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. 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
Introduction

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.
**CORRECTION**

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 Correction Principle in the Privacy and Security Framework.

**CORRECTION PRINCIPLE:** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

**CORRECTION AND THE HIPAA PRIVACY RULE**

The Privacy Rule provides individuals with the right to have their protected health information (PHI) amended in a manner that is fully consistent with the Correction Principle in the Privacy and Security Framework. See 45 C.F.R. § 164.526. Both the Privacy Rule and the Correction Principle recognize that individuals have a critical stake in the accuracy of their individually identifiable health information and play an important role in ensuring the integrity of that data. Under the Privacy Rule, individuals have the right to have a covered entity amend their PHI in a designated record set, as defined in § 164.501, for as long as the entity maintains the records. The covered entity must act timely, usually within 60 days, to correct the record as requested by the individual or to notify the individual the request is denied. When a correction is made, the covered entity must make reasonable efforts to see that the corrected information is provided generally to its business associates, such as a health information organization (HIO), and others who are known to have the PHI that was amended.

A covered entity may deny a requested amendment if it determines that the information is complete and accurate, and on limited other grounds. When a request is denied, but the individual continues to dispute the accuracy of the information, the individual must be provided an opportunity to file a statement of disagreement with the covered entity and the covered entity must provide documentation of the dispute with any subsequent disclosure of the disputed PHI.
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

**Amendment and HIos**

One of the major benefits of being able to share information electronically to or through a HIO is the ability to perform a number of tasks in a more efficient and timely manner. For example, under the Privacy Rule, a covered entity has up to 60 days to act on a request for an amendment, with an additional 30 day extension in certain circumstances. The efficiencies of retrieving, verifying, and updating information in electronic form should enable covered entities to readily comply with this timeframe and, indeed, even to offer individuals a shorter timeframe for amending their medical records.

In addition, since the various requests and notifications required to effectuate an amendment or to deny a request can be done electronically, significant time can be saved in communicating and responding to requests for amendments. The following written exchanges are contemplated by the Privacy Rule: the individual’s request for an amendment, the covered entity’s notice to the individual that the amendment has been accepted or, if denied, the reasons for denial, the individual’s statement of disagreement, the covered entity’s rebuttal statement, if any, and the notification generally of others known to hold the data that is the subject of the correction. The Privacy Rule allows the covered entity and individual to agree to conduct any of these written exchanges electronically. Allowing individuals to make requests for amendment electronically, rather than using paper that must be mailed or delivered to the covered entity, and communicating the covered entity’s actions on the requests electronically to the individual should expedite the process.

Moreover, when PHI has been electronically disclosed to or through a HIO, the covered entity’s ability to notify other holders of the information can be expedited. For example, through the HIO, the covered entity should be able to identify other participants in the network that maintain information on the individual and who, therefore, should be notified of the amended information.

The Privacy Rule is flexible in how a covered entity amends the PHI, allowing the covered entity to effectuate corrections in the most efficient manner and to comply with recordkeeping requirements imposed by states or other authorities with respect to medical and other records of care. Thus, a covered entity should be able to adopt a reasonable method of amending electronic health records that will satisfy the Privacy Rule. When an amendment is denied and the individual continues to dispute the accuracy of the PHI, the Privacy Rule does require documentation of the dispute to be linked to the disputed information and for that documentation to accompany any future disclosure of the disputed information. Having all of the exchanges related to amendment in electronic form (e.g., as scanned images or electronic annotations) may facilitate compliance with these requirements when the information itself is subject to electronic disclosure to or through a HIO. However, if some or all of the documentation related to the disputed information remains in paper form, but the disclosure of the disputed information itself is done electronically, note that the covered entity still must
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

provide for a means of transmitting the non-electronic documentation to the recipient of a disclosure of the PHI and clearly linking this documentation to the disputed electronic PHI.

