State Bar of Michigan

Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

http://www.michbar.org/computer

Table of Contents

January 2010 ▪ Vol. 27, Issue 1

- Bits and Bytes from the Chair 1
- Personal Health Records May Not Be So Personal: How to Resolve the Privacy and Security Issues in Personal Health Records.....2
- Not Quite to Copyright? Your Idea May Still Be Entitled to Protection 29
- Meet a Section Member.....31
- Publicly Available Websites for IT Lawyers 32
- 2010 Edward F. Langs Writing Award ..32

Michigan IT Lawyer is published every other month. Previously published issues of the *Michigan IT Lawyer*, and its predecessor the *Michigan Computer Lawyer*, are available at http://www.michbar.org/computer/newsletters.cfm. If you have an article you would like considered for publication, send a copy to:

Brian A. Hall
Traverse Legal, PLC
810 Cottageview Drive
Suite G-20
Traverse City, Michigan 49684
e-mail: brianhall@traverselegal.com

Bits and Bytes from the Chair

By Jeremy D. Bisdorf, *Jaffe Raitt Heuer & Weiss PC*

Happy New Year!

Over the course of the past month we have been planning activities for our February 18, 2010 Section Council Meeting at Cooley Law School's new Ann Arbor campus. In addition to being able to introduce our Section to a new group of law students, we will also be hearing a presentation on "Technology Escrow – Then and Now." This presentation will show us some unique contract provisions, applications and ways to advocate on behalf of our clients on either side of a software related transaction.

Pizza will be served beginning at 5:30 p.m. and the presentation will begin at 6:00 p.m. The Section Council meeting will immediately follow the presentation.

During the Council meeting we will hear a report from Ron Nixon on the status of our Section's HB 5468 Analysis Committee. There will also be discussions on the progress of our Spring Networking Event and our 2010 ICLE Seminar/Annual Meeting.

Be sure to be there early before the law students get to all the food!

Also, please note that IT Law with be the theme for the December 2010 *Michigan Bar Journal*. If you have an interest in including an article in that issue, please contact Mark Malven at *MMalven@dykema.com*.

We are looking forward to a great 2010 and seeing you on February 18!

Jeremy D. Bisdorf

The Michigan IT Lawyer is pleased to present "Personal Health Records May Not Be So Personal: How to Resolve the Privacy and Security Issues in Personal Health Records" by David Schneider. Mr. Schneider is one of three student authors to receive a 2009 Edward F. Langs Writing Award from the State Bar of Michigan's Information Technology Law Section. The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the *Michigan IT Lawyer*, care of brianhall@traverselegal.com or michael@gallo.us.com. Enjoy!

Personal Health Records May Not Be So Personal: How to Resolve the Privacy and Security Issues in Personal Health Records

By David Schneider*

"To improve the quality of our health care while lowering its cost, we will make the immediate investments necessary to ensure that within five years, all of America's medical records are computerized. This will cut waste, eliminate red tape, and reduce the need to repeat expensive medical tests. But it just won't save billions of dollars and thousands of jobs—it will save lives by reducing the deadly but preventable medical errors that pervade our health care system."[1]

Introduction

When Susan went in for her annual mammogram, the radiologist detected an abnormal mass, but the radiologist was unable to compare this current mammogram to previous mammograms because Susan changed radiology providers when she moved to a new city.[2] The radiologist referred Susan to a general surgeon, who took a biopsy and sent the sample to a clinical laboratory. When the test revealed that Susan had a malignant tumor, Susan's general practitioner referred her to an oncologist.

Before her first appointment with the oncologist, the onus was on Susan to collect all of her previous medical records, which were scattered across multiple providers in different cities. After she collected her medical records, Susan and her oncologist decided that her treatment plan would entail a combination of radiation therapy, chemotherapy, and surgery, each requiring a separate physician. Susan assumed that they were communicating with each other to achieve the best outcome, but usually they were not. As a result, her physicians often made health care decisions with incomplete

information and ordered duplicate or unnecessary tests.

During her first week of chemotherapy, Susan had to be suddenly hospitalized when she experienced an adverse drug interaction between her chemotherapy medications and an over-the-counter drug. The hospital had no access to Susan's medical records and because she was unconscious the hospital had no means to determine what conditions she had, what medications she was taking, and whether she had any allergies.

During the periods between her physician visits, Susan felt distanced from her physicians. They were difficult to reach when she had questions and unresponsive to her often fluctuating health condition. Meanwhile, Susan's general practitioner was unable to follow-up on her progress or access her other physicians' records. Despite the obstacles she faced during her treatment, Susan successfully combated her cancer.

Susan's experience did not have to be so complicated, but she was forced to navigate a world of fragmented health care—one in which providers, consumers, and payers are constantly struggling to communicate and coordinate with each other and medical records are scattered across multiple providers.[3] Transitioning from a paper-based medical records system to one that utilizes electronic-based medical records may help close the communication gaps between providers, consumers, and payers.

