

The age of the electronic health record (“EHR”—managed by providers) and web-based personal health record (“PHR”—managed by consumers) is here. After a decade of mostly small-scale efforts, over the past several months the largest technology companies, state and municipal governments, national insurers and elite health care providers have all stepped up efforts to establish large scale platforms for EHRs and PHRs. This recent surge in EHR and PHR implementation will likely affect all of the various arenas of the healthcare sector. We provide a snapshot in this Client Alert of some of the major EHR and PHR initiatives happening right now and offer advice about how to assess the risks and rewards of adopting or interfacing with an EHR and PHR platforms.

In the fall of 2007, Microsoft unveiled its HealthVault program, which offers a platform for consumers to manage their personal health records on the Web. Microsoft has partnered with entities such as New York Presbyterian Hospital, the Mayo Clinic, Johnson & Johnson, and the American Heart Association to help build the program and encourage consumers to utilize the website. While consumers have ultimate control over their records via HealthVault, Microsoft hopes that consumers will permit health care providers to send their health information directly into their HealthVault record.

Google also has plans to launch a consumer-centered digital health records system later in 2008. While the details of the plan are still being worked out, it is currently testing the service with the Cleveland Clinic, and has signed deals with Quest Diagnostics, Aetna, Walgreens and Wal-Mart. Google’s aim is to encourage information exchanges between healthcare entities, but wants to have consumers keep control of their medical records.

At the end of February, Mayor Bloomberg announced that New York City was ready to equip 1000 Medicaid providers with a unified electronic medical records and practice management system by the end of 2008. The goal of this initiative would be for the system to cover one million patients, many of whom would be from the poorest and sickest neighborhoods in New York City. 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 will also make certain data available to physicians and provide best practices information.

Also at the end of February, the state of Tennessee and AT&T 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. According to AT&T, the system will link to the state Department of Health in order to provide access to the immunization and disease registry, death certificate processing and medical license renewals. Under a state grant program, providers may apply for reimbursement of the costs of equipment, software and services required to connect to the network.

All of the EHR and PHR platforms described above have the potential to revolutionize the way health information is stored and shared, making them far more easily accessible to consumers and to an array of providers. With the right coordination, EHRs and PHRs could be used in ways that could result in earlier detection and more aggressive treatment of illness and could also help to prevent medical errors that would usually result from incomplete medical information.

However, the privacy protections that these new EHR and PHR platforms offer are questionable. Because Google and Microsoft are not explicitly regulated under the Health Insurance Portability and Accountability Act (HIPAA), 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, insurers and clearinghouses, and breaches in the privacy and security of patient records by these entities result in significant penalties. However, 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). While publicly-sponsored initiatives such as the ones in Tennessee and New York City would be more strictly regulated (most likely subject to HIPAA indirectly through these public entities' activities as business associates and other state privacy laws), questions remain about just how secure their EHR and PHR platforms are.

All of these initiatives would, however, be subject to state security breach notification laws, which would require disclosure to consumers of any breach in their personal data. Under most states' laws, "personal information" only includes basic identifying information, but under the amended California security breach notification law, breaches in health insurance information and medical information are also covered. Therefore, any healthcare entity that has clients or patients who reside in California would be subject to these heightened requirements. Regardless of which state security law(s) apply to a particular healthcare 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. Healthcare entities should respond now by strengthening their security measures in anticipation of dealing with EHRs and PHRs on a daily basis.

Whether or not your business is eligible to become directly involved with the initiatives described above, all players in 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 dealing with consumers or other entities who use EHRs or PHRs now. Understanding how privacy and security law affects your 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. Making sure your business is in full compliance with these laws is an important first step.

We will continue to update you on developments with electronic health records and privacy and security laws.

Linda A. Malek

(212) 554-7814

lmalek@mosessinger.com

Jill E. Anderson

(212) 554-7836

janderson@mosessinger.com

Jay D. Meisel

(212) 554-7823

jmeisel@mosessinger.com

Samuel J. Servello

(212) 554-7872

sservello@mosessinger.com

MOSES & SINGER LLP

MOSES & SINGER LLP has served its clients skillfully and decisively since 1919. We provide cost-effective and result-focused legal services in the following primary areas:

- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate Securities and M & A
- Employment and Labor
- Entertainment, Advertising, IP and Internet/Technology
- Healthcare
- Hotel and Hospitality
- Litigation
- Matrimonial
- Private Funds
- Legal Ethics & Law Firm Practice
- Real Estate
- Tax
- Trusts and Estates and Wealth Preservation

The Chrysler Building
405 Lexington Avenue
New York, NY 10174-1299
Tel: 212.554.7800
Fax: 212.554.7700

2200 Fletcher Avenue
Fort Lee, NJ 07024
Tel: 201.363.1210
Fax: 201.363.9210
Abraham Y. Skoff, Esq.,
Managing Attorney for New Jersey

Disclaimer

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship. This is intended as a general comment on certain legal issues. 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 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. To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

Attorney Advertising

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

Copyright © 2008 Moses & Singer LLP
All Rights Reserved