**Frequently Asked Questions**

**Q1: Who is responsible for amendment of protected health information in an electronic health information exchange environment?**

A1: The HIPAA Privacy Rule designates a covered entity as the responsible party for acting on an amendment request. However, a health information organization (HIO), acting as a business associate of the covered entity, may be required by its business associate contract to perform certain functions related to amendments, such as informing other participants in the HIO’s health information exchange who are known to have the individual’s information, of the amendment. See 45 C.F.R. § 164.504(e)(2)(i)(F).

**Q2: What are a covered entity’s responsibilities to notify others in a network if an amendment to protected health information is made?**

A2: Under the HIPAA Privacy Rule, a covered entity must make reasonable efforts to communicate an amendment to others in the network identified by the individual as needing the amendment, as well as generally to other parties that are known to have the information about the individual. It is also the entity’s responsibility to communicate the amendment within a reasonable timeframe. A health information organization (HIO), with the ability to track where information was exchanged in the past, or to otherwise identify where an individual’s information resides on the network, can assist the covered entity, as its business associate, in efficiently disseminating amended information to appropriate recipients throughout the electronic network.
OPENNESS AND TRANSPARENCY

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 Openness and Transparency Principle in the Privacy and Security Framework.

**OPENNESS AND TRANSPARENCY PRINCIPLE:** There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

**OPENNESS AND TRANSPARENCY AND THE HIPAA PRIVACY RULE**

As health information technologies evolve into complex systems that provide ease of access to health information and increase storage capacity and interoperability across networks, it is essential that individuals have trust in the use of these technologies that can ultimately enhance the quality of their care. Trust in evolving health information technologies can best be established with openness and transparency about the policies, procedures, and technologies that affect how individuals’ health information is used. To that end, health information organizations (HIOs) and entities that participate in HIOs should provide clear notice of their policies and procedures regarding how they use and disclose individuals’ identifiable health information and how they will protect the privacy of this information.

The Openness and Transparency Principle in the Privacy and Security Framework emphasizes the concept that trust in electronic health information exchange can best be established in an open and transparent environment. It also stresses that it is important for individuals to understand what individually identifiable health information exists about them, how that information is collected, used, and disclosed, and how reasonable choices can be exercised with respect to that information.

This guidance addresses the Privacy Rule’s notice of privacy practices (NPP) provision and how this Privacy Rule requirement may apply to, or support openness and transparency in, electronic health information exchange in a networked environment. The guidance also answers some frequently asked questions about the Privacy Rule’s NPP provision and its potential application to HIOs and the functions they perform. As explained in the Introduction, because HIOs can take many different forms and support any number of functions, for simplicity, the guidance is written with a hypothetical HIO, HIO-X, in mind. HIO-X is a separate legal entity (i.e., not part of any HIPAA covered entity) that facilitates the exchange of electronic protected health information (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. While HIO-X itself is not a HIPAA covered entity, because HIO-X performs certain functions or activities on behalf of covered entities that require access to PHI, HIO-X is a business associate under the Privacy Rule. As a result, the HIPAA covered entities participating in the networked environment with HIO-X must enter into contracts that require HIO-X to safeguard and appropriately protect the privacy of PHI.

**HIPAA Notice of Privacy Practices (NPP)**

The Privacy Rule provides individuals, with certain limited exceptions, with a right to receive a NPP, which, among other things, describes how a covered entity may use and disclose their PHI, the individuals’ rights with respect to that information, as well as the covered entity’s obligations to protect the information. The Privacy Rule generally requires that covered health care providers with direct treatment relationships with individuals provide a copy of the NPP directly to the individual on the date the first service is provided, and make a good faith effort to obtain the individual’s written acknowledgment of receipt of the NPP. In addition, the provider must post its NPP at its facility or office and have it available for any person who requests a copy. The Privacy Rule requires that a covered entity’s NPP be written in plain language. See 45 C.F.R. § 164.520.

