JANUARY 2011

MEMBER BRIEFING

HEALTH INFORMATION AND TECHNOLOGY PRACTICE GROUP

Personal Health Records: History, Evolution, and the Implications of ARRA

PHR Series #1

Robert L. Coffield, JD*
Flaherty Sensabaugh & Bonasso PLLC
Charleston, WV

Jonathan Ishee, JD, MPH, MS, LLM
University of Texas Health Science Center at Houston
Northwest Diagnostic Clinic PA
Houston, TX

Jeffrey L. Kapp, JD
Jones Day
Cleveland, OH

Kevin D. Lyles, JD
Jones Day
Columbus, OH

Rebecca L. Williams, RN, JD
Davis Wright Tremaine LLP
Seattle, WA

Introduction

Computerized personal health records (PHRs) have existed for more than a decade. But it was not until late 2007 when large technology companies such as Microsoft and Google began to offer PHR products. That initial development was followed in 2008 by the formation of Dossia, a consortium of large employers created to offer PHRs to their employees. A number of other PHR vendors have recently introduced new PHR products to the market to connect consumers with their healthcare information. Recognizing this market activity, Congress for the first time addressed privacy and security requirements for PHRs in the American Recovery and Reinvestment Act of

2009 (ARRA) under Title XIII, Health Information Technology for Economic and Clinical Health Act (HITECH Act).

The efforts by these large technology companies and other "Health 2.0" technology companies likely will play a vital role in shaping the health information technology (HIT) landscape. Although it is too early to predict how PHRs will evolve and what their role will be in the new era of healthcare reform, health lawyers need to understand the spectrum of legal issues associated with PHRs and consider how a consumer-focused PHR revolution might impact their health industry clients.

A convergence of factors is causing a fundamental shift away from the paper-based, provider-centric manner in which health information has historically been stored and exchanged. Innovations in health information management technology are altering the way that patients, healthcare providers, and payors maintain, use, control, and disclose health information. Through such technology, the current decentralized system in which records are maintained by multiple providers and entities at multiple locations—often with conflicting and duplicative information—is being transformed into a centralized record maintenance system that may rely on personal health information (PHI) networks (PHINs), where the PHR serves as the central repository for health information shared through a system of developing regional or national health information exchanges (HIEs).

This transformation in the way information is maintained, stored, and exchanged empowers the patient using a PHR as a consumer of healthcare by offering a new level of control and responsibility over his or her care. It also directly impacts the patient-provider relationship. Vince Kuraitis of the e-CareManagement Blog calls this change a "transformation from Industrial Age medicine to Information Age health care."[1] We have watched the e-transformation of other industries—such as banking and commerce—over the last ten years, and the time appears ripe, if not overdue, for such transformation of the healthcare industry.

[1] Vince Kuraitis, E-CareManagement Blog, Birth Announcement: the Personal Health Information Network, March 8, 2008, http://e-caremanagement.com/birth-announcement-the-personal-health-information-network-phin/.

The traditional model for maintaining medical records, in which the provider of care stores, maintains, and updates the record, is based upon the need to provide the patient with continuity of care. The medical record reflects the plan for patient care, documents the care provided to the patient, and records communications among providers. Health lawyers know that the medical record also assists in protecting the legal rights and interests of both patients and providers.

In the twenty-first century, our healthcare system simultaneously has become more fragmented and specialized on one hand, and more coordinated and holistic on the other. Patients have become more mobile and now seek services from a variety of providers engaging in numerous specialties. These same patients change providers on a regular basis and take advantage of new models of care, like urgent care services, to complement traditional primary care services. The increasingly mobile population has caused breakdowns in continuity of care. As individuals move from city to city and state to state, they leave behind a trail of partial medical records—some on paper, some electronic—with various providers, insurers, and others.

The increasing popularity of electronic medical records (EMRs), electronic health records (EHRs), regional health information organizations (RHIOs), and health information organizations (HIOs) signals a need to address the increasing complexity of maintaining and sharing these different types and silos of health information. PHRs may be the disruptive technology that provides a simple alternative to ongoing efforts to create an interconnected network of interoperable health information systems with detailed querying functions capable of making accessible, in one place, the health information and continuity of care record for individual patients. In contrast, PHRs may travel with patients and provide a central location for information regarding patients' individualized needs.

