

BLOOMBERG LAW REPORTS®

Privacy & Information

a
BLOOMBERG LAW™
publication

BLOOMBERG LAW REPORTS®—Privacy & Information is one in the comprehensive set of analytical reports from BLOOMBERG LAW™. For more information about BLOOMBERG LAW™ or the BLOOMBERG PROFESSIONAL® service, call:

In the US +1 212 617 6569

In EMEA +44 20 7330 7182

In Asia +852 2977 6407

Featured Article

The Privacy and Security Challenges of Electronic and Personal Health Records: Is Your Business Prepared?

Contributed by:

Linda A. Malek and Jay D. Meisel, Moses & Singer LLP

Every advance in healthcare information technology presents a new challenge to a patient's privacy. The recent initiatives promoting electronic health records (EHRs) and personal health records (PHRs) are no exception. While the use of these records could potentially revolutionize the way physicians treat patients and both patients and physicians manage medical data, they will also put unprecedented amounts of personal information at the fingertips of thousands of third parties. An increased number of individuals with access to health information will only increase the likelihood that, whether inadvertently or purposefully, data security will be breached. The federal Health Insurance Portability and Accountability Act (HIPAA), state health information privacy laws, and state security breach laws all aim to protect an individual's data from various incidents in which personal information may be compromised. However, the mere existence of these laws does not mean that a person's health data is necessarily safe. Scores of high profile security breaches have occurred over the past several years, including breaches resulting in unauthorized access to massive amounts of private data at pharmaceutical companies, major data brokers such as ChoicePoint, hospitals, and the Veteran's Administration. In the dawning era of EHRs and PHRs, physicians, hospitals, insurers, claims processing companies, and various information technology entities must be ready to combat threats to electronic health information. The reality is that many are unprepared.

There is a growing tension between the rapid growth in the use of EHRs and PHRs and the tightening regulation of the security of personal information. In order to effectively navigate the emerging technology and opportunities afforded by EHRs and PHRs, entities conducting business involving such records must be equipped to prevent or mitigate any threat to personal data that may occur, as we will discuss in greater detail below.

Electronic Health Records and Personal Health Records: Overview and Trends

EHRs are typically defined as clinical patient health records in electronic format that are originated, managed and maintained principally by healthcare providers. They may include 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 have many attributes; if used effectively they can reduce medical errors and costs, as well as increase efficiency. Their advantages range from eliminating confusion resulting from a physician's handwriting to enhanced searchability, making it easier for a provider to assess possible drug interactions or for a consistent pattern of symptoms. Depending on the platform, another advantage EHRs may offer is accessibility. If they can be transmitted outside of a particular entity's local information system, they have the potential to be shared with providers and other healthcare entities throughout the world.

PHRs are clinical patient health records in an electronic format that are created by patients themselves, but are maintained by an outside vendor such as an HMO member site or an information technology entity such as Microsoft 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 healthcare entities. PHRs have advantages similar to those of EHRs if a patient grants his or her providers full access to records.

Adoption of EHR platforms has been historically 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.¹ In a study by the Healthcare Financial Management Association in 2006, 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.² 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.³ However, the use of EHR systems by office-based physicians has increased over 50 percent in the past five years.⁴

A wave of recent local, state and federally-sponsored initiatives should help to increase the implementation rate of EHRs. New York State and New York City have been particularly active in encouraging expanded use of EHRs by healthcare providers. At the end of February 2008, Mayor Bloomberg announced that New York City was ready to equip 1,000 Medicaid providers with an EHR system by the end of 2008. Already more than 200 primary care doctors in New York City are using EHRs, and the city says it is on track to reach its goal of 1,000 providers serving more than a million patients by the end of the year.⁵ Furthermore, Mayor Bloomberg is collaborating with a coalition of House Democrats to help achieve the goal of linking 75 percent of the nation's health care providers through an e-record system within a decade. On the state level, New York Governor David Patterson awarded \$105 million in grants in late March 2008 to 19 community based health information technology projects to help build a

statewide EHR system.⁶ Grant recipients include Regional Health Information Organizations (RHIOs) such as the Bronx Regional Health Information Organization and Brooklyn Health Information Exchange, which facilitate the exchange of health information electronically within a specific geographic area.

Last year, a groundbreaking bill was introduced in the Senate by U.S. Senator Kennedy that, if passed into law, would “recommend specific actions to achieve a nationwide interoperable health information technology infrastructure” and “make recommendations concerning standards, implementation specifications, and certification criteria for the electronic exchange of health information for adoption by the federal government.”⁷ The “Wired for Health Care Quality Act” would also authorize the Department of Health and Human Services (HHS) to award grants to facilitate the “widespread adoption of interoperable health information technology.”⁸ Essentially, it would serve to boost implementation of EHRs throughout the U.S. using a common platform. At the time of publication, the sponsors of this legislation were hopeful that the legislation would pass by unanimous consent in the coming weeks.