The Privacy Rule also contains several NPP provisions that are relevant to covered entities that operate in an electronic environment. First, the Privacy Rule requires a covered entity that maintains a web site providing information about the covered entity’s services or benefits to prominently post its NPP on its web site. Further, where a health care provider delivers its first health care service to an individual electronically, such as through e-mail, or over the Internet, the provider must send an electronic NPP automatically and contemporaneously in response to the individual’s request for service. Also, in general, a covered entity is permitted to e-mail its NPP to an individual if the individual agrees to receive an electronic NPP (although the individual always retains the right to receive a paper copy of the NPP upon request). See 45 C.F.R. § 164.520(c)(3).

While HIO-X, as a business associate of the covered entities participating in the electronic health information exchange, does not itself have an obligation to provide a NPP to individuals, the Privacy Rule permits the participating covered entities to provide notice to individuals of the disclosures that will be made to and through HIO-X, as well as how individuals’ health information will be protected in a networked environment. Indeed, such notice would help facilitate the openness and transparency in electronic health information exchange that is important for building trust and thus, is encouraged. Some individuals also may find the fact that a health care provider participates in electronic health information exchange to be an important factor that could lead individuals to choose that provider over another. Covered entities could provide notice of their participation with HIO-X and the network by integrating such information into their HIPAA NPPs or by creating and providing a separate notice of this information. Also, to the extent the individual is provided with certain choices of how or if the
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

individual’s information is to be exchanged through HIO-X, notice of the disclosures a covered entity may make to and through HIO-X, as well as how the individual’s information will be protected, would be an important element of informing such choices.

FREQUENTLY ASKED QUESTIONS

Q1: May a HIPAA Notice of Privacy Practices (NPP) specifically mention that protected health information (PHI) will be disclosed to and through a health information organization (HIO)? May the NPP mention that the covered health care provider uses an electronic health record (EHR)?

A1: Yes, covered entities are permitted to include such information in their NPPs. The HIPAA Privacy Rule requires that a covered entity’s NPP describe the types of uses and disclosures of PHI a covered entity is permitted to make. The Rule also requires that a covered entity’s NPP include at least one example of the uses and disclosures the covered entity is permitted to make for treatment, payment, and health care operations purposes. See 45 C.F.R. § 164.520(b). While the Privacy Rule does not require that these examples describe the covered entity’s disclosure of PHI to and through a HIO for treatment and other purposes, or that a covered health care provider uses an EHR, the Privacy Rule does not preclude a covered entity from including in its NPP additional information concerning the covered entity’s participation in these activities. Alternatively, a covered entity may wish to provide the individual with a separate notice of the disclosures that may be made to and through a HIO, and how the individual’s health information will be protected.

Such notice that mentions that PHI will be disclosed to and through a HIO or that the covered health care provider uses an EHR would help facilitate the openness and transparency in electronic health information exchange that is important for building trust and thus, is encouraged. Some individuals also may find the fact that a health care provider participates in electronic health information exchange, or that the provider uses an EHR, to be an important factor that could lead individuals to choose that provider over another. Also, to the extent the individual is provided with certain choices of how or if the individual’s information is to be exchanged through a HIO, notice of the disclosures a covered entity may make to and through a HIO, as well as how the individual’s information will be protected, would be an important element of informing such choices.

Q2: Are health information organizations (HIOs) required to have a HIPAA Notice of Privacy Practices (NPP)?

A2: Generally, no. The HIPAA Privacy Rule’s NPP obligations extend only to HIPAA covered entities and the functions a HIO generally performs do not make it a HIPAA covered entity (i.e., a health plan, health care clearinghouse, or covered health care provider). See 45 C.F.R. § 160.103 (definition of “covered entity”). However, while a HIO does not itself have a HIPAA obligation to provide a NPP to individuals, the Privacy Rule permits covered entities that participate in
electronic health information exchange with the HIO to provide notice to individuals of the disclosures that will be made to and through the HIO and through the network, as well as how individuals’ health information will be protected by the HIO.