Despite steps to move towards an electronic-based medical records system,[4] most providers still use paper-based medical records.[5] Some providers, in contrast, have adopted electronic medical records ("EMRs")[6] and electronic health records ("EHRs")[7] to better manage their consumers' health care data and enable information sharing between providers. The potential benefits of EMRs and EHRs are decreasing health care costs and improving the quality of health care.[8]

The downside of EMRs and EHRs, however, is that they are not designed to establish a communication link to consumers. First, consumers still lack the ability to conveniently access, centralize, and control their medical records. Second, consumers are unable to supplement EMRs or EHRs with important health information. Third, consumers are unable to harness the internet to communicate with their physicians or enhance their quality of health care. Unless consumers are empowered to become active participants in their own health care, the U.S. health care system cannot maximize the potential benefits that electronic-based medical records offer.[9]

Personal health records ("PHRs"), on the other hand, promise to truly integrate the U.S. health care system—syncing providers, consumers, and payers in one central location.[10] Unlike EMRs and EHRs, PHRs empower consumers to become active participants in their own health care because PHRs allow consumers to conveniently access, centralize, and control their medical records through a user-friendly, internet-based platform. A PHR is essentially "[a]n 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."[11] PHR system providers are the entities that provide or offer PHRs to consumers.[12]

Using the hypothetical above, Susan would have had a dramatically different health care experience if she had the opportunity to utilize PHRs. Instead of physically collecting all of her medical records, PHRs could have allowed Susan to electronically store her medical records and instantly transmit them to her oncologist. Susan's providers could have made more informed and accurate health care decisions because Susan or her providers can electronically share her medical records with each other. Because of increased inter-provider coordination, Susan and her providers could have realized that they were creating unnecessary costs because they were ordering duplicate clinical tests. In addition, Susan could have avoided a costly hospitalization because her PHR could have alerted her to the adverse drug interaction between her chemotherapy medications and over-the-counter drugs. In an emergency, Susan could have been able to designate someone the authority to give the hospital access to her medical records maintained on her PHR platform. When Susan was home feeling isolated and helpless, PHRs could have empowered Susan to communicate with her providers over the internet, consult medical information resources, make physician appointments and set reminders, and use applications to track her progress. Therefore, PHRs are capable of dramatically changing the U.S. health care system both on the individual level and the system-wide-level.

Overview of Key Issues Affecting PHRs

Although PHRs have the potential to decrease health care costs, improve health care quality, and empower consumers with convenient access to and control over their medical records, there is a tradeoff with privacy and security.[13] Because PHRs introduce a new party—the

Personal Health Records. . .

Continued from page 3

PHR system provider—into the health care equation, the privacy and security of consumer's protected health information ("PHI")[14] is exposed to an increased risk of improper use and disclosure. These risks are exacerbated by the fact that many PHR system providers are under no legal obligation to comply with minimum federal privacy and security standards that protect against the use and disclosure of an individual's PHI.[15]

Some entities, however, are under a legal obligation to comply with minimum federal privacy and security standards. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[16] mandates that any (1) health plan, (2) health care clearinghouse, and (3) health care provider who transmit any health information in electronic form—collectively called "covered entities"[17]—comply with minimum privacy and security standards.[18] HIPAA authorized the United States Department of Health and Human Services ("HHS") to promulgate the regulations that establish the minimum privacy and security standards.[19] Under this authority, HHS has promulgated the Privacy Rule,[20] the Security Rule,[21] and the Enforcement Rule[22] to prevent a covered entity from improperly using or disclosing an individual's PHI. In general, the Privacy Rule restricts the ability of covered entities to use and disclose PHI, the Security Rule requires covered entities to protect electronic PHI from disclosure, and the Enforcement Rule punishes covered entities that do not comply with the Privacy and Security Rules.[23]

The scope of HIPAA's privacy and security requirements are not universal—only "covered entities" are obligated to comply with these requirements. Some PHR system providers fall within the definition of a covered entity ("covered PHR system providers"). Most covered PHR system providers are operated or managed by covered entities, such as hospitals and insurance companies. Other PHR system providers, however, do not fall within HIPAA's definition of a covered entity ("uncovered PHR system providers").[24] Most uncovered PHR system providers are operated or managed by commercial companies that are not covered entities, such as Google or Microsoft.

Because HIPAA's privacy and security requirements apply to covered PHR system providers, but do not apply to uncovered PHR system providers, this inconsistency threatens the success of the entire PHR industry.[25] Consumers are unconvinced that PHRs will protect their PHI from improper use and disclosure.[26] Similarly, providers are uncertain whether PHR system providers can keep their patients' PHI private and secure.[27] If PHRs are underutilized by both consumers and providers, the potential benefits of PHRs will be diminished. Therefore, to foster trust in the privacy and security of PHRs and to maximize the potential benefits of PHRs, *all* PHR system providers, both covered and uncovered, should be required to comply with HIPAA's privacy and security requirements.

This Article advocates that HIPAA should be amended to require all PHR system providers to comply with HIPAA's privacy and security standards. Part I of this Article discusses the definition of PHRs and PHR system providers, weighs the advantages and disadvantages of integrating PHRs into the U.S. health system, and concludes that the benefits of PHRs outweigh their costs. Part II explains the HIPAA legal framework, including the Privacy Rule, the Security Rule, the Enforcement Rule, the 2008 Office for Civil Rights Guidance, and the modifications made to HIPAA under the American Recovery and Reinvestment Act of 2009 ("ARRA"). Part III advocates that Congress amends HIPAA to include all PHR system providers under the definition of covered entities and provides model legislation to achieve this goal. If Congress chooses not to amend HIPAA, however, Part IV explores alternatives that Congress and other policymakers should consider.

The Rise of Personal Health Records

Personal Health Records and Personal Health Record System Providers

What Is a Personal Health Record?