Various private entities are now offering their own versions of PHR platforms. These platforms would allow consumers to manage and access their health records online. It would also give consumers the option of giving providers and insurers access to their records as well. Microsoft (through its website HealthVault), Google and a variety of HMOs are all developing such platforms, with security and privacy controls tailored to the needs of the consumer. Additionally, the Medical Banking Project, a policy group that focuses on the integration of banking technology, infrastructure and credit with healthcare administrative operations, is also conceiving of a private PHR-type platform, which it calls “consumer-directed healthcare (CDH) platforms.” CDH platforms aim to go a step further than the PHR-platforms offered by Microsoft and Google, as they would not only give a consumer control of his or her health records, but also engage the consumer more fully in the financial aspects of his or her healthcare-related activities. A CDH platform would combine information from an individual’s health plan and personal health accounts such as Health Savings Accounts (HSAs) and Flexible Spending Accounts (FSAs). The main objective of a CDH platform would be “to provide a coordinated link between the healthcare and financial services systems to offer the most comprehensive consumer-directed solution.”⁹ Such a platform would also benefit from enhanced security from the banks that help to administer CDH platforms. Banks would protect health-related information much as they presently protect financial information.

However, despite the recent surge in EHR and PHR initiatives, efforts still remain highly fragmented. The available EHR

and PHR frameworks are driven by different philosophies, potentially compete with each other, and appeal to different types of users, therefore creating different standards for privacy and security. The current lack of coordination between these various frameworks may lead to an increased risk of security breaches, as communication between multiple and possibly incompatible platforms could lead to data leaks and subsequent tampering with records by outside parties. The patchwork of state laws as well as the general lack of regulation in this area beg for federal legislation to set a uniform standard that will harmonize these efforts.

Security Breach Laws, HIPAA and Their Application to EHRs and PHRs

Because private PHRs such as those offered by Microsoft are not explicitly regulated under HIPAA, which governs the use and disclosure of an individual’s identifiable health information, health records created by consumers using these services would not be protected by HIPAA’s privacy and security provisions. HIPAA generally applies to “covered entities”, i.e. providers, health plans and clearinghouses, and breaches in the privacy and security of patient records by these entities result in significant penalties.¹⁰ However, when an entity such as Microsoft 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 protection of HIPAA, 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 Microsoft). While publicly-sponsored initiatives such as the ones in New York would be more strictly regulated (as they would be most likely subject to HIPAA indirectly through these public entities” activities as business associates of covered entities as well as other state privacy laws), questions remain about just how secure their EHR platforms are.

The Wired for Health Care Quality Act, described above, would have amended HIPAA so that “an operator of a health information electronic database” would essentially become a covered entity.¹¹ This would have resulted in entities that offer PHR platforms such as Microsoft becoming subject to HIPAA and would create a new class of businesses that would be required to adopt more stringent policies and procedures related to the privacy and security of certain health data. However, at the time of publication, an amendment authored by Senator Leahy significantly altering the privacy provisions of the bill had been accepted by Senator Kennedy in order to “ensure the privacy of individual protected health information.”¹² Senator Leahy stated in a recent press release

that the amendment would prevent “operators of personal health information databases” from giving sensitive health records “to virtually anyone under the [HIPAA] Privacy Rule.”¹³ This amendment eliminates the requirement that operators of PHR databases would be automatically covered under HIPAA. Rather, it would require that HHS submit to the Senate recommendations for privacy and security protections for PHRs, including whether it is appropriate to apply certain privacy regulations promulgated under HIPAA to PHRs and “the extent to which the implementation of separate privacy and security measures is necessary.”¹⁴

Certain covered entities dealing with EHRs and PHRs must also be prepared for heightened scrutiny of their security policies and procedures related to HIPAA. Earlier this year, the Office of E-Health Standards and Services of the Centers for Medicare and Medicaid Services (CMS) distributed a sample Interview and Document Request list for HIPAA Security Onsite Investigations and Compliance Reviews.¹⁵ This list indicates that CMS may request that a covered entity which contracts with CMS produce evidence of policies and procedures that address prevention, detection, containment and correction of security violations as well as other technical documents that address security matters.

Regardless of whether an entity operating an EHR or PHR platform is a “covered entity,” all such entities would be subject to state security breach notification laws (currently enacted in 43 states, the District of Columbia and Puerto Rico) which require disclosure to consumers of any breach in their personal data. Under most states’ laws, “personal information” includes only basic identifying information, but under the amended California security breach notification law, breaches in health insurance information and medical information¹⁶ are also covered. Therefore, any entity that has clients or patients who reside in California would be subject to these heightened requirements. The Arkansas security breach notification law also has similar requirements regarding medical information. Regardless of which state security law(s) apply to a particular entity, the increased aggregation of data in EHR and PHR platforms as a result of the initiatives described above will leave more personal data vulnerable to security breaches.