PHRs Defined

An April 2008 report issued by the Office of the National Coordinator for Health Information Technology (ONC) defined a PHR as "an electronic record of health related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared

and controlled by the individual."[2] The report was intended to create a common understanding of health technology terms, including PHRs.

The report notes that the impetus behind PHRs is the growing importance of individuals' interest and participation in their own healthcare and wellness activities. By enabling and encouraging individuals to become more engaged in their healthcare and providing the means to document, track, and evaluate their health conditions, a PHR can lead to more informed healthcare decisions, improved health status, and ultimately reduced costs and improved quality of treatment.

The July 2006 joint position statement on PHRs issued by the American Health Information Management Association (AHIMA) and the American Medical Informatics Association defines the PHR as "a tool for collecting, tracking and sharing important, up-to-date information about an individual's health or the health of someone in their care."[3] By providing a single, detailed, and comprehensive profile of a person's health status and healthcare activity, a PHR allows an individual to become an active partner in his or her healthcare treatment. A PHR helps a person prepare for appointments, facilitates care in emergency situations, and assists in tracking health changes.

As discussed further below, the HITECH Act provides additional insight into the nature and functioning of a PHR, defining it as "an electronic record of PHR identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[4]

Although related, PHRs can be distinguished from EMRs and EHRs. A key distinction is that a PHR typically is under the patient's control, so that an individual patient is the ultimate guardian and editor of information stored or accessible within his or her PHR. The PHR is more comprehensive than a medical record and contains any information relevant to an individual's health, including diet and exercise logs, a list of over-the-counter medications, and a core set of personal information. As patients take increasing

---

[2] The report defines key health information technology terms in an effort to create a common understanding of such concepts. National Alliance for Health Information Technology, Defining Key Health Information Technology Terms, April 2008, www.hhs.gov/healthit/documents/m20080603/10.1_bell_files/textonly/index.html.

[3] The Value of Personal Health Records, A Joint Position Statement for Consumers of Health Care, American Health Information Management Association and American Medical Informatics Association, February 2007, https://www.amia.org/files/ahima-amiaphrstatement.pdf.

[4] HITECH Act, § 13400(11).

responsibility for and control of their own health status and information, it will be critical to determine (and develop standards and policies that address) how individuals can delete and/or modify PHR information that originated from another source, such as an EHR, and how such modifications will be communicated to other providers who treat the patient in the future. Portability is another key component and distinguishing characteristic of the PHR.

A PHR's goal is to be a life-long source of pertinent and relevant health information for an individual. The PHR becomes a vehicle for patients to understand their own health information and move from being passive recipients to active participants in their own personal health management.

History of PHRs

PHR 1.0

According to Wikipedia, the earliest article indexed in PubMed mentioning PHRs was published in June 1978. Most articles written about PHRs have been published since 2000. In the November 2001 report, "Strategy for Building the National Health Information Infrastructure," the National Committee on Vital & Health Statistics (NCVHS) mentions PHRs and the growing consumer use of Internet-based health information services.[5] This initial report was followed by a February 2006 report in which NCVHS recommended developing a framework for characterizing PHRs and further recommended that the Secretary of the U.S. Department of Health and Human Services develop privacy best practices for PHRs.[6]

In January 2005, AHIMA formed a workgroup to examine the role of PHRs in relation to EHRs. The pace of interest in PHRs continued to increase, and in February 2006, NCVHS issued a report and recommendations on "Personal Health Records and Personal Health Record Systems."[7]

---

[5] Report and Recommendations From the National Committee on Vital and Health Statistics, Information for Health, A Strategy for Building the National Health Information Infrastructure, November 15, 2001, http://aspe.hhs.gov/sp/NHII/Documents/NHIIReport2001/default.htm.

[6] NCVHS, *Privacy Report to the Secretary: Recommendations on Privacy and Confidentiality*, 2006-2008, http://ncvhs.hhs.gov/privacyreport0608.pdf.

[7] A Report and Recommendations from the National Committee on Vital and Health Statistics, Personal Health Records and Personal Health Record Systems, February 2006, www.ncvhs.hhs.gov/0602nhiirpt.pdf.

In April 2006, the AARP Public Policy Institute issued a report examining twenty-four PHRs available to consumers in November 2005.[8] Of the twenty-four PHRs examined, one-half of them had been introduced into the market in 2004 or 2005, with the oldest dating back to 1999.