Types of Personal Health Records. The earliest PHRs were paper-based records that allowed an individual to compile their basic health care information, such as past or current illnesses, surgeries, hospitalizations, medications, and allergies. For example, diabetics may record their glucose levels throughout the day, persons with high blood pressure may track their blood pressure over a year, and family members may compile a family health history to provide insight into medical predispositions.[28] Although

paper-based PHRs are inexpensive to maintain and they centralize a consumer's health information, they suffer from four main weaknesses. First, they lack the ability to perform complex tasks because they cannot consult external medical resources. For example, paper-based PHRs are unable to alert the consumer of an adverse drug interaction or allow a consumer to research a medication's side effects. Second, their utility is limited to the consumer's perseverance because the onus is on the consumer to compile and organize their medical records. Third, providers may have difficulty accessing paper-based PHRs, especially in emergency situations when the consumer is unlikely to have the PHR on-hand.[29] Fourth, providers may doubt the reliability and accuracy of patient-created information contained in PHRs.[30]

Some of the weaknesses inherent in paper-based PHRs were eliminated when computers enabled PHRs to become software-based. Software-based PHRs provide users with the ability to organize multiple individuals' health care data and perform complex tasks, such as alerting the user of an adverse drug interaction or calculating the users risk for diabetes and heart-disease using medically-proven formulas.[31] Even software-based PHRs, however, have weaknesses. Convenience and accessibility are limited because software-based PHRs are usually bound to one physical location. For example, a family on vacation would not be able to access a software-based PHR contained on their home desktop computer.[32] To increase accessibility, some software-based PHRs can transfer health care data onto portable information devices ("PIDs"), such as CD-ROMs, USB flash drives, or PDAs.[33] Even with PIDs, however, PHRs are still anchored to a physical location and PIDs are not always interoperable with the provider's information system. Like their paper-based predecessors, software-based PHRs are effective at centralizing a consumer's health care data, but they still lack the ability to provide a convenient, accessible, and up-to-date link between consumers and their providers.

Finally, the Internet Age revolutionized PHRs because it enabled so-called "cloud computing," where internet-based software is accessible from any computer that can connect to the internet.[34] In addition to increased accessibility, internet-based PHRs enhance convenience and efficiency because there is often a real-time link between consumers and their providers. For example, PHRs enable clinical results to be sent almost instantly to the provider that ordered the test, the consumer, and any other provider selected by the consumer. Since the first internet-based PHR appeared in 1999,[35] over 200 PHR system providers have entered this market, including two information technology behemoths Google and Microsoft.[36]

One downside of internet-based PHRs is that they implicate additional privacy and security concerns.[37] While locked file cabinets and password protections may have been adequate for paper- and software-based PHRs because they were in the consumer's physical possession, internet-based PHRs may require additional privacy and security protections because the information is within the possession of a third party—the PHR system provider.

Defining Personal Health Records. Before health information contained in PHRs can be protected, PHRs must be defined. Defining PHRs is difficult because as technology continues to change, PHRs continue to evolve with it.[38] Although there is no universal definition,[39] Congress adopted the first statutory definition of PHRs under ARRA in 2009. ARRA defines PHRs 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."[40]

The central characteristic of a PHR is that "[p]atients are the dominant managers and custodians of their [PHRs]."[41] Beyond this central characteristic, PHRs diverge along a vast spectrum. On one end of the spectrum, the consumer has the power to *create and maintain* all of the data in the PHR.[42] On the other end of the spectrum, the consumer has the power to only *import and view* physician-created EHRs.[43] To strike a balance between accessibility and privacy, the modern trend in the PHR industry is to take a hybrid approach: the consumer can both (1) create, maintain, and sometimes export consumer-provided health data,[44] and (2) import and view certain physician-created EHRs.[45] In addition, most PHR systems perform other functions in addition to centralizing health care data, such as alerting consumers to adverse drug interactions, reminding consumers of physician appointments, and providing access to medical information and expert advice.[46]

What Is a Personal Health Record System Provider?

A PHR system "refers to the internet-based tools that help an individual understand and manage the information contained in a PHR."[47] A PHR system provider is an entity that creates, maintains, and operates the PHR system.[48]

Covered PHR system providers, such as health insurance companies and hospital systems, must comply with

Personal Health Records. . .

Continued from page 5

HIPAA's privacy and security standards.[49] In most cases, covered PHR system providers offer PHRs as a free additional service to complement the medical services that they provide to consumers. In contrast, uncovered PHR system providers, such as Google and Microsoft,[50] are not required to comply with HIPAA's privacy and security standards.[51] Because uncovered PHR system providers do not provide medical services to consumers, the motives behind offering consumers free access to a PHR system is less clear. Although some uncovered PHR system providers charge health care providers who want to use their PHR platform, other uncovered PHR system providers could sell the information contained in a consumer's PHR or use the information to sell advertisements targeted at the consumer. The World Privacy Forum, a non-profit interest group that focuses on privacy issues, argues that uncovered PHR system providers with access to PHI have an incentive to exploit an individual's information because they have duties to shareholders to earn a profit and HIPAA does not prevent them from using the health information.[52]

Google Health, which does not charge users, doctors' offices, hospitals, pharmacies, and other companies that partner with Google Health, or post advertisements, contends that the company is providing the free service because Google's "primary focus is providing a good user experience and meeting our users' needs."[53] In the future, however, Google may decide to use a consumer's information to direct targeted advertisements at the consumer.[54] Although this is currently prohibited under Google's privacy policy, the policy reserves Google's right to make changes to the privacy policy in the future.[55] In addition, Google Health has a "search the web" toolbar within the platform that contains sponsored links within the search results.[56]

Uncovered PHR system providers are still searching for a balance between profits and privacy. On one hand, uncovered PHR system providers need to earn a profit on their investment. On the other hand, violating their users' trust that their personal information will be kept private and secure could undermine their business.

