PERSONAL HEALTH RECORDS AND THE HIPAA PRIVACY RULE

INTRODUCTION

A personal health record (PHR) is an emerging health information technology that individuals can use to engage in their own health care to improve the quality and efficiency of that care. In this rapidly developing market, there are several types of PHRs available to individuals with varying functionalities. Some PHRs are offered by health care providers and health plans covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, known as HIPAA covered entities. The HIPAA Privacy Rule applies to these PHRs and protects the privacy of the information in them. Alternatively, some PHRs are not offered by HIPAA covered entities, and, in these cases, it is the privacy policies of the PHR vendor as well as any other applicable laws, which will govern how information in the PHR is protected. This document describes how the Privacy Rule may apply to and supports the use of PHRs.

What is a PHR?

There is currently no universal definition of a PHR, although several relatively similar definitions exist within the industry. In general, a PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care. A PHR should not be confused with an electronic health record (EHR). An EHR is held and maintained by a health care provider and may contain all the information that once existed in a patient's paper medical record, but in electronic form.

PHRs universally focus on providing individuals with the ability to manage their health information and to control, to varying extents, who can access that health information. A PHR has the potential to provide individuals with a way to create a longitudinal health history and may include common information such as medical diagnoses, medications, and test results. Most PHRs also provide individuals with the capability to control who can access the health information in the PHR, and because PHRs are electronic and generally accessible over the Internet, individuals have the flexibility to view their health information at any time and from any computer at any location. The accessibility of health information in a PHR may facilitate appropriate and improved treatment for conditions or emergencies that occur away from an individual's usual health care provider. Additionally, the ability to access one's own health information in a PHR may assist individuals in identifying potential errors or mistakes in their information.

Depending on the type of PHR, individuals also may be able to input family histories and emergency contact information, to track and chart their own health information and the health information of their children or others whose care they manage, to schedule and receive reminders about upcoming appointments or procedures, to research medical conditions, to renew prescriptions, and to communicate directly with their health care providers through secure messaging systems. The PHR also may function as a way for both individuals and health care providers to streamline the administrative processes involved in transferring patient records or for coordinating patient care.

Types of PHRs

The PHR market continues to evolve at a rapid pace, with new types of PHRs continually emerging. For the purposes of this document, however, the universe of PHRs can be broken down into two categories: those subject to the Privacy Rule and those that fall outside of its scope. PHRs that are subject to the Privacy Rule are those that a covered health care provider or health plan offers. Examples of PHRs that fall outside the scope of the Privacy Rule are those offered by an employer (separate from the employer's group health plan) or those made available directly to an individual by a PHR vendor that is not a HIPAA covered entity. Some stand-alone software packages or portable devices also may be available for use by individuals as PHRs. However, while third parties may provide individuals with information to upload into these tools, since they are solely in the custody of the individual and are not offered by or connected to a third party, they will not be addressed in this document.