Over the past ten years, PHRs have been used in a rudimentary fashion as a way for individuals to track their own specific healthcare information, conditions, and services provided. "First generation" PHRs can be categorized as either stand-alone PHRs, which require patients to gather and enter their own information, or tethered PHRs, which are provided by a health plan, provider, or employer sponsor that populates the PHR with information. The growth of tethered PHRs has been slow both because patients sometimes lack trust that the sponsor is acting in the patient's best interests and because sponsors often do not have access to all of a patient's health records.

PHR 2.0

The past few years have marked a new era of innovative PHR activity: Call it a second generation of PHRs, or PHR 2.0. The advancement has been led by the entrance of large technology companies into the PHR marketplace, including Google with Google Health and Microsoft with HealthVault, and the establishment of employer-led PHR initiatives such as Dossia. PHR 2.0 is not merely a data collection application, but rather a platform for the electronic aggregation and storage of health information, as well as the foundation for various applications. From this platform, the PHR can be coupled with alerts, reminders, and disease management and decision-support tools that can empower individuals to improve and manage their health. This second generation of PHRs may lead to the creation of one or more PHINs, which in turn may complement, supplement, or challenge the current efforts in developing a nationwide health information network (NHIN).[9]

The continuing movement from paper to electronic medical records storage, along with additional PHR 2.0 companies entering the healthcare marketplace, likely will spur

[8] AARP Public Policy Institute, Personal Health Records: An Overview of What Is Available to the Public, April 2006, www.aarp.org/health/doctors-hospitals/info-05-2006/2006_11_phr.html.
[9] Vince Kuraitis, E-CareManagement blog, Birth Announcement: The Personal Health Information Network, March 8, 2008, http://e-caremanagement.com/birth-announcement-the-personal-health-information-network-phin/.

larger-scale consumer adoption of PHRs. Should consumers and the federal government (through HITECH Act initiatives) embrace PHRs, the result may be the arrival of a more organized, patient-centric, and coordinated source of clinical health and wellness information, accompanied by improvements in the level of clinical and health decision-making and collaboration with providers.

The PHR 2.0 model, in which all records are managed and maintained by the patient, inverts the current provider-based model of health information management. Instead of the provider seeking authorization from the patient to release medical information and furnishing access to and/or copies of the record, the patient controls his or her medical information and allows others to access it. Centering the control of health records around the patient, rather than around the provider, raises some interesting issues for health lawyers. For example, what becomes part of the official medical record when a provider receives a PHR containing 800 pages of a patient's medical history? What is the provider's duty to review this data?

National Initiatives

At the federal level, ONC also is focusing on patient-centered healthcare. Released in June 2008, the ONC-Coordinated Federal Health Information Technology Strategic Plan: 2008-2012 serves as the guide to coordinate the government's HIT efforts to achieve nationwide implementation of an interoperable HIE system.[10] One critical goal is to create "patient-focused healthcare" by promoting the deployment of EHRs, PHRs, and other consumer HIT tools. ONC developed one such tool, the Draft PHR Model Privacy Notice & Facts-at-a-Glance, which proposes to develop a model PHR fact sheet that enables consumers to clearly understand and compare privacy policies across PHRs. The information would be presented in a simple-to-understand format similar to a nutrition label. While use of this notice would be voluntary, the proposal signals ONC's acknowledgment of the importance of consumer tools and empowerment in widespread HIT adoption and implementation.[11]

---

[10] ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012, June 3, 2008, www.hhs.gov/healthit/resources/reports.html.

[11] ONC Draft Model Personal Health Record (PHR) Privacy Notice & Facts-At-A-Glance, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848091_0_0_18/PHR_NoticeBlankTemplate.pdf.

Are Consumers Ready for PHRs?

A May 2008 Markle Foundation public opinion survey looked at the current public understanding of the privacy considerations and potential of PHRs.[12] The study indicates that the public has a high interest in using PHRs: almost half of those surveyed (46.5%) said they would be interested in using an online PHR service. However, the survey also found that utilization of PHRs remains very low—only 2.7% indicated that they use electronic PHRs. More than 57% of adults do not keep any form of PHR, while the remaining 40% keep some paper health records. Of those who said they were not interested in using a PHR, 56.8% mentioned concerns over privacy and security as the reason for their reluctance.