Advantages of Personal Health Records

PHR advocates contend that PHRs are uniquely configured to combat the twin evils that are weakening the U.S. health care system—increasing health care costs and decreasing quality of health care.[57] Because PHRs allow health care information to become more accessible to consumers and providers, the U.S. health care system will operate more efficiently and effectively.

Personal Health Records Decrease Health Care Costs

Many observers contend that U.S. health care costs are rising at an unsustainable trajectory.[58] In 2007, far outpacing peer OECD countries, U.S. health care spending reached $2.2 trillion, or about $7,421 per resident, and accounted for 16.2% of the nation's GDP.[59] The issue continues to worsen. In 2006, total health expenditures increased 6.7% from the previous year and increased again in 2007 by 6.1%.[60] Unless the U.S. health care system adopts drastic cost-saving measures, health care costs will continue to increase.[61]

The spillover effects of increasing health care costs can have devastating effects on the general public. As a result of increasing costs:

> many Americans struggl[e] to pay their medical bills. Workers complain that they cannot afford high premiums for health insurance. Patients forgo recommended care rather than pay the out-of-pocket costs. Employers are cutting back or eliminating health benefits, forcing millions more people into the ranks of the uninsured. And state and federal governments strain to meet the expanding costs of public programs like Medicaid and Medicare.[62]

The U.S. health care system has three main options: (1) allow costs to continue to increase, shifting more of the cost burden onto the consumer and making health insurance unaffordable to more consumers;[63] (2) decrease costs by decreasing the amount and range of services provided to consumers and discouraging the development and use of expensive technological advances, or (3) decrease costs without sacrificing quality of health care by operating the health care system more efficiently. The first two options, while less costly in the short-term, could have dire long-term consequences on both the economy and public health. The third option, in contrast, entails incurring short-term costs for long-term benefits.

One reason that U.S. health care costs are rising is because the "U.S. health care system is highly fragmented

among multiple payers, hundreds of thousands of providers often functioning in isolation, and patients with different levels of private and public coverage or no coverage at all."[64] Such fragmentation, which is exacerbated by the use of paper-based medical records, increases costs for two reasons. First, there are high administrative costs because providers must physically store medical records, incur duplication costs, and employ staff to act as the intermediary between consumers, providers, and payers.[65]

Second, there are high costs of care because providers often have an incomplete picture of the consumer's health profile when the provider makes a health care decision because the paper-based system scatters a consumer's medical records across providers. The Center for Information Technology Leadership ("CITL"), a research organization focusing on health information technology, conservatively estimated that PHRs could save the U.S. health system between $13 billion to $21 billion annually, or about 1% of the U.S.'s total health care expenditures in 2007.[66] CITL's report, however, failed to account for other cost-saving spillover benefits. PHRs could reduce the approximately $300 billion dollars a year that are spent on duplicative or ineffective treatment that does not improve patient outcomes.[67] In addition, PHRs could reduce the cost of medical errors estimated between $17 billion and $29 billion annually and medication errors estimated between $1.56 and $5.6 billion annually.[68]

PHRs would allow the U.S. health care system to realize efficiencies because "widespread computerization could greatly reduce the paperwork burden on doctors and hospitals, head off medication errors, and reduce the costly repetition of diagnostic tests as consumers move from one doctor to another."[69] Therefore, PHRs have the potential to be a potent weapon in the struggle to reduce costs in the U.S. health care system.

Personal Health Records Improve Health Care Quality

Despite spending more on health as a percentage of GDP than any other OECD country,[70] the World Health Organization ranked the U.S. 37th out of 191 countries in terms of quality of health care in its 2000 World Health Report.[71] In the years following, the Institute of Medicine, a non-profit organization that provides science-based advice on health matters, has released several reports that expose the prevalence and costs of medical errors in the U.S. health care system,[72] and criticize the U.S. health care system's decreasing quality of health care,[73] and depict the prevalence and costs of medication errors in the U.S. health care system.[74]

PHRs would improve the quality of health care for two reasons. First, on the consumer side, PHRs empower consumers to become active participants in their health care rather than passive bystanders. PHRs provide consumers with easier access to their EHRs, and an opportunity to review the EHRs for errors.[75] PHRs also allow consumers to supplement their medical records with personal information, such as allergies and current medications that may not be included in their EHRs. To combat the U.S. health systems weakness in preventative medicine, PHRs allow consumers "to manage their own health care through alerts and reminders[76] that help to improve medication adherence;[77] or make appointments to receive recommended screening (e.g., cancer) and immunizations (e.g., flu shots);" or track important diagnostic information (e.g., glucose levels, blood pressure).[78]

Second, on the provider side, PHRs provide physicians with information and tools that enable them deliver higher quality care. When providers have more information about a consumer's health profile, they reduce the likelihood of medical errors and adverse drug events, make more accurate diagnoses, and prescribe more effective treatments.[79] In addition, providers are also able to give patients customized content to help them manage their own care[80] and achieve additional administrative benefits by being able to electronically handle referrals to specialists.[81] Third, PHRs can help providers monitor a patient's progress and prescribe treatment and medications instantly over the internet.

Disadvantages of Personal Health Records

PHRs' greatest strength—accessibility—is also its greatest weakness. Although PHRs may decrease health care costs and improve health care quality because consumers and providers have more access to information, these benefits come at a cost. First, PHRs expose consumers to more risk that their PHI will be wrongly used or disclosed. Second, building the infrastructure needed to integrate PHRs into the U.S. health care system is a costly and risky venture.

Personal Health Records Increase the Risks to Consumer Privacy and Security

Senator Leahy stated that "[i]n America today, if you have a health record, you have a health privacy problem. . . . The ability to easily access this information electronically . . . can be useful in providing more cost-effective health care, but it can also lead to a loss of personal privacy."[82]

Personal Health Records. . .