An entity that deals with medical data should be prepared to adapt its policies and procedures to the changes in California law. If the entity has a national presence, it is more than likely to have customers or patients from California. Also, because California was the first state to codify a security breach notification law, and most states followed its lead, one could expect that other states will soon follow its example of including “medical information” in the definition of “personal information.”

The challenges in complying with California’s recently enacted amendments are already apparent. Even an advisory group

affiliated with the California Office of Privacy Protection, which assists with the implementation and enforcement of the California security breach notification law, has struggled with formulating recommendations as to how best to comply with the new requirement that businesses and state agencies protect against and notify California residents of security breaches in medical information. Prior to being amended, the California breach notification law and related guidance was geared toward breaches affecting financial information. According to Joanne McNabb, Chief of the California Office of Privacy Protection, a breach of medical information is “a different kind of breach in a lot of ways The risk it poses is not the same” as a financial data breach.¹⁷ The advisory group found that there is not an obvious way to “flag” a person’s medical record in the same way a person’s financial records would be flagged in the event of a security breach. Still, the recommendations are likely to include suggestions that breach notices be as specific as possible, stating what types of records were breached. Pam Dixon, a member of the California Office of Privacy Protection advisory group, said that the amended California law “may drive the debate nationally toward a uniform system like the credit bureaus for medical information.”¹⁸

Lack of Preparedness and Increased Enforcement

While entities increasingly adopt EHR platforms and promote the use of PHRs, they may not be prepared to assume the security risks associated with these types of data systems. In a 2008 study conducted by Kroll Fraud Solutions/HIMSS Analytics to better understand the status of patient data security at hospitals, the hospitals surveyed reported an average level of preparedness to deal with a security breach of 5.88 on a one to seven ascending scale.¹⁹ Yet the same study indicated that only 56 percent of these hospitals had notified patients whose information was compromised as a result of a security breach.²⁰ 13 percent of the respondents to the survey reported that their organization had a security breach in the previous 12 months, with a patient’s name and high level patient information, such as diagnosis, most frequently compromised.²¹ Also, according to the Government Accountability Office (GAO), in 2004–2005, 47 percent of Medicare Advantage contractors, 42 percent of Medicare fee-for-service contractors, and 38 percent of TRICARE contractors reported experiencing a privacy breach.²² While hospitals and health plan contractors may have policies and procedures in place to combat security breaches, the Kroll survey and the GAO report would seem to indicate that the implementation of such policies and procedures is insufficient.

As healthcare institutions lag behind in their preparedness to deal with data security issues, HHS has stepped up its

enforcement efforts to counter noncompliance with HIPAA. In 2007, the total number of resolutions of possible Privacy Rule and Security Rule violations totaled 7,176, compared with only 4,761 resolutions in 2004. Of those resolutions, there were 2,199 investigations in 2007, compared to just 1,392 investigations in 2004.²³ HHS is clearly responding to the proliferation of data security incidents that occur with increasing frequency as more health records become digitized and thus susceptible to compromise.

The short history of enforcement of security breach notification laws on the state level has been quite robust. Unlike HIPAA, which puts the onus on a covered entity to come up with its own solution to mitigate a violation of the Privacy and Security Rules, security breach laws mandate disclosure to individuals and, in some instances, to law enforcement agencies. Companies found to have violated a notification law may face civil penalties, injunctive relief and attorney's fees and costs.

Recommendations for Implementation, Prevention and Response

Businesses that retain individuals' healthcare data, especially those that interface with EHRs and/or PHRs, should revisit their existing policies and procedures to ensure that they are not only compliant with existing federal and state law, but also to anticipate inevitable changes to the privacy and security regulations and increased enforcement activities. As individuals and healthcare providers become more comfortable with putting personal health information in electronic format, they will expect a heightened level of security to accompany this data. Businesses must be vigilant about protecting this data, as a security incident of any magnitude may cause substantial reputational damage. Providers, insurers, and any other businesses that possess personal health information should consider taking the following measures in order to smoothly transition to a work environment incorporating EHRs and PHRs:

- First, an entity should determine exactly what types of data it possesses (if it is a covered entity, it should inventory its protected health information). The entity should also assess whether sensitive information is encrypted and the level of accessibility of such data.
- Next, an entity should assess its vulnerability to a security breach. It should look across its organization to identify strengths and weaknesses, i.e. not only should an information technology department be prepared to deal with increases in electronic data and potential security threats, but also departments such as human resources, claims processing, and recordkeeping that view and use individuals' health information.