**Q3:** *May covered entities that operate in electronic environments provide individuals with their HIPAA Notice of Privacy Practices (NPP) electronically?*

**A3:** Yes, provided the individual agrees to receive the covered entity’s NPP electronically and such agreement has not been withdrawn (although the individual always retains the right to receive a paper copy of the NPP upon request). Further, where health care is delivered to an individual electronically, such as through e-mail, or over the Internet, the provider must send an electronic NPP automatically and contemporaneously in response to the individual’s request for service. Except in an emergency treatment situation, a covered entity that has a direct treatment relationship with an individual and who delivers an NPP electronically also must make a good faith effort to obtain a written acknowledgment of receipt, either electronically or through other means. In addition, the HIPAA Privacy Rule requires a covered entity that maintains a website providing information about the covered entity’s services or benefits to prominently post its NPP on its website. See 45 C.F.R. § 164.520(c).
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.
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,
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

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 locator 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.
SAFEGUARDS

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 Safeguards Principle in the Privacy and Security Framework.

SAFEGUARDS PRINCIPLE: Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

SAFEGUARDS AND THE HIPAA PRIVACY RULE

The Safeguards Principle in the Privacy and Security Framework emphasizes that trust in electronic health information exchange can only be achieved if reasonable administrative, technical, and physical safeguards are in place. The HIPAA Privacy Rule supports the Safeguards Principle by requiring covered entities to implement appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI). See 45 C.F.R. § 164.530(c). (See also the HIPAA Security Rule at 45 C.F.R. §§ 164.308, 164.310, and 164.312 for specific requirements related to administrative, physical, and technical safeguards for electronic PHI.)

The Privacy Rule’s safeguards standard assures the privacy of PHI by requiring covered entities to reasonably safeguard PHI from any intentional or unintentional use or disclosure in violation of the Privacy Rule. The safeguards requirement, as with all other requirements in the Privacy Rule, establishes protections for PHI in all forms: paper, electronic, and oral. Safeguards include such actions and practices as securing locations and equipment; implementing technical solutions to mitigate risks; and workforce training.

The Privacy Rule’s safeguards standard is flexible and does not prescribe any specific practices or actions that must be taken by covered entities. This allows entities of different sizes, functions, and needs to adequately protect the privacy of PHI as appropriate to their circumstances. However, since each covered entity chooses the safeguards that best meet its individual needs, the types of protections applied may not be the same across all participants exchanging electronic health information to or through a health information organization (HIO), and some participants may not be covered entities.
When covered entities and others participate in electronic health information exchange with a HIO, the actual exchange of information may be facilitated and even enhanced if all participants adopt and adhere to the same or consistent safeguard policies and procedures. To that end, the flexibility of the Privacy Rule would allow covered entities and the HIO, as their business associate, to agree on appropriate, common safeguards that would apply to their electronic exchange of information. In addition, as a requirement of participation in the electronic health information exchange with the HIO, these commonly agreed to safeguards also could be extended to other participants, even though they are not covered entities. For example, HIO participants may agree to use a common set of procedures and mechanisms to verify the credentials of and to authenticate persons requesting and accessing information through the network or to apply the same standard training for persons who utilize the network.

Common safeguards policies can be formalized through a business associate agreement, data sharing agreement, or any other contract mechanism, and may include enforcement mechanisms and penalties for breaches and violations. A HIO also may establish and centrally control the exchange network, network equipment, and exchange conduits, so that the exchange process itself is protected by a single set of safeguards and security mechanisms.

FREQUENTLY ASKED QUESTIONS

Q1: Does the HIPAA Privacy Rule permit a covered health care provider to e-mail or otherwise electronically exchange protected health information (PHI) with another provider for treatment purposes?

A1: Yes. The Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so. Thus, for example, a physician may consult with another physician by e-mail about a patient’s condition, or health care providers may electronically exchange PHI to and through a health information organization (HIO) for patient care.