Continued from page 7

Many consumers agree with Senator Leahy. In a recent survey, although 79% or more of the public believe using an online PHR provides major benefits, 87% to 92% said that privacy practices would be essential or significant in their decision to sign up for a PHR and 56.8% cited privacy concerns as the reason for not utilizing PHRs.[83]

The WPF believes it is both rational and accurate for the public to perceive PHRs as a privacy threat for the following reasons:

- Health records in a PHR may lose their privileged status.[84]
- PHR records can be more easily subpoenaed by a third party than health records covered under HIPAA.[85]
- Identifiable health information may leak out of a PHR into the marketing system or to commercial data brokers.
- In some cases, the information in a non-HIPAA covered PHR may be sold, rented, or otherwise shared.
- It may be easier for consumers to accidentally or casually authorize the sharing of records in a PHR.
- Consumers may think they have more control over the disclosure of PHR records than they actually do.
- The linkage of PHR records from different sources may be embarrassing, cause family problems, or have other unexpected consequences.
- Privacy protections offered by PHR vendors may be weaker than consumers expect and may be subject to change without notice or consumer consent.[86]

To alleviate consumers' privacy concerns, most uncovered PHR system providers have adopted their own internal privacy policies. Under Section 5 of the Federal Trade Commission Act, the Federal Trade Commission may bring enforcement actions against companies that do not adhere to their privacy policies.[87] The Altarum Institute examined the privacy policies and procedures of thirty uncovered PHR system providers and found a "wide variation in understanding and implementation."[88]

Altarum concluded that:

- Existing privacy policies are incomplete;
- Consensus requirements for the contents of a PHR privacy policy do not yet exist, and many vendors appear to have focused instead on security procedures and Internet privacy descriptions;
- Transparency of secondary use of data could be greatly improved;
- The majority of vendors reviewed did not reference HIPAA;
- Data disposal rules and regulations are ill-defined, especially for closed accounts and vendors that go out of business; and
- Many specific terms including 'personal health information' are not defined in the privacy policy or related documentation.[89]

To overcome these flaws, HHS proposed a model PHR privacy policy.[90] But even if effective privacy policies were adopted, uncovered PHR system providers could modify their privacy policies without notice and are still not required by law to adhere to minimum privacy and security standards.[91] Without such legal baseline, many privacy organizations fear that "relying entirely on market forces to determine the nature and direction of PHR systems could cause personal health information to be exploited for its economic value without adequate consumer controls."[92] Even if an entity is not affirmatively selling health information or using it to direct advertisements at the consumer, the lack of economic incentives to provide privacy and security safeguards could allow computer hackers and other third parties to illegally obtain personal health information and use it for fraudulent purposes, such as medical identity theft.[93] Unless privacy protections are mandated under the law, the incentives to use personal health information to earn a profit are far stronger than voluntary privacy protections.

Setting baseline standards are particularly important to the PHR industry because they build trust between the consumer and PHR system providers. If there are disparities between the privacy and security standards of PHR system providers and no assurances that PHR system providers are bound to provide a minimum standard of

privacy and security, consumers may not trust their personal health information with PHRs.

HIPAA is one such Act that sets baseline security and privacy standards on protected health information created or maintained by "covered entities," but many PHR system providers are not subject to the security and privacy requirements under HIPAA because they are not considered "covered entities" under HIPAA.[94]

Transitioning from a Paper-based Medical Records System to an Electronic-based Medical Records System Is Costly and Risky

Building the infrastructure to transition from a paper-based medical records system to an electronic-based medical records system has high upfront costs. Even if the infrastructure is built, the outcome is uncertain whether the benefits of decreased health care costs and improved health care quality can be realized because the system's success depends on provider adoption and consumer utilization rates.

Interoperability means the ability to exchange information between consumers, health care providers, and public health organizations.[95] In other words, all three groups have the ability to access the same patient data. Although the hope is to use PHR systems as the focal point for exchanging patient information, today's reality consists of narrow one-way transactions. For example, some health care providers have agreements with PHR system providers that limit consumers to only that PHR system.[96] Not only does this limit the consumer's choice of PHR systems, but also providers may not be able to communicate with each other because the information contained on many PHR systems are incompatible with other PHR systems.[97]

The cost of making PHR systems interoperable includes building infrastructure and creating applications that provide consumers with the services that they need.[98] PHR infrastructure consists of functions that allow consumers to store and view their health information (e.g., data centers, user interfaces, user support, data storage, secure messaging).[99] PHR applications are any function within a PHR system that allows consumers to learn about, monitor, manage their own health and the health of others, and to exchange data with others regarding their health and well-being (e.g., smoking cessation management, appointment scheduling, and e-visits.).[100]

Depending on the PHR architectural model,[101] the acquisition costs could range between $3.7 and $134 billion dollars and it could take years to realize a positive net value.[102] Even if the infrastructure was built, the effectiveness of the system depends on provider adoption and consumer utilization rates. Providers may not adopt PHRs because they may not have the resources to take advantage of the infrastructure and their legal duties on using and disclosing information contained in PHRs are uncertain.[103] Consumers may not utilize PHRs because they may not trust their sensitive health information will be kept private and secure.[104] Therefore, transitioning to an electronic-based medical records system that will maximize the benefits of PHRs is both costly to implement and carries an uncertain outcome.