This study demonstrates that the public appears to see value in PHRs. Seventy-nine percent of those polled said they believed using an online PHR provides major benefits in managing their health and healthcare services.

Social Networking and Health 2.0

Transformation to a PHR-based health information system will be fueled by the intensifying interest in web-based social networking and the Health 2.0 movement. The increasing adoption of social networking and lightweight web-based tools among the general public indicates increasing comfort with sharing personal information online, which should lead to an increased willingness to utilize PHRs. Health consumers drive demand, and the healthcare industry should not underestimate the desire for robust, yet user-friendly PHRs. Various technology companies are positioning themselves to create the "killer PHR application" that will become the default standard for the industry and the personal portal for patients' involvement in and control over PHI.

The definition of the Health 2.0 movement is still being refined.[13] Jane Sarasohn-Kahn of THINK-health defines Health 2.0 as "the use of social software and its ability to promote collaboration between patients, their caregivers, medical professionals and

---

[12] Markle Foundation, Survey: Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve Their Health, June 2008, www.connectingforhealth.org/resources/ResearchBrief-200806.pdf.

[13] Health 2.0 Wiki, http://health20.org/wiki/Main_Page, a wiki set up as a service to the community of visionaries, entrepreneurs, intrapreneurs, policy makers, and professionals who are working on fundamentally redefining the healthcare industry along the lines of "Web 2.0."

other stakeholders in health."[14] Early use of the Internet for healthcare was limited to the distribution of and search for healthcare information. Yesterday's read-only World Wide Web has been transformed into today's World "Live" Web, where user-generated content is being created by businesses, professionals, and ordinary people at lightning speed through social media tools such as blogs, wikis, collaborative websites, and a variety of web-based products.

Online health social networking and software as a service (SaaS) models harness the power of networking and collective intelligence to generate a new level of collective knowledge. Whether through patient networking and management of chronic conditions,[15] global physician exchange of clinical information and insight,[16] human powered health service searching,[17] online consulting,[18] or increased transparency through tools for organizing, managing, and comparing healthcare paperwork,[19]—the Health 2.0 movement is creating innovative business models and becoming a catalyst for improving the efficiency, quality, and safety of healthcare.

---

[14] California Healthcare Foundation, The Wisdom of Patients: Health Care Meets Online Social Media, Jane Sarasohn-Kahn, M.A., H.H.S.A., THINK-Health, April 2008, www.chcf.org/publications/2008/04/the-wisdom-of-patients-health-care-meets-online-social-media.

[15] At www.patientslikeme.com, patients mutually share progress, track outcomes, and collectively discover the best answer to questions as a community. Currently, the site has communities for patients with ALS, MS, Parkinson's, and HIV. *See also,* http://tudiabetes.org, an online community for diabetics; http://dailystrength.org, a collection of online support groups focused on more than 500 specific personal challenge categories; www.sugarstats.com, blood sugar management for diabetics including tracking, monitoring and sharing blood sugar levels and key statistics; www.revolutionhealth.com, a consumer-centric health portal with a variety of health and social networking tools.

[16] *See, e.g.,* Sermo, a site for physicians to aggregate observations from their daily practice and then rapidly and in large numbers challenge or corroborate others' opinions, accelerating the emergence of trends and new insights on medications, devices, and treatments, www.sermo.com/.

[17] Organized Wisdom, A human-powered, physician guided search service for health information using wisdom cards centered around health topic areas and live connection with physicians and health professionals to seek advice and information, http://organizedwisdom.com.

[18] American Well, an online healthcare marketplace for providers to make themselves available to consumers online and by phone consultation to gain immediate, live access to physicians in multiple specialties without leaving their homes or scheduling an appointment, www.americanwell.com.

[19] change:healthcare, a technology firm dedicated to promoting transparency in the healthcare industry and helping individuals become more informed healthcare consumers through the use of Internet-based solutions and online tools for organizing and managing healthcare paperwork, http://company.changehealthcare.com/; Quicken Health, an online tool that lets patients manage out-of-pocket spending, find and fix medical billing errors and maintain a medical history in one location. http://quickenhealth.intuit.com/.

PHRs and the Use of Cloud Computing

The rise in popularity of PHRs also can be linked to the explosion of cloud computing and the ease of use this technology provides. The flood of services, applications, and data hosted in the "cloud" has the potential to complicate issues surrounding privacy, security, and data ownership of health information.