Q2: How may the HIPAA Privacy Rule’s requirements for verification of identity and authority be met in an electronic health information exchange environment?

A2: The Privacy Rule requires covered entities to verify the identity and authority of a person requesting protected health information (PHI), if not known to the covered entity. See 45 C.F.R. § 164.514(h). The Privacy Rule allows for verification in most instances in either oral or written form, although verification does require written documentation when such documentation is a condition of the disclosure.

The Privacy Rule generally does not include specific or technical verification requirements and thus, can flexibly be applied to an electronic health information
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

exchange environment in a manner that best supports the needs of the exchange participants and the health information organization (HIO). For example, in an electronic health information exchange environment:

- Participants can agree by contract or otherwise to keep current and provide to the HIO a list of authorized persons so the HIO can appropriately authenticate each user of the network.
- For persons claiming to be government officials, proof of government status may be provided by having a legitimate government e-mail extension (e.g., xxx.gov).
- Documentation required for certain uses and disclosures may be provided in electronic form, such as scanned images or pdf files.
- Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.

Q3: Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

A3: Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual’s request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the
provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

**Q4:** Does the HIPAA Privacy Rule allow covered entities participating in electronic health information exchange with a health information organization (HIO) to establish a common set of safeguards?

**A4:** Yes. The Privacy Rule requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), including reasonable safeguards to protect against any intentional or unintentional use or disclosure in violation of the Privacy Rule. See 45 C.F.R. § 164.530(c). Each covered entity can evaluate its own business functions and needs, the types and amounts of PHI it collects, uses, and discloses, size, and business risks to determine adequate safeguards for its particular circumstances.

With respect to electronic health information exchange, the Privacy Rule would allow covered entities participating in an exchange with a HIO to agree on a common set of privacy safeguards that are appropriate to the risks associated with exchanging PHI to and through the HIO. In addition, as a requirement of participation in the electronic health information exchange with the HIO, these commonly agreed to safeguards also could be extended to other participants, even if they are not covered entities. A common or consistent set of standards applied to the HIO and its participants may help not only to facilitate the efficient exchange of information, but also to foster trust among both participants and individuals.
ACCOUNTABILITY

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 Accountability Principle in the Privacy and Security Framework.

ACCOUNTABILITY PRINCIPLE: The Principles in the Privacy and Security Framework should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

ACCOUNTABILITY AND THE HIPAA PRIVACY RULE
The Accountability Principle in the Privacy and Security Framework emphasizes that compliance with, and appropriate mechanisms to report and mitigate non-compliance with, the Principles are important to building trust in the electronic exchange of individually identifiable health information. The Privacy Rule provides the foundation for accountability within an electronic health information exchange environment by requiring covered entities that exchange protected health information (PHI), whether on paper or electronically, to comply with its administrative requirements and extend such obligations to their business associates. The Privacy Rule also promotes accountability by establishing mechanisms for addressing potential non-compliance with privacy standards through a covered entity’s voluntary compliance, a resolution agreement and corrective action plan, or the imposition of civil money penalties, if necessary.

Administrative Requirements
The Privacy Rule’s administrative requirements provide a management, accountability, and oversight structure for covered entities to ensure that proper safeguards and policies and procedures are in place for PHI. See 45 C.F.R. § 164.530. The Privacy Rule provides covered entities considerable flexibility, however, to develop and implement policies and procedures which are appropriate and scalable to their own environment. This flexibility allows covered entities that will be engaging in electronic health information exchange to or through a health information organization (HIO) to consider how best to comply with the Privacy Rule’s administrative standards.
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

Workforce Training and Sanctions
The Privacy Rule requires a covered entity to have written policies and procedures as necessary to implement the privacy standards in the Rule and to train workforce members on those policies and procedures, as necessary and appropriate for the workforce members to perform their functions. See 45 C.F.R. § 164.530(b). A covered entity also must have and apply appropriate sanctions for workforce members who violate the Privacy Rule or the entity’s own privacy policies and procedures. See 45 C.F.R. § 164.530(e).