- An entity should review its physical, technical and administrative safeguards. It should make sure that passwords, encryption, physical locks and barriers allow only authorized personnel access to sensitive data and equipment.
- After the steps outlined above, an entity should revise its policies and procedures to reflect any new information gained and processes developed through its own assessment. For example, if the entity determines that it is inadequately prepared to respond to a security breach, it should create or revamp any related guidelines and protocols, such as, with respect to an entity handling medical information of California residents, how to notify a California resident of a breach in his or her medical information.
- An entity should periodically train new and existing employees to effectively administer electronic data and comply with rules, regulations and policies and procedures. Existing employees should be required to attend "refresher" courses on policies and procedures related to privacy and security matters.
- A business should reevaluate its contracts that include provisions regarding healthcare data and assess what types of provisions it could incorporate into its agreements regarding potential security breaches—how it will coordinate with the other party to prevent and/or notify individuals of security breaches.
- Specifically with respect to EHRs and PHRs, providers and insurers should assess whether they wish to develop their own systems, contract with an outside vendor, or try to become part of a state or federal program that facilitates the use of electronic records.
- If a provider or insurer 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 or insurer 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 or insurer should also be aware of the potential for out-of-date, incomplete or inaccurate records from other providers or insurers to be kept on an individual's PHR account and plan accordingly for associated risks.

Entities involved with all sectors of the healthcare industry should start strategizing now about how they can best

coordinate their operations in anticipation of either adopting an EHR or PHR platform or merely interacting with consumers or other entities that use EHRs or PHRs now. Understanding how privacy and security laws affect a business in connection with EHRs and PHRs is crucial, as most healthcare operations deal with patient records at some point or another and will inevitably deal with EHRs and PHRs in the future. Preparedness is key. Making sure your business is in full compliance with existing privacy and security laws and anticipating changes to relevant laws are necessary steps to effectively navigate the increasingly regulated environment of digital healthcare information.

Linda A. Malek is a partner at Moses & Singer LLP, chair of the firm's Healthcare practice group and co-chair of the firm's Privacy practice group. Jay D. Meisel is an associate in the firm's Healthcare and Privacy practice groups. Moses & Singer counsels a variety of entities in the healthcare industry and other industry sectors on matters related to privacy and security. For more information on this topic, please contact Linda A. Malek at lmalek@mosessinger.com or 212-554-7814 or Jay D. Meisel at jmeisel@mosessinger.com or 212-554-7823. For further information about Moses & Singer LLP, please visit www.mosessinger.com.

©Bloomberg 2008. Originally published by Bloomberg Finance L.P.
Reprinted by permission.

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.

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

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

³ 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>.

⁴ *Id.*

⁵ Mayor Bloomberg And Commissioner Frieden Unveil State-Of-The-Art Electronic Health Record Technology (Feb. 25, 2008) available at http://www.mikebloomberg.com/en/issues/public_health/mayor_bloomberg_and_commissioner_frieden_unveil_state_of_the_art_electronic_health_record_technology

⁶ American Medical News. "New York awards \$105 million in health IT projects" at <http://www.ama-assn.org/amednews/2008/4/28gvsc0428.htm>.

⁷ Wired for Healthcare Quality Act, S. 1693, 110th Cong. (2007).

⁸ *Id.*

⁹ Achim Welter. *An Overview of Consumer-Directed Healthcare Platforms*. The International Journal of Medical Banking. Volume 1 (2008).

¹⁰ See 45 C.F.R. § 160.103 for the definition of "Covered entity."

¹¹ S. 1693.

¹² Amendment No. __ to S. 1693.

¹³ Press Release. U.S. Senator Patrick Leahy, Leahy Announces Agreement On Privacy Provisions In Health IT Bill (May 14, 2008).

¹⁴ Amendment No. __ to S. 1693.

¹⁵ This document is available at: <http://www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf>.

¹⁶ Medical information may include medical history, diagnosis, policy number, subscriber number, and claims and appeals histories.

¹⁷ Laura Mahoney. *Advisory Group Struggles to Pen Guidance On California's Medical Breach Notice Law*. BNA's Privacy and Security Law Report. Volume 7 Number 18 (2008).

¹⁸ *Id.*

¹⁹ 2008 HIMSS Analytics Report: Security of Patient Data (Commissioned by Kroll Fraud Solutions), Apr. 2008, 21.

²⁰ *Id.* at 4.

²¹ *Id.* at 19.

²² Government Accountability Office, *Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE* (GAO-06-676, Sept. 2006).

²³ Department of Health and Human Services, Office of Civil Rights. *Compliance and Enforcement – Enforcement Results by Year* at <http://www.hhs.gov/ocr/privacy/enforcement/data/historicalnumbers.html>.