



**BNA's**

# HEALTH LAW REPORTER



Reproduced with permission from BNA's Health Law Reporter, Vol. 17, No. 16, 04/17/2008. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## Health Information

### Electronic and Personal Health Records: The Risks and Benefits for Providers

By LINDA A. MALEK  
AND JAY D. MEISEL

In December 2007, the Bush Administration announced that physicians must adopt electronic record-keeping to avoid an already mandated 10 percent pay cut from the Centers for Medicare and Medicaid Services in 2008. While Congress ultimately prevented the pay cut from going through, this statement by the administration is a sure sign that electronic health records' (EHRs), and their counterparts, personal health records' (PHRs), time has come. Yet health care providers have been slow to adopt EHRs because of unfamiliarity with a new and costly system. Increasingly stringent privacy and security laws which regulate the use and exchange of personal electronic data also should be a cause of concern for providers, as a failure to comply with such laws when implementing an EHR system would subject providers to the possibility of significant liability. Also, the growing use of PHRs initi-

*Linda A. Malek is chair of the health care practice at Moses & Singer LLP, New York. She can be reached at (212) 554-7814 or [lmalek@mosessinger.com](mailto:lmalek@mosessinger.com). Jay D. Meisel is an associate in the firm's health care practice and he can be reached at (212) 554-7823 or [jmeisel@mosessinger.com](mailto:jmeisel@mosessinger.com).*

ated by patients will impact doctors, both administratively and from the standpoint of liability, as they almost certainly will be asked by patients to provide medical data for updates to such records.

This article will explore two opposing trends affecting health care record-keeping practices today: the increasing adoption of EHRs by providers and PHRs by consumers juxtaposed with a movement toward stronger and more comprehensive state and federal privacy and security regulations. It also will offer recommendations as to how providers should proceed with adopting EHRs and interfacing with PHRs while complying with such privacy and security laws and regulations.

While EHRs can be described in a variety of ways, for the purposes of this article they are conventionally defined as clinical patient health records in electronic format that are originated, managed, and maintained principally by health care providers. They may include, for example, information about a patient such as medical history, lifestyle, demographics, any prescription medication, test results, and billing information, and in some instances, they are made accessible to patients. EHRs are, for the most part, limited in accessibility to a particular provider. PHRs are clinical patient health records in electronic form that are originated and managed by patients themselves, but are maintained by an outside vendor such as an HMO member site, Microsoft's Health Vault, or Google. They are accessed principally by the patient, but in some formats can be accessed by providers and/or insurers depending on

what level of access the patient provides to health care entities.

### Advantages of EHRs.

The use of EHRs offers significant advantages to providers, as they may reduce medical errors and costs, as well as increase physician efficiency. Clarity is one advantage. For example, reading a physician's handwriting becomes a nonissue, and therefore the use of EHRs negates the risk of pharmacists misreading a prescription or subsequent providers struggling to decipher records of earlier treatment. Another advantage is that EHRs are searchable, making it easier for a provider to assess possible drug interactions or for a consistent pattern of symptoms. For public health purposes, EHRs may help in detecting patterns of disease outbreaks. Perhaps the most important advantage is that, unlike paper records, EHRs can be made readily accessible to providers throughout the world. PHRs would have advantages similar to those of EHRs if a patient grants his or her providers full access to records.

Implementation of EHRs in the United States has been slow. In late 2006, approximately 11 percent of hospitals had a fully implemented EHR system, according to a survey conducted by the American Hospital Association.<sup>1</sup> A study by the Healthcare Financial Management Association in 2006 found that hospitals "had a long road ahead to adoption of electronic health records."<sup>2</sup> In that study, hospitals cited lack of national information standards and code sets, lack of funding, concern about physician usage, lack of interoperability and concerns about privacy as obstacles to EHR adoption. Physician practices also lag in implementation of EHRs. Less than 30 percent of office-based physicians reported using EHR systems in a recent study by the National Center for Health Statistics, and only 12.4 percent used comprehensive EHR systems.<sup>3</sup> However, the use of EHR systems by office-based physicians has increased over 50 percent in the past five years.<sup>4</sup> Physicians cite similar obstacles as do hospitals to EHR adoption.

However, two recent initiatives by public entities may help to speed EHR implementation. At the end of February 2008, New York Mayor Michael Bloomberg announced that the city was ready to equip 1,000 Medicaid providers with an EHR system by the end of 2008. The goal of this initiative would be for the system to cover 1 million patients. The initiative offers a subsidized software package to eligible primary care practices (those where Medicaid and uninsured patients make up more than 30 percent of the practice). City officials have stated that the system will give current health information to physicians through a series of alerts, like overdue dates on prescriptions or cholesterol checks, and also will make certain data available to physicians and provide best practices information. Also at the end of February, the state of Tennessee and AT&T jointly launched a statewide health information

exchange. The effort will allow electronic prescribing and the exchange of health information on a secure network and will be essentially a provider-to-provider network. Under a state grant program, providers would be able to apply for reimbursement of the costs of equipment, software and services required to connect to the network.