Cost-Benefit Analysis

PHRs are a good fit for the U.S. health care system because the benefits outweigh the risks.[105] First, the advantages of PHRs match the weaknesses currently afflicting the U.S. health system, maximizing their potential impact. PHRs are promising tools to both (1) decrease costs and allow the health system to function more efficiently and (2) improve the quality of care. Both of these advantages form a symbiotic relationship—as the quality of care improves, costs decrease and vice versa. For example, higher quality care will resolve issues before they become expensive issues or require fewer resources to diagnose. As health care costs decrease, the size of the population that can afford health care or health care insurance will increase and, as a result, they will receive higher quality health care.

Second, the disadvantages of PHRs can be resolved with federal legislation. For example, the lack of privacy and security can be resolved if the federal government mandates minimum privacy and security standards. Furthermore, once privacy and security was assured, interoperability could be facilitated because medical records would be safe.

To overcome these disadvantages, this Article advocates that Congress amend HIPAA to define all PHR system providers as covered entities. Thus, all PHR system providers would be required to comply with HIPAA's baseline security and privacy standards. HIPAA would be the ideal vehicle to ensure that all PHR system providers comply with minimum privacy and security standards because there are already well-tested regulations and enforcement mechanisms in place. The next Part discusses the HIPAA framework.

Personal Health Records. . .

Continued from page 9

The Health Insurance Portability and Accountability Act Framework

An Overview of HIPAA

On August 21, 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA)[106] to "combat waste, fraud, and abuse in health insurance and health care delivery . . . ."[107] In furtherance of this purpose, HIPAA contained administrative simplification provisions[108] that were intended to promote the "efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[109] Such a system envisioned by Congress depends on trust—consumers had to trust that those with access to their personal health information would keep it private and secure. To ensure that those with access to personal health information did not violate this trust, HIPAA required the HHS Secretary to promulgate privacy and security standards for "protected health information"[110] and also gave the Secretary the authority to enforce these standards.[111] Fulfilling this obligation, the Secretary promulgated the Privacy Rule, the Security Rule, and the Enforcement Rule (collectively, the "Rules").[112]

Applicability

Generally speaking, HIPAA imposes strict limitations on the disclosure of PHI and requires those with access to PHI to adhere to stringent security safeguards to prevent disclosure of PHI. However, HIPAA does not apply to every person with access to PHI. HIPAA applies only to "covered entities." Covered entity means any (1) health plan;[113] (2) health care clearinghouse;[114] and (3) health care provider who transmits health information in connection with a transaction covered under HIPAA.[115] Because some PHR system providers do not fall within the definition of a covered entity, they are not obligated to comply with HIPAA's privacy and security requirements.[116] Therefore, if a consumer discloses PHI to an uncovered PHR system provider, the PHR system provider is not required to adhere to HIPAA's privacy and security requirements.

The Privacy Rule

HIPAA authorized HHS to promulgate standards for the privacy of PHI if Congress did not enact health care privacy legislation by August 21, 1999.[117] Despite making recommendations to Congress in consultation with the National Committee on Vital and Health Statistics and the Attorney General.[118] Congress failed to pass such legislation by its self-imposed deadline.[119]

As a result, in 2000, the HHS issued the first version of the HIPAA Privacy Rule.[120] For the first time, a floor of national protections for the privacy of health information was established.[121] Shortly after the rule became effective, however, HHS was inundated with complaints because the Privacy Rule "*required* covered entities to seek individual consent before using or disclosing protected health information for routine uses."[122] The prior consent requirement created administrative burdens and had unintended negative effects on health care quality and access to health care.[123] For example, the prior consent requirement barred pharmacists from filling prescriptions and searching for potential drug interactions before patients arrived at the pharmacy.[124] In 2002, the Privacy Rule was modified to allow uses and disclosures without an individual's consent for routine uses such as "treatment, payment, and health care operations" while "maintain[ing] strong protections for the privacy of individually identifiable health information . . . ."[125]

Under the HIPAA Privacy Rule, "[a] covered entity may not use or disclose [PHI], except as permitted or required" by the Privacy Rule.[126] The Privacy Rule permits covered entities to use or disclose PHI in a few enumerated circumstances, such as: (1) to the individual;[127] (2) for treatment, payment, or health care operations;[128] (3) the health information is de-identified protected health information;[129] (4) to business associates;[130] (5) by law, court order, or for public health research;[131] and (6) other approved transactions.[132] In other circumstances, the individual's authorization is required or the individual must be given an opportunity to agree or reject the disclosure before the covered entity may use or disclose the PHI.[133] The Privacy Rule requires covered entities to use or disclose PHI under two main circumstances: (1) to the individual after a request has been made pursuant to HIPAA's right to access provisions;[134] and (2) to investigate or determine the covered

entity's compliance with the Privacy Rule.[135] In most cases, the disclosure must be limited to the extent necessary to achieve the intended purpose.[136]

Notably, covered entities may disclose PHI to business associates[137] and allow a business associate to create or receive PHI on its behalf.[138] To use a business associate, the covered entity must (1) "obtain[] satisfactory assurance[s] that the business associate will appropriately safeguard the information" and (2) "document the satisfactory assurances . . . through a written contract or other written agreement or arrangement with the business associate" that satisfied certain requirements under the Privacy Rule.[139]