Traditionally, consumer software applications and data resided locally on a user's computer or on a central data server (using client-server architecture). This allowed the user to exercise some control over the use, storage, and destruction of data. In cloud computing, users utilize services without knowledge of or control over the technology infrastructure that supports the particular service or application at issue. This allows application providers to reduce the costs of providing a particular application by storing the data in server farms throughout the world, in countries with varying levels of baseline privacy and data ownership protection. Thus, users of a cloud-based PHR application may have little to no privacy protection for health information stored in the application apart from the protections provided in the user agreement.

The Common Framework for Networked PHI

In 2008, the Markle Foundation announced the Common Framework for Networked Personal Health Information (Framework),[20] which has been endorsed by a collaborative group of providers, health insurers, consumer groups, and privacy groups. The Framework outlines a set of practices to encourage appropriate handling of PHI as it flows to and from PHRs and similar applications or services. The objective of the Framework is to enable consumers to compile electronic copies of their PHI and to promote respect for consumers' personal preferences as to how their health information may be collected and shared.

The Framework uses the term "consumer access services," which it defines as an emerging set of services designed to help individuals make secure connections with health data sources in an electronic environment. These services may be offered to consumers by a variety of organizations, ranging from existing healthcare entities (e.g., providers, payors, self-insured employers) to new entrants to the health sector

[20] Markle Foundation, Connecting for Health, Connecting Consumers Common Framework for Networked Personal Health Information, June 2008, www.connectingforhealth.org/phti/.

(e.g., technology companies, employer coalitions, affinity groups, health record banks, etc.). Consumer access services are likely to include functions such as authentication, as well as data hosting and management. The Framework also evaluates the application of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule to consumer access services.[21]

The Framework could serve as a good starting point from which those offering consumer access services could develop a recommended industry standard for vendors offering PHR related services. PHRs currently exist in an uncertain regulatory environment because of the evolving interplay of a variety of state and federal laws emerging to address twenty-first century healthcare delivery and technology issues. Before the recent HITECH Act provisions that apply to PHR vendors, there was no federal or state legislation directly regulating the direct-to-consumer PHR sector. The Framework suggests certain core principles to form best business practices in areas including consumer consent for uses and disclosures, notice, privacy, security, chain of trust agreements, authentication, dispute resolution, and enforcement. The Framework's ultimate goal is to encourage proper handling of individual health information and to create and sustain public confidence in those offering consumer access services. As the Markle survey results indicated, such confidence currently does not exist; this must be addressed in order for PHR adoption to escalate.

Ownership of Health Information

The shift from a provider-based and -controlled medical record to a patient-controlled PHR raises traditional property law issues. As health information becomes increasingly networked and technology permits health information to be transferred more easily, the lines demarcating ownership of health information become further blurred.

Health information is often viewed under the traditional notion of property as a "bundle of rights," including the right to use, dispose, and exclude others from using. This application of historic property law may not be well suited to the information age, in which patient information is shared through a variety of formats, copied, duplicated,

[21] Markle Foundation, Connecting for Health, Connecting Consumers Common Framework for Networked Personal Health Information, CP1: Policy Overview, June 2008, www.connectingforhealth.org/phti/reports/cp1.html.

merged, and combined with other patient records into large-scale databases of highly valuable information.

Who owns health information? The physician? The insurer? The patient? Under the traditional theory, providers own the medical records they maintain, subject to the patient's rights of access to the information contained in the record.[22] This tradition stems from the era of paper records, where physical control meant control and ownership. As noted above, however, provider ownership of the record is not absolute; HIPAA and most state laws provide patients with some right to access and receive a copy of their records.[23] Patients have received other health information property rights, including the right to request corrections to their medical information and the assurance that such records are maintained confidentially.

Implications of the HITECH Act for PHRs

The HITECH Act, enacted as part of ARRA (also known as the "economic stimulus package"), provides funding, loans, incentives, disincentives, and education to promote the electronic sharing of health information. With this increased momentum toward electronic HIE come concerns about the privacy and security of HIE, particularly in the hands of entities not directly regulated by the administrative simplification provisions of HIPAA.