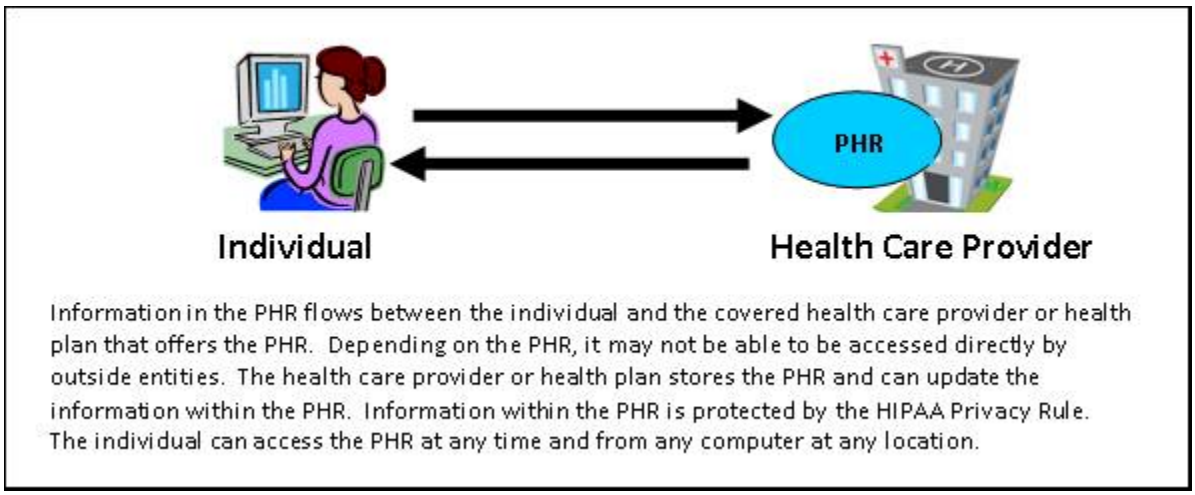
PHRs Offered by HIPAA Covered Entities

PHRs offered by HIPAA covered entities, such as health care providers or health plans, generally link individuals to, and allow them to view, some or all of the health records maintained about them within the covered entity. In many cases, an individual may not be given access to the entirety of his or her health record held by the health care provider or health plan and may only have the ability to view and not update or edit the information that is assembled by the health care provider or health plan. These PHRs also may allow individuals to add their own information into their PHRs and to update or edit this self-entered information. Many PHRs will include notations as to the sources of information in the PHR, whether it be self-entered by the individual or entered by the health care provider or health plan. The individual may be able to control who else has access to the information in the PHR, such as, for example, a spouse, family member, or another health care provider.

A PHR offered by a health care provider or health plan may not be a comprehensive record of the individual's health care, because it may not be automatically updated with information from all health care providers that treat the individual or health plans that cover the individual. However, in many cases, individuals can request copies of their health information from other health care providers or health plans and can update their PHRs with this information to ensure that their PHRs are up-to-date and as comprehensive as possible. Alternatively, if the

functionality exists, individuals may authorize other health care providers or health plans to update the individual's information into the individual's PHR directly. In addition, a PHR offered by a covered entity may not be portable, so individuals may not be able to take their PHR with them when they switch health care providers or health plans. In these cases, as above, individuals who want comprehensive records may have to retrieve information from their prior PHR or directly from their health care provider or health plan and input the information directly into any new PHR.

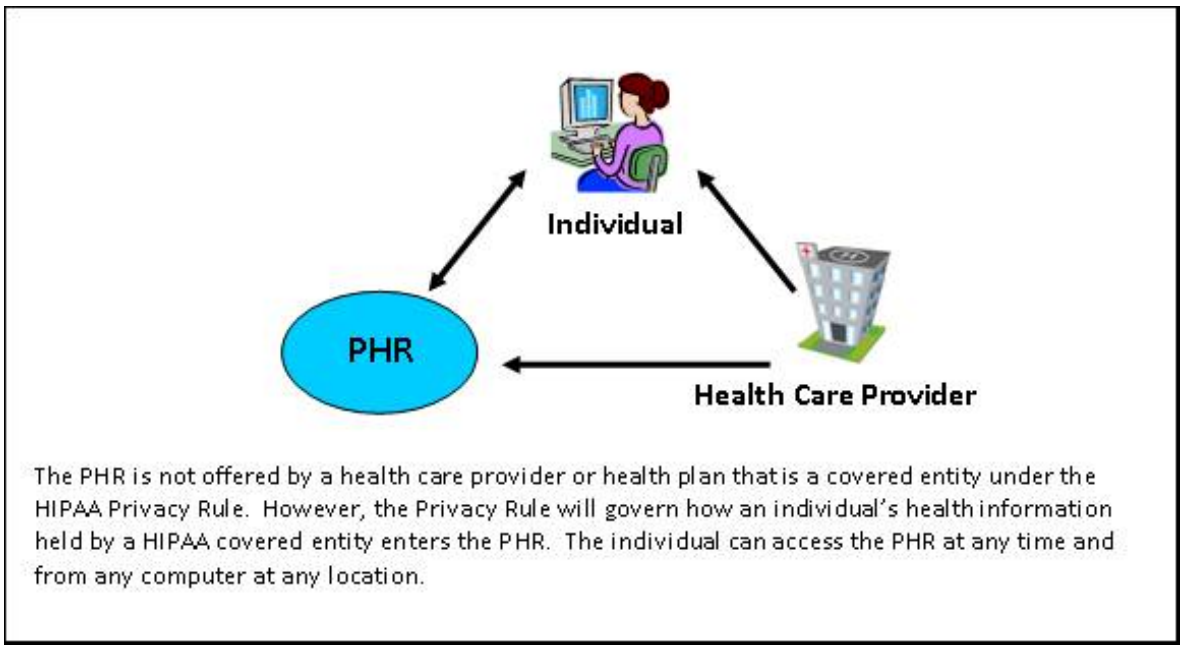
Image 1: Information flow for PHRs offered by covered entities