A HIPAA Privacy Rule violation occurs when a covered entity uses or discloses PHI that does not satisfy any of the exceptions permitting disclosure. For example, a violation can be as minimal as discussing an individual's PHI in a hospital elevator or as drastic as allowing backup tapes, optical disks, and laptops containing over 386,000 individual's unencrypted electronic PHI to be lost or stolen.[141] The Privacy Rule is not only limited to use and disclosure requirements, but also includes administrative requirements. Among the administrative requirements, a covered entity must: (1) train all members of its workforce on the policies and procedures with respect to protected health information;[141] (2) have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information;[142] and (3) have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of the Privacy Rule.[143] For example, in 2009 settlement agreement, CVS agreed to pay $2.25 million because the pharmacy had violated the administrative requirements of the Privacy Rule violations by improperly disposing of PHI, failing to train employees how to properly dispose of PHI, and failing to maintain and implement a sanction policy for employees who did not properly dispose of PHI.[144]

The Security Rule

HIPAA required HHS to adopt standards to protect information while in the custody of covered entities and in transit between covered entities and from covered entities to others.[145] In 2003, the HHS Secretary issued the final HIPAA Security Rule.[146] Similar to the Privacy Rule, the Security Rule requires covered entities to protect and safeguard PHI.[147] The Security Rule, however, applies a more comprehensive set of safeguards to only electronic PHI, while the Privacy Rule applies a less comprehensive set of safeguards to all electronic, oral, or written PHI.[148] Under the Security Rule, covered entities must:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits;

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [the Privacy Rule; and]

(4) Ensure compliance with [the Security Rule] by its workforce.[149]

Recognizing that covered entities had varying degrees of resources and exposure to security risks, HHS granted covered entities flexibility when determining how to implement the standards under Security Rule.[150] The factors are: (1) the size, complexity, and capabilities of the covered entity; (2) the covered entity's technical infrastructure, hardware, and software security capabilities; (3) the costs of security measures; and (4) the probability and criticality of potential risks to electronic protected health information.[151]

To satisfy the four elements under the Security Rule, covered entities, taking into account the four factors for implementation, have to comply with three main safeguards—administrative, physical, and technical.[152] To satisfy each safeguard, there are standards under each safeguard with required or addressable implementation specifications to provide guidance to the covered entities.

Administrative Safeguards

The Security Rule defines administrative safeguards as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[153] The administrative safeguards provision contains eight standards. The first standard under administrative safeguards is that the covered entity must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[154] To satisfy this standard, a covered entity is required to (1) conduct an accurate and thorough risk analysis; (2) implement security measures sufficient to reduce risks and vulner-

Personal Health Records. . .

Continued from page 9

abilities; (3) apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures; and (4) implement procedures to regularly review records of information system activity.[155] The other standards include identifying the security official who is responsible for the development and implementation of the policies and procedures;[156] implementing policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information;[157] and others.[158]

Like the Privacy Rule, the Security Rule contains an exception for the business associates of covered entities.[159] The Security Rule "permit[s] a business associate to create, receive, maintain, or transmit electronic [PHI] on the covered entity's behalf."[160] To use a business associate, the covered entity must (1) "obtain[] satisfactory assurance[s] that the business associate will appropriately safeguard the information" and (2) "document the satisfactory assurances . . . through a written contract or other written agreement or arrangement with the business associate" that satisfied certain requirements under the Privacy Rule.[161]

Physical Safeguards

The Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[162] The physical safeguards provision contains four standards. Covered entities are required to: (1) implement policies and procedures for access to facilities that house its electronic information systems;[163] (2) implement policies and procedures for workstation use;[164] (3) implement physical safeguards for all workstations;[165] and (4) implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI.[166]

Technical Safeguards

The Security Rule defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."[167] The technical safeguards provision contains five standards. Covered entities are required to: (1) control access to electronic information systems that maintain electronic PHI;[168] (2) implement audit controls that record and examine activity in information systems that contain or use electronic protected health information;[169] (3) implement policies and procedures to protect electronic protected health information from improper alteration or destruction;[170] (4) authenticate the person or entity seeking access to electronic PHI;[171] and (5) guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.[172]

The Enforcement Rule

HIPAA established civil money penalties and criminal penalties when a covered entity violates a provision in the Act.[173] HIPAA delegated HHS to enforce the civil money penalties and the U.S. Department of Justice to enforce the criminal penalties.[174] In 2000, HHS further delegated the authority to administer and enforce compliance with the Privacy Rule to the Office for Civil Rights ("OCR").[175] In 2003, HHS delegated the authority to administer and enforce compliance with the Security Rule to the Centers for Medicare and Medicaid Services ("CMS").[176] The public must make complaints to either OCR or CMS, or both,[177] because "HIPAA itself and the regulations adopted to implement its privacy protection contain no explicit private right of action, and courts have refused to infer a private cause of action under HIPAA for privacy violations."[178] In 2006, the HHS Secretary issued the final HIPAA Enforcement Rule to guide OCR and CMS in their compliance and enforcement activities.[179]

The Enforcement Rule outlines the process for imposing civil money penalties on a covered entity that violates HIPAA. First, the Enforcement Rule states that OCR and CMS will "seek the cooperation of covered entities in obtaining compliance with the applicable administrative simplification provisions" and authorizes them to "provide technical assistance to covered entities to help them comply voluntarily with the applicable administrative simplification provisions."[180] Second, if a person believes that a covered entity has violated a HIPAA provision or rule, a per-

son may file a complaint with OCR or CMS, who will then investigate the complaint.[181] Third, even if there is no public complaint, OCR and CMS may conduct compliance reviews to determine whether a covered entity is complying with HIPAA.[182] During complaint investigations or compliance reviews, covered entities are required to cooperate with investigators, provide records and compliance reports, and permit access to information needed by investigators.[183]