Under HIPAA, only those PHR vendors that provide PHRs on behalf of covered entities are deemed business associates subject to HIPAA, including the business associate contract requirements. Vendors of PHRs that only deal directly with consumers have been entirely unregulated under HIPAA. This includes most PHR vendors, because the bulk of them tend not to be associated with healthcare providers, health plans, healthcare clearinghouses, or sponsors of Medicare prescription drug cards, thus avoiding offering a service for or on behalf of a covered entity. In its efforts to address concerns of privacy advocates, Congress, in the HITECH Act, imposed breach notification requirements on PHR vendors and required the Federal Trade Commission (FTC) to issue the Health Breach Notification Rule, which became effective on

[22] Alcantara, Oscar L. and Waller, Adelle, Ownership of Health Information in the Information Age, originally published in Journal of the AHIMA, March 30, 1998, www.goldbergkohn.com/news-publications-57.html.
[23] 45 C.F.R § 164.524.

September 24, 2009 with a full compliance date of February 22, 2010.[24] The FTC Rule applies to all PHR vendors not subject to the new breach notification rules under HIPAA, either as a covered entity or business associate.

Definitions

Under the FTC's Health Breach Notification Rule, a "personal health record" means "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[25] "PHR identifiable health information" is broadly defined as individually identifiable health information, relying on the HIPAA definition,[26] and "includes, with respect to an individual, information . . . that is provided by or on behalf of the individual" and "that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[27]

Breach Notification Requirements

Overview

The Health Breach Notification Rule imposes breach notification requirements on PHR vendors and "PHR related entities."[28] On balance, however, PHR vendors and PHRrelated entities avoided some of the more onerous privacy and security requirements imposed on business associates by the HITECH Act.

---

[24] The Health Breach Notification Rule is found at 16 CFR Part 318.
[25] 16 CFR Part 318, § 318.2(d).
[26] *See* Section 1171(6) of the Social Security Act, 42 USC § 1320d(6), and 45 CFR § 160.103. Individually identifiable health information is a subset of health information, including demographic information collected from an individual, that: is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual. It is interesting to note that the HITECH Act steered away from using the terminology "protected health information" as a basis for "PHR identifiable health information." One wonders if incorporating the concept of individually identifiable health information into PHR identifiable health information overly narrows the definition and requires the involvement of healthcare providers, health plans, employers, or healthcare clearinghouses.
[27] 16 CFR Part 318, § 318.2(e).
[28] A PHR related entity is defined as: an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) offers products or services through the website of a vendor of PHRs; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; and (3) accesses information in a PHR or sends information to a PHR. 16 CFR Part 318, § 318.2(f).

The Health Breach Notification Rule requires each vendor of PHRs, and each PHR related entity, following the discovery of a breach of security involving unsecured PHR identifiable health information in a PHR maintained or offered by such vendor, to provide notice to the FTC and to any U.S. citizen or resident whose unsecured health information is acquired by an unauthorized person as a result of the breach.

Moreover, a third-party service provider that provides services to either a PHR vendor or a PHR related entity in connection with offering or maintaining PHRs (or related products or services) and that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information must notify the PHR vendor (or the PHR related entity) of a breach of such information, which notice shall include identification of each affected individual."[29]

Unlike many state breach notification laws, the new federal law's notification requirements are not limited to breaches of the security of online or electronic information. Nor are they restricted to financially sensitive information, such as Social Security number, bank account information, or the like. Therefore, these notification requirements will constitute additional obligations for PHR vendors and others covered by the Health Breach Notification Rule, even in states with existing breach notification laws.

Timing of Notice

The Health Breach Notification Rule generally requires that breach notices be sent without unreasonable delay, and in no case later than sixty calendar days after discovery. For purposes of notification, a breach is "discovered" on the first day on which such breach is known to the covered entity or PHR related entity—or reasonably should have been known. The clock starts running as soon as anyone (other than the person committing the breach) in the organization knows or should have known about the breach. Entities providing notification have the burden of demonstrating that all required notifications were made, including evidence demonstrating the necessity of any delay in notification. Accordingly, such entities should take care to document the process and rationale for providing notification under the Health Breach Notification

[29] 16 CFR Part 318, § 318.3(b).

