business associate but generally may not authorize the business associate to use or disclose PHI in a manner that would violate the Privacy Rule. The contract also must require the business associate to appropriately safeguard PHI, among other things. See 45 C.F.R. § 164.504(e). A business associate contract can authorize the business associate to make any number of uses and disclosures permitted under the Privacy Rule. However, the parties can, and likely would want, depending on the purposes of the network and any assurances made to individuals, to further restrict in the contract what

the HIO can do with the PHI it uses or discloses through its network. In addition, in the context of a networked environment in which multiple covered entities participate, the Privacy Rule would allow the participating covered entities to enter into a single, multi-party business associate agreement with the HIO managing the network that defines the scope of the HIO's services and functions, the uses and disclosures the HIO is permitted or required to make of health information in the network, the safeguards the HIO will implement to protect the privacy and security of PHI, as well as the other elements of a business associate contract that are required by 45 C.F.R. § 164.504(e)(2).

FREQUENTLY ASKED QUESTIONS

Q1: Is a health information organization (HIO) covered by the HIPAA Privacy Rule?

A1: Generally, no. The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and health care providers that conduct covered transactions. The functions a HIO typically performs do not make it a health plan, health care clearinghouse, or covered health care provider. Thus, a HIO is generally not a HIPAA covered entity. However, a HIO that performs certain functions or activities on behalf of, or provides certain services to, a covered entity which require access to PHI would be a business associate under the Privacy Rule. See 45 C.F.R. § 160.103 (definition of "business associate"). HIPAA covered entities must enter into contracts or other agreements with their business associates that require the business associates to safeguard and appropriately protect the privacy of protected health information. See 45 C.F.R. §§ 164.502(e), 164.504(e). (See also the relevant business associate requirements in the HIPAA Security Rule at 45 C.F.R. §§ 164.308(b), 164.314(a).) For instance, a HIO that manages the exchange of PHI through a network on behalf of multiple covered health care providers is a business associate of the covered providers, and thus, one or more business associate agreements would need to be in place between the covered providers and the HIO.

Q2: Can a health information organization (HIO) operate as a business associate of multiple covered entities participating in a networked environment?

A2: Yes. A HIO can operate as a business associate of multiple covered entities participating in a networked environment. The HIPAA Privacy Rule does not prohibit an entity from acting as a business associate of multiple covered entities and performing functions or activities that involve access to protected health information for the collective benefit of the covered entities. In addition, the Privacy Rule would not require separate business associate agreements between each of the covered entities and the business associate. Rather, the Privacy Rule would permit the covered entities participating in a networked environment and the HIO to operate under a single business associate agreement that was executed by all participating covered entities and the common business associate.

Q3: What are some considerations in developing and implementing a business associate agreement with a health information organization (HIO)?

A3: In general, the HIPAA Privacy Rule requires that the contract between a covered entity and its business associate establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate, but provides that the contract may not authorize the business associate to use or disclose PHI in a manner that would violate the Privacy Rule. In addition, the contract must require the business associate to appropriately safeguard PHI. See 45 C.F.R. § 164.504(e). See also the relevant business associate requirements of the HIPAA Security Rule at 45 C.F.R. § 164.314(a). Given these required elements of a business associate agreement, covered entities participating in a networked environment with a HIO can use the business associate agreement as a tool to help shape the specific terms and conditions of the information exchange the HIO will manage, as well as the safeguards that will be in place to ensure information is protected and only shared appropriately.

While a business associate contract technically can authorize the business associate to make any number of uses and disclosures permitted under the Privacy Rule, the parties can, and likely would want to, further restrict in the contract what the HIO can and will do with PHI. Defining the permitted uses and disclosures by the HIO may depend on a number of factors, including the purposes of the information exchange through the network (e.g., for treatment purposes), how individual preferences and choice will be honored, as applicable, and any other legal obligations on covered entities and/or HIOs with respect to the PHI in the network. For instance, if the HIO will primarily manage the exchange of PHI among participating entities for treatment purposes, then the parties should, in the business associate agreement, define the HIO's permitted uses and disclosures of PHI with those limited purposes in mind.

Q4: Can a health information organization (HIO), as a business associate, exchange protected health information (PHI) with another HIO acting as a business associate?

A4: 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 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.

Q5: Can a health information organization (HIO) participate as part of an organized health care arrangement (OHCA)?

A5: A HIO, by definition, cannot participate as part of an OHCA because the HIPAA Privacy Rule defines OHCA as an arrangement involving only health care providers or health plans, neither of which a HIO qualifies as. However, a HIO may be a business associate of an OHCA if the HIO performs functions or activities on behalf of the OHCA. See 45 C.F.R. § 160.103 (definitions of "organized health care arrangement" and "business associate"). For example, a hospital and the health care providers with staff privileges at the hospital are an OHCA for purposes of the Privacy Rule. To the extent such an arrangement uses a HIO for electronic health information exchange, the HIO would be a business associate of the OHCA.

Q6: Can a health information organization (HIO) participate as part of an affiliated covered entity?

A6: A HIO generally is not a HIPAA covered entity and the HIPAA Privacy Rule allows only certain legally separate covered entities to designate themselves as a single affiliated covered entity for purposes of complying with the Privacy Rule. Thus, a HIO generally may not participate as part of an affiliated covered entity. See 45 C.F.R. § 160.105(b) for the requirements and conditions regarding affiliated covered entities.