### New Products.

Microsoft, Google, and a variety of HMOs are developing products to facilitate the use of PHRs, which could accelerate PHR adoption dramatically. The cornerstone of their approaches would be to give much more control to individuals, making patients the stewards of their own information, and would make such information readily accessible via the Internet. Microsoft's "Health Vault" system is targeted at consumers and offers a personal health record and Internet searches tailored for health queries. The personal health information contained within Health Vault is stored in a secure, encrypted database and privacy controls are set by the individual. The hope behind Health Vault and similar systems is that patients will coordinate with providers. However, PHR systems may prove to be unpopular among providers, as providers would, to an extent, relinquish control over a patient's records and therefore face uncertainty about the accuracy and privacy of such records. Without such control, providers should be concerned about the comprehensiveness of a given patient's records, which will necessarily mean that they may not be getting the complete picture about a patient's health. Granting providers higher levels of access to PHRs so as to facilitate any updates to a patient's records would ameliorate this problem, but it would not guarantee accuracy. A significant danger posed by PHRs is that a physician could make a diagnosis based on data in an inaccurate PHR with the potential of committing a serious medical error and malpractice.

Despite the increased pressure from federal, state, and local government to adopt EHR platforms and the expanding development of consumer-friendly PHRs, EHR and PHR implementation and usage should be approached cautiously. Protection of patient privacy should be the first consideration when deciding to adopt an EHR platform or interface with a PHR platform. According to at least one estimate, roughly 150 people have access to at least part of a patient's records during a hospital stay and it is estimated that 600,000 payers, providers, and clearinghouses have some access to an individual's health records.<sup>5</sup> With such a large number of persons *authorized* to view a particular EHR, it is easy to see how, somewhere within the chain of authorization, an unauthorized person could gain access to a record. The Health Insurance Portability and Accountability Act's (HIPAA) Privacy and Security Rules and other federal and state privacy and security laws, such as security breach statutes, sanction providers when a patient's health information is leaked—regardless of who leaks the information. Thus, the promise of accessibility of EHRs (and PHRs) is a double-edged sword—while providers can easily locate and share patient data for quicker and more accurate

<sup>1</sup> American Hospital Association. "Continued Progress: Hospital Use of Information Technology" (2007) at 3.

<sup>2</sup> Health Financial Management Association. "Overcoming Barriers to Electronic Health Record Adoption" (2006) at 2.

<sup>3</sup> National Center for Health Statistics. "Electronic Medical Record Use by Office-Based Physicians: United States 2005" at <http://www.cdc.gov/nchs/products/pubs/pubd/hestats/electronic/electronic.htm>.

<sup>4</sup> *Id.*

<sup>5</sup> Foreman, Judy. *At Risk of Exposure*, Los Angeles Times June 26, 2006 at <http://www.latimes.com/features/health/medicine/la-he-privacy26jun26,1,3180537.column>.

treatment, the more accessible a patient's record becomes, the greater the potential that this record may fall into the wrong hands.

HIPAA aims to promote the free flow of health information needed for high quality health care, yet the Privacy and Security Rules promulgated as a result of HIPAA place stringent restrictions on the use of this information. The Privacy Rule establishes regulations for the use and disclosure of protected health information (PHI), i.e. any information about health status, provision of health care, or payment for health care that can be linked to an individual. It requires that, under many circumstances, the entity holding the records—a "covered entity"—obtain authorization from an individual when disclosing records to another party. It also requires that a covered entity must take remedial steps when the privacy of a person's PHI is compromised, such as imposing appropriate sanctions against employees. The Security Rule complements the Privacy Rule, as it requires covered entities to ensure the confidentiality, integrity and availability of PHI in electronic form and to protect against reasonably anticipated threats or hazards to the security of such information. It provides that entities must develop administrative, technical and physical safeguards—ranging from risk assessment to encryption of data—to keep PHI from being compromised. If PHI is compromised, the Security Rule requires that a covered entity sanction those employees who are responsible for such compromise.

### State Security Breach Notification.

State security breach notification laws are relatively new. The first such law was enacted in California in 2003 and was crucial in taking the first step to sanction companies such as the data broker ChoicePoint, which inadvertently exposed almost 145,000 persons to identity theft in February 2005. Nearly 40 states have followed California's lead since 2005, passing nearly identical statutes and thereby establishing an almost *de facto* federal security breach notification standard. These laws generally provide that any entity that conducts business in a particular state, and that owns or licenses computerized data that includes personal information, must disclose any security breach following discovery or notification of the breach in the security of the data to any resident of that state whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.