PHRs Not Offered by HIPAA Covered Entities

The Privacy Rule does not apply to PHRs that are not offered by health plans or health care providers that are covered by the Privacy Rule. For example, PHRs may be offered by employers (separate from the employer's group health plan) or by PHR vendors directly to individuals. These types of PHRs are governed by the privacy policies of the entity that offers them, and in certain cases, may be governed by laws other than the Privacy Rule. However, the Privacy Rule still regulates how an individual's health information held by a HIPAA covered entity enters the PHR.

Image 2: Information flow for PHRs not offered by covered entities



THE HIPAA PRIVACY RULE'S APPLICATION TO PHRS OFFERED BY COVERED ENTITIES

The Privacy Rule protects the privacy of certain individually identifiable health information, known as protected health information (PHI), created or maintained by covered entities. Covered entities include health plans and those health care providers that transmit any health information in electronic form in connection with certain standard transactions, such as health care claims. See 45 C.F.R. § 160.103. The Privacy Rule governs how these covered entities may use and disclose an individual's PHI and grants individuals certain rights regarding their health information. PHRs that are offered by a covered entity will contain PHI and thus, the covered entity must appropriately safeguard this information as required by the Privacy Rule.

Business Associates

Covered entities offering a PHR may hire another entity as a business associate to administer the PHR or perform other PHR-related services or functions. The Privacy Rule allows a covered entity to use a business associate to perform functions or activities on behalf of, or provide services to, the covered entity that involve the use or disclosure of PHI, provided the covered entity obtains satisfactory assurances, through a contract or agreement, that the business associate will appropriately safeguard the information. See 45 C.F.R. §§ 164.502(e), 164.504(e). A business associate agreement must specify, among other things, the business associate's permitted uses and disclosures of PHI and that the business associate will appropriately safeguard the information. See 45 C.F.R. § 164.504(e). The business associate

may not use or disclose the information for any purpose that would violate the Privacy Rule. The agreement may specify the manner in which the individual will control access to the information in the PHR, including whether, and the circumstances under which, the business associate is to allow third parties and even the covered entity access to the information.

The Use and Disclosure of Protected Health Information

Covered entities may not use or disclose an individual's PHI except as the Privacy Rule expressly permits or requires, or with an individual's written authorization. See 45 C.F.R. §§ 164.502, 164.508. The Privacy Rule's use and disclosure provisions were designed with the typical business or clinical health care record in mind, whether paper or electronic, and the uses and disclosures covered entities would need to make of this information for their core health care functions. Thus, the Privacy Rule generally allows covered entities to use and disclose an individual's PHI for treatment, payment of health care, and health care operations (certain functions that support treatment and payment). See 45 C.F.R. § 164.506. Also, in recognition that there are certain legitimate and important additional uses of an individual's health information, the Privacy Rule allows a covered entity to disclose, subject to conditions, an individual's PHI for certain other purposes, such as research and public health. See 45 C.F.R. §§ 164.510, 164.512, 164.514(e).

With respect to offering and maintaining a PHR, a covered entity is generally permitted by the Privacy Rule to use and disclose an individual's PHI for purposes of providing this service to the individual, as well as communicating with the individual through the use of a PHR. With respect to PHI within the PHR, a covered entity offering a PHR may establish privacy policies that restrict its uses and disclosures of such information beyond what is required by the Privacy Rule. Because the fundamental purpose of a PHR is to give individuals more control over, and access to, their health information, covered entities are encouraged to reassess what uses and disclosures of individuals' information in the PHR may be appropriate, and to give individuals greater control over the information in their PHRs. This may include, for example, allowing an individual to control not only access to the information in the PHR by third parties, but even by the covered entity itself. However, covered entities should be aware of the circumstances in which they may need to access or disclose information within an individual's PHR to comply with other legal obligations, and should make these circumstances clear to the individual.