Covered entities either will need to write new privacy policies and procedures or adapt their existing policies and procedures to address the changes in their business practices needed to accommodate electronic exchanges of PHI to or through a HIO. Workforce members, whose functions involve the electronic exchange of PHI to or through a HIO, including those workforce members responsible for monitoring and overseeing the entity’s participation in an electronic health information exchange, should receive training on these new or changed policies and procedures. A covered entity engaging in the electronic exchange of PHI to or through a HIO also should review and amend as necessary its policies and procedures for sanctioning workforce members who fail to comply with the entity’s privacy policies and procedures or the requirements of the Privacy Rule. As the covered entity’s privacy practices may change to accommodate electronic exchanges of information to or through a HIO, the entity’s sanction policies may likewise need to address changes in responsibility for accessing, using, and disclosing PHI, the types of noncompliance that may arise in an electronic environment, and the appropriate sanctions for such noncompliance. For example, electronic access privileges may need to be suspended or even revoked for workforce members found to be abusing such privileges.

Complaint Process
The Privacy Rule requires a covered entity to develop and implement procedures which allow individuals to make complaints about its compliance with the Privacy Rule, as well as its own privacy policies and procedures. See 45 C.F.R. § 164.530(d). Through this complaint mechanism, covered entities can learn of and address the problems and concerns of individuals with the entity’s privacy practices, including concerns or problems involving the electronic exchange of PHI to or through a HIO. The covered entity’s notice of privacy practices should inform individuals of how to file a complaint and provide appropriate contact information. See 45 C.F.R. § 164.520(b)(1)(vi)-(vii).

Mitigation
Under the Privacy Rule, at 45 C.F.R. § 164.530(f), a covered entity must mitigate, to the extent practicable, any harmful effects that are known to the covered entity and that result from a use or disclosure of PHI in violation of its own privacy policies and procedures or the Privacy Rule by the covered entity or its business associates. Thus, mitigation is required, where practicable, for known harmful effects caused by the covered entity’s own workforce misusing or disclosing electronic PHI or by such misuse or wrongful disclosure by a HIO that is a business associate.
of the covered entity. While appropriate steps to mitigate harm caused by an improper use or disclosure in an electronic environment will vary based on a totality of the circumstances, some mitigation steps to consider would be:

- Identifying the cause of the violation and amending privacy policies and technical procedures, as necessary, to assure it does not happen again;
- Contacting the network administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information;
- Notifying the individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identity theft.

**Liability for Violations of the HIPAA Privacy Rule in an Electronic Health Information Exchange Environment**

Liability for civil money penalties arising from violations of the Privacy Rule continues to rest exclusively on covered entities, even in an electronic health information exchange environment. Thus, covered entities that participate in or exchange PHI to or through a HIO are responsible for their own non-compliance with the Privacy Rule, as well as that of their workforce. HIOs that are not otherwise covered entities in their own right are not directly liable for noncompliance with the Privacy Rule. However, where a business associate agreement exists between a covered entity and a HIO for the electronic exchange of PHI, the HIO will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by the business associate, and if unable to do so, to terminate the business associate relationship. Pursuant to its business associate agreement, the business associate is required to extend these contractual provisions to its agents or subcontractors, as well. See 45 C.F.R. §§ 164.502(e), 164.504(e). See also the parallel business associate requirements in the HIPAA Security Rule at 45 C.F.R. § 164.314(a).