If an investigation or compliance review shows a HIPAA violation, then OCR and CMS has the discretion to resolve the matter through informal means (e.g., demonstrated compliance, completed corrective action plan, or resolution agreements) or formal means (e.g., civil money penalties, referral to DOJ for criminal charges).[184] Although the civil penalties used to be relatively small,[185] the American Recovery and Reinvestment Act of 2009[186] drastically increased the civil money penalties as high as $50,000 per violation, not exceeding $1,500,000 annually for identical violations.[187] The criminal penalties, depending on the severity of the violation, are between $50,000 and $250,000 or up to 10 years in prison, or both.[188]

2008 HHS Guidance on Personal Health Records

Uncovered PHR system providers want their users to have access to EHRs held by covered entities, but HIPAA prohibits covered entities from sharing this information with uncovered PHR system providers. One way to circumvent this barrier is for covered entities to sign a formal agreement with uncovered PHR system providers that makes them the covered entities' "business associates" as defined under HIPAA regulations.[189] Such business associations allow covered entities to share EHRs with uncovered entities as long as they receive adequate assurances in writing that they will comply with HIPAA.[190] For example, the Cleveland Clinic and Google Health have signed an agreement that allows the clinic's EHRs to be accessed through Google Health.[191]

On December 15, 2008, the OCR issued a guidance confirming that covered entities could hire an uncovered PHR system provider as a business associate to administer a PHR or perform other PHR-related services or functions.[192] HHS's rationale was that "the Privacy Rule supports individuals' use of PHRs as a mechanism to facilitate access to, and control over, their health information."[193]

American Recovery and Reinvestment Act of 2009

On February 17, 2009, Congress passed the American Recovery and Reinvestment Act of 2009 to revitalize the American economy. Title XIII of ARRA promotes the use of health information technology to decrease the health care costs that is both crippling the government's medical services (Medicare and Medicaid) and making health care unaffordable to many Americans. Because health information technology utilizes EHRs and PHRs, ARRA seeks to improve and clarify HIPAA's privacy and security provisions.

ARRA can be organized into two parts. The first part applies to covered entities and their business associates. ARRA provides that HIPAA's privacy and security standards apply equally to both covered entities and business associates.[194] The new privacy and security safeguards are: (1) covered entities must notify individuals of PHI breaches (business associates must notify covered entities);[195] (2) individuals are allowed to restrict a covered entity from disclosing PHI;[196] (3) covered entities and business associates are required to provide a record of all PHI disclosures;[197] (4) covered entity or business associate are prohibited from selling EHRs or PHI;[198] and (5) covered entities and business associates are limited in their ability to provide marketing services based on their PHI.[199]

The second part applies to uncovered PHR system providers, or "vendors of PHRs" as defined under ARRA.[200] ARRA provides that vendors of PHRs and other non-HIPAA-covered entities are required to notify individuals when there has been a breach of their PHR identifiable health information.[201]

Revising HIPAA to Cover Personal Health Records

Problems with the Current HIPAA Framework

Despite ARRA's attempt to improve privacy and security safeguards, the Act failed to address all of HIPAA's privacy and security weaknesses, and may have undercut the viability of the commercial PHR industry. There are four major problems with the current HIPAA framework. First, some uncovered PHR system providers may still be able to avoid HIPAA's privacy and security standards. Although crafters of HIPAA, enacted in 1996, likely could not have foreseen the proliferation of PHRs by uncovered entities through the internet, which first appeared in 1999, the crafters of ARRA knew the extent and potential of PHRs. Despite this knowledge, uncovered PHR system providers

Personal Health Records. . .

Continued from page 13

can still avoid the definition of PHR because it must be *primarily* managed, shared, or controlled by or for the individual.[202] This definition could be circumvented when, for instance, an individual's personally identifiable information is maintained electronically by someone else, such as a family member who is compiling a family health history.

Second, even if an uncovered PHR system provider is deemed to be a "vendor of PHRs" under ARRA, the uncovered PHR system provider is still not subject to HIPAA's minimum privacy and security safeguards, but only must provide notification to the individual of a breach after the harm has already occurred.[203] Instead, all PHR system providers, whether uncovered or covered, should comply with HIPAA's privacy and security safeguards.

Third, ARRA provides statutory confirmation that covered entities can hire uncovered PHR system providers as business associates and disclose a consumer's PHI to the business associate, as long as business associates agree to comply with HIPAA's privacy and security standards.[204] Congress's acceptance of the ability of covered entities form business associate relationships with uncovered PHR system providers, however, may stifle competition and innovation in the PHR industry. The use of business associations causes division within the PHR industry because PHR system providers compete for contracts by offering the most beneficial terms to covered entities, rather than competing by allowing consumers to choose the PHR system provider that offers the best product.

Furthermore, Congress' reliance on business associate relationships will inhibit interoperability within the U.S. health care system because it promotes the use of system-specific representations of medical information that are incompatible with other PHR systems.[205] For example, because the Mayo Clinic and the Cleveland Clinic have business associate relationships with different PHR system providers, a consumer who has EHRs at both clinics may not be able to access their EHRs through the same PHR system provider and may not be able to transfer their records between the two providers. Due to the lack of interoperability, once a business associate relationship is formed, the relationship is difficult to unwind because EHRs would have to be transferred between two incompatible systems.[206]

Instead of limiting a consumer's access to their health information based on a business associate relationship, all PHR system providers should be deemed covered entities. This would allow covered entities to share an individual's PHI, upon consent, with the now-covered PHR system provider that the consumer chooses, not the PHR system provider selected by their health care provider.

Fourth, ARRA's increased civil money penalties for HIPAA violations,[207] clarification of the criminal penalties,[208] accounting rules that require covered entities and business associates to maintain a record of all uses and disclosures of