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

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).