**Accountability and the Business Associate Agreement**

The Privacy Rule requires business associate agreements to contain satisfactory assurances that a business associate will adequately safeguard PHI. Some of the satisfactory assurances by a HIO acting as a business associate would include, for example, that:

- the HIO will not use or disclose PHI except as allowed by the agreement;
- the HIO will implement reasonable and appropriate safeguards for PHI; and
- the HIO will report any uses or disclosures of PHI that violate the agreement to the covered entity.
The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

Although the Privacy Rule requires business associates to self-report to the covered entity uses and disclosures of PHI that constitute a material breach or violation of the agreement, the covered entity may want to consider other means and methods to monitor the activities of the HIO and its compliance with its business associate obligations. Where, through the business associate self-reports or based on other substantial and credible evidence, the covered entity becomes aware of a pattern or practice by the HIO in material breach or violation of the agreement, the covered entity must attempt to cure the breach or end the violation by the HIO. If such attempts are unsuccessful, the Privacy Rule would require the covered entity to terminate its agreement with the HIO. In the event termination is not feasible, the covered entity must report the HIO’s violation(s) to the Secretary of HHS through OCR.

Frequently Asked Questions

Q1: What is a covered entity’s liability under the HIPAA Privacy Rule for sharing data inappropriately to or through a health information organization (HIO) or other electronic health information exchange network?

A1: A covered entity that exchanges protected health information (PHI) to or through a HIO or otherwise participates in electronic health information exchange is responsible for its own non-compliance with the Privacy Rule, and for violations by its workforce. A covered entity is not directly liable for a violation of the Privacy Rule by a HIO acting as its business associate, if an appropriate business associate agreement is in place. Nor can a HIO as a business associate be held liable for civil money penalties arising from violations of the Privacy Rule. Rather, where a business associate agreement exists between a covered entity and a HIO for the electronic exchange of PHI, the HIO will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by the business associate, and if unable to do so, to terminate the business associate relationship. See 45 C.F.R. §§ 164.502(e), 164.504(e). Furthermore, a covered entity is not liable for a disclosure that is based on the non-compliance of another entity within the health information exchange, as long as the covered entity has complied with the Privacy Rule.

Q2: Does the HIPAA Privacy Rule require a covered entity to “police” a health information organization (HIO), which functions as its business associate?

A2: No. As with other business associates, the Privacy Rule would require that a covered entity enter into a relationship with a HIO in a way which anticipates and reasonably safeguards against the potential for inappropriate uses and disclosures, specifically through the use of a business associate agreement. The Privacy Rule also would require the covered entity to respond appropriately to complaints and evidence of violations, but it would not
otherwise require the covered entity to actively monitor or oversee the extent to which a HIO, acting as its business associate, abides by the privacy provisions of the agreement, or the means by which the HIO carries out its privacy safeguard obligations. See 45 C.F.R. §§ 164.502(e), 164.504(e).

Q3: **How should a covered entity respond to any HIPAA Privacy Rule violation of a health information organization (HIO) acting as its business associate?**

A3: The Privacy Rule establishes a series of steps a covered entity should take in response to any complaints or other evidence it receives that a HIO has violated its business associate agreement, which include the following:
- investigation of any complaint received, as well as of other information containing credible evidence of a violation;
- reasonable steps to cure/end any material breaches or violations it becomes aware of;
- termination of the agreement where attempts to cure a material breach are unsuccessful; and
- in the event termination of the agreement is not feasible, the report of violation(s) to the Secretary of HHS, through OCR. See 45 C.F.R. § 164.504(e).

Q4: **Who is liable under the HIPAA Privacy Rule where multiple covered entities have signed on to a single business associate agreement and one member breaches the agreement?**

A4: The Privacy Rule is flexible enough to allow multiple covered entities to exchange information with each other in an electronically networked environment upon entering into a single, multi-party business associate agreement. Regardless of the number of signatories, the obligations in a multi-party business associate agreement will be largely bi-directional. Covered entities will still be accountable for the actions of their workforce, as well as the contents and enforcement of its business associate agreement with the health information organization (HIO). See 45 C.F.R. §§ 164.530(b),(e) and 164.504(e). Covered entities will not be liable, however, for the violations of other participants in the HIO’s health information exchange.