Rule. Although sixty days is the outside time limit, PHR vendors and PHR related entities should be able to justify their rationale for utilizing the entire sixty days.[30]

Manner of Notice

Notices to affected individuals generally must be sent by first class mail. They may be sent by electronic mail if the individual has expressed a preference for it after he or she has been given an opportunity to receive notification by first class mail and has not exercised that choice—or, in an emergency, by telephone (although this does not obviate the need for written notice). Further, if ten or more individuals require notification for which there is insufficient or out-of-date contact information, then the notifying entity is required to either place a conspicuous posting on its website homepage for a period of ninety days, *or* place a notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice by media or web posting must include a toll-free phone number where an individual can learn whether his or her information may have been included in the breach.

Contents of Notice

All notices must contain:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured PHI involved in the breach.
- The steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the entity involved is doing to investigate the breach, mitigate losses, and protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

[30] HITECH Act, § 13407(c), which references HITECH Act, §§ 13402 (c), (d), (e), and (f), creating substantially similar notification requirements for vendors of PHRs and covered entities. Third-party service providers to PHRs and business associates also have similar notification provisions.

If the breach involves 500 or more residents of a state (or jurisdiction), the PHR vendor or PHR related entity also must provide notice to prominent media outlets serving the area. Further, a PHR vendor or PHR related entity must notify FTC as soon as possible and not later than ten business days after discovery of the breach if the breach involves 500 or more individuals. If the breach involves fewer than 500 individuals, the PHR vendor or PHR related entity may maintain a log of any such breach and submit the log annually to FTC.

Violations of the notification requirements related to PHR identifiable health information will be treated as unfair and deceptive acts or practices under the Federal Trade Commission Act.[31]

The PHR vendor provisions are billed as "temporary," with a sunset provision if Congress enacts new legislation establishing breach notification requirements for PHR vendors and PHR related entities.[32]

Report to Congress on Non-Covered Entities

The HITECH Act also requires the U.S. Department of Health & Human Services (HHS), in consultation with FTC, to submit a report that includes recommendations on privacy and security requirements for entities not currently covered by HIPAA. This report requirement is notable, as it acknowledges the future importance of PHRs in medical care and the lack of adequate privacy and protections currently mandated.

Specifically, the report will focus on requirements relating to security, privacy, and notification in the case of a breach of security or privacy that should be applied to:

- PHR vendors;
- Entities that offer products or services through the website of a PHR vendor;
- Entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals PHRs;
- Entities that are not covered entities and that access information in a PHR or send information to a PHR; and

[31] 16 CFR Part 318, § 318.7.
[32] 16 CFR Part 318, § 318.9.

- Third-party service providers used by an entity listed above to assist in providing PHR products or services;

The report also will recommend the federal agency that is best equipped to enforce such requirements and a timeframe for implementing the regulations based on the report's findings.[33] ONC has been tasked with developing the report, which will be developed and written by a contractor.

Conclusion

PHRs bring a new dimension to the debate over how to create an interoperable health information network. The shift of authority into the hands of patients and consumers could bring about a sustainable model of HIE that bypasses the current concerns about streamlining the patchwork quilt of consent laws among the various states. The increased interest by industry and government in health information systems anchored by PHRs will introduce and highlight legal issues that health lawyers must recognize, understand, and advise clients about. Over the coming years, federal legislation will spur a variety of new federal regulations that will impact how these systems are implemented.

**Bob Coffield is member of Flaherty Sensabaugh & Bonasso PLLC in Charleston, WV. Bob is also a co-chair of the Privacy and Security Compliance and Enforcement Affinity Group, a part of AHLA's Health Information and Technology Practice Group.*

Jeff Kapp is a partner at Jones Day in Cleveland, OH.

Kevin Lyles is a partner and co-chair of the healthcare practice at Jones Day. He resides in its Columbus, OH office. Kevin is also a co-chair of the Electronic Health Records Affinity Group, a part of AHLA's Health Information and Technology Practice Group.

Jonathan Ishee, JD, MPH, MS, LLM is general counsel of Northwest Diagnostic Clinic PA and Access Health Providers in Houston, TX. He is also an Assistant Professor at the University of Texas–Health Science Center at Houston, School of Biomedical Informatics.

Rebecca L. Williams, RN, JD is a partner at Davis Wright Tremaine LLP in Seattle, WA. Rebecca is also a vice chair of AHLA's Health Information and Technology Practice Group.

[33] HITECH Act, § 13424(b).