Individual Rights

The Privacy Rule grants individuals several rights with respect to their own health information, such as the right to view and obtain a copy of much of their health information and to have corrections made to such information. See, for example, 45 C.F.R. §§ 164.524, 164.526. Because PHRs provide individuals with access to their health information and can facilitate communication between individuals and their health care providers or health plans, PHRs may be useful mechanisms for covered entities to facilitate providing individuals with their HIPAA rights.

Access

The Privacy Rule gives individuals a right of access to inspect and obtain a copy of their PHI in a designated record set held by a covered entity. See 45 C.F.R. § 164.524. A designated record set is the medical records, billing records, enrollment and claims records, and other information used by the covered entity to make decisions about the individual. See 45 C.F.R. § 164.501 (definition of "designated record set"). A PHR offered by a HIPAA covered entity may allow individuals to view all or part of their PHI held by a covered entity and to download and print this information. Thus, depending on the breadth and usefulness of the information to which the individual has access, a PHR could eliminate or reduce the need for individuals to otherwise request access to their complete designated record set held by the HIPAA covered entity. However, access to health information through a PHR would not replace an individual's right to obtain access to health information in his or her designated record set that is not available through the PHR and to which he or she is entitled under the Privacy Rule. Thus, covered entities providing the individual with access to only a portion of the individual's health information in a designated record set through a PHR should make clear the individual's right to obtain access to the information in the designated record set that is not available through the PHR. Also, individuals always retain the right to a paper copy of the individual's health information in the designated record set held by the covered entity. In addition, the Privacy Rule requires a covered entity to have a mechanism to provide an individual's personal representatives with access to the individual's PHI and, as with access provided to the individual, a PHR may be a way to eliminate or reduce the need for personal representatives to otherwise request access to the complete designated record set about the individual. Additionally, covered entities are not precluded from setting up a PHR system that allows individuals to designate family members or other persons to have access to the information in their PHRs.

Amendment

The Privacy Rule gives individuals the right to have amendments or corrections made to the PHI in their health records or other designated record set held by a covered entity. See 45 C.F.R. § 164.526. PHRs that replicate some or all of the information in the health record may be helpful mechanisms for individuals to identify potential errors in their health information and to request that the covered entity correct the information. If there is a mistake, the covered entity can correct or append additional information to the individual's health information held in the covered entity's health records system and can update the PHR with the corrected information. The individual control inherent in PHRs also may allow individuals to revise and update some information, such as that information they themselves have entered in their PHRs.

Notice of Privacy Practices

The Privacy Rule requires covered entities to provide individuals with a notice of privacy practices (NPP) outlining individuals' rights with respect to their health information and how the covered entity may use and disclose this information. See 45 C.F.R. § 164.520. The PHR may be a useful mechanism for a covered entity to distribute its HIPAA NPP, in addition to the other distribution methods required by the Privacy Rule. Also, a covered entity that offers a PHR to individuals is encouraged to consider highlighting its privacy practices with respect to the PHR explicitly in its HIPAA NPP, particularly to the extent such practices provide greater restrictions on the use and disclosure of health information compared to the covered entity's policies generally with respect to PHI. Alternatively, covered entities may consider creating a separate and more detailed NPP specific to PHRs that outlines the privacy practices and highlights the extent to which individuals can control information in their PHRs. Making available to individuals specific information about the privacy protections and controls over information in a PHR may build trust in, and help promote use of, PHRs by individuals.

Accounting of Disclosures

The Privacy Rule gives individuals the right to receive an accounting of certain disclosures of their PHI made by a covered entity for the six years prior to the request for the accounting, so that individuals are aware of how their information has been shared. See 45 C.F.R. § 164.528. However, because disclosures from the PHR will generally be to the individual or for limited other purposes, such as for administering the PHR, disclosures of information from a PHR generally would not be subject to the HIPAA accounting requirement. However, consistent with the intent of the accounting for disclosures, covered entities may want to consider setting up a functionality within a PHR that provides individuals with the ability to view a log of who accessed their PHR.