Most state security breach statutes define "personal information" as a person's name and one or more of the following: (1) Social Security number; (2) driver's license or identification card; or (3) information permitting access to a financial account. However, California amended its security breach notification statute as of Jan. 1, expanding its definition of "personal information." It now includes "medical information" and "health insurance information." "Medical information" is defined as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." "Health insurance information" is defined as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claim history, including any appeals records." Any health care entity that has clients or patients who reside in

California would be subject to these heightened requirements.

### Federal Legislation.

A variety of federal security breach notification legislation currently is being considered in Congress, such as the Identity Theft Enforcement and Restitution Act (S. 2168), which passed the Senate in November 2007 but was stalled in the House as of the date of publication of this article. Moreover, in 2007 the Office of Management and Budget required that federal agencies develop and implement a security breach notification policy and ensure the security of data by adopting policies and procedures similar to that of the HIPAA Security Rule.

Both HIPAA and security breach notification laws regulate patient information stored in EHR platforms. They place obligations on providers to maintain patient information in a highly secure format or face the consequences of disclosing to potentially thousands of individuals that their medical records have been compromised. As providers adopt EHR platforms or begin to participate in patient or HMO-driven systems, the first step they should take is to ensure that the provision of any electronic health information must be transferred and displayed in a secure and legally compliant manner. Current privacy and security laws were not necessarily developed to compliment EHRs. One could argue that they were implemented to *prevent* a more accessible display of health records, which is contrary to the purpose of an EHR system. That said, these privacy laws also should serve an important role as the use of EHRs increase, because these laws will provide a baseline level of privacy to reassure both patients and providers that compliance with existing law should, at least, in theory, protect confidential health information.

Unlike EHR systems, PHR systems, especially in the forms developed by Microsoft and Google, are not explicitly regulated under HIPAA (but PHR systems would be subject to state security breach laws). Therefore, health records created by consumers using these services would not be protected by HIPAA's privacy and security provisions. When an entity such as Google enters into an agreement with a consumer, it is not subject to the obligations of a covered entity; it would not even need to enter into a business associate agreement, which extends HIPAA protections from a covered entity to its business partners. Thus, without the protections of HIPAA extended to PHRs, consumers may be left vulnerable and could potentially shift blame in any privacy breach situation to the providers viewing their PHRs (unless comparable state law protections extended to entities like Google).

### Things to Consider.

Providers should start strategizing now about how they can best coordinate their operations in anticipation of either adopting an EHR platform or interfacing with consumers and other health care entities which use EHRs or PHRs. Therefore, providers should consider the following with respect to EHRs and PHRs:

- Given resource constraints, can the provider build an effective EHR platform for its facility? If not, does it wish to encourage patients to use a PHR platform like Health Vault or an HMO-based system? Is there a public program that facilitates EHR adoption that a provider could participate in?

- If the provider does adopt a facility-based EHR platform, it should first assess the current level of privacy and security of health records by assessing its compliance with HIPAA and any state privacy and security laws that are more stringent than HIPAA.
- If a provider finds that it is not in full compliance, it must make necessary upgrades to protect against data breaches before going live with an EHR system.
- If a provider does not wish to adopt its own EHR system, it should weigh the risks and benefits of encouraging its patients to utilize a PHR Web-based system such as Health Vault. The provider should be comfortable with uploading patient records to an accessible Web site and ensure it obtains necessary authorizations from the patient before transferring health records. The provider also

should be aware of the potential for out-of-date, incomplete, or inaccurate records from other providers to be kept on an individual's PHR account and plan accordingly for associated risks.

EHRs and PHRs potentially can revolutionize the way providers, insurers and patients interact: they may pave the way to a more accurate and rapid method of treating illness and assessing wellbeing. However, making health records centrally accessible also potentially opens up new security and privacy risks and will require providers to be even more vigilant about protecting how records are accessed and filtering who accesses them. The growing use of EHRs and PHRs is an undeniable reality in today's health industry. Providers who wish to stay current must ensure that they are prepared to effectuate the benefits that these types of data systems provide and face the challenges they present.

## MOSES & SINGER LLP

---

### **Disclaimer**

Viewing this article or contacting Moses & Singer LLP does not create an attorney-client relationship.

This article is intended as a general comment on certain recent developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This article contains timely information that may eventually be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions but that professional advice be sought in connection with any such transaction.

### **Attorney Advertising**

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.