PHRs Not Offered By HIPAA Covered Entities

In contrast to the PHRs discussed above, some PHRs fall outside the scope of the Privacy Rule because they are not offered by covered entities. For example, PHRs may be offered by employers (separate from the employer's group health plan) or by PHR vendors directly to individuals. Although some of these PHRs may advertise that they are "HIPAA-compliant," the Privacy Rule does not apply to or protect the health information within these PHRs. These PHRs are governed by the privacy policies and practices of the entities offering or administering the PHRs, as well as by any other applicable laws. When selecting a PHR, individuals should evaluate these privacy policies to decide if they are comfortable with the protections and rights offered, such as how their information will be safeguarded, for what purposes their information will be used and disclosed, and the extent to which the individual will control access to information in the PHR. Additionally, in some cases, an entity offering a PHR may share an individual's health information with contractors or other business partners.

Individuals may wish to evaluate whether these contractors or business partners also will be limited in how they can use or disclose the individual's health information.

Although the information in these PHRs is not covered by the Privacy Rule, the Privacy Rule does govern how PHI held by a covered entity enters a PHR. There are a number of ways in which a covered entity may disclose PHI about an individual for purposes of populating a third party PHR consistent with the Privacy Rule.

Authorization

The Privacy Rule permits a covered entity to disclose an individual's PHI to a third party with the individual's written authorization. See 45 C.F.R. § 164.508. Thus, in cases where the entity offering the PHR is able to or has agreed to input information directly into the PHR for the individual, a covered entity is permitted to disclose PHI about the individual directly to the entity administering the PHR if the covered entity has a written authorization from the individual for the disclosure.

The Privacy Rule specifies the required elements of the authorization, including that it describe the information to be disclosed, identify the recipients of the information, be signed by the individual, and include an expiration date or expiration event. See 45 C.F.R. § 164.508(c). However, the Privacy Rule does not require that a HIPAA authorization be drafted or distributed by the covered entity, and a PHR vendor, for example, could create a HIPAA compliant authorization form that the individual could use to authorize his or her health care providers or health plans to disclose PHI directly to the PHR vendor. HIPAA authorizations also may be executed on paper or electronically, provided any electronic signature obtained from the individual complies with applicable law.

Disclosure to the Individual

The Privacy Rule also permits a covered entity to disclose PHI about an individual to the individual. See 45 C.F.R. § 164.502(a)(1)(i). The individual may grant the covered entity authority to upload information about the individual directly into the individual's PHR. Alternatively, a covered entity may provide this information directly to the individual for the individual to enter into the PHR.

Individual's Right of Access

In addition to covered entities being permitted to disclose an individual's PHI to the individual, individuals also have a right under the Privacy Rule to obtain a copy of their PHI in a designated record set, such as a medical or billing record, maintained by the covered entity. A covered entity generally must provide the individual with access to the information to which the individual is entitled within 30 days of the request. In addition, the covered entity must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format. See 45 C.F.R. § 164.524. Thus, covered

entities are required to provide the individual with a copy of the PHI in the electronic form requested by the individual if such form is readily producible by the covered entity. Here, as above, a covered entity may provide the PHI directly to the individual for the individual to enter into the PHR or, if the functionality exists, and where the individual has granted the covered entity authority to upload information directly to the PHR, the covered entity can comply with the access request by entering the information directly into the PHR rather than giving the individual a separate paper or electronic copy.

CONCLUSION

PHRs are a mechanism for individuals to engage in their own health care by being able to access and control their health information potentially at any time and from any computer at any location. The Privacy Rule applies directly to some PHRs and in other cases, will govern the flow of PHI from a covered entity into a PHR. In either situation, the Privacy Rule supports individuals' use of PHRs as a mechanism to facilitate access to, and control over, their health information. Additionally, the use of PHRs can ensure that health care providers and health plans provide an individual with access to the individual's health information, so that this information can be used by the individual in his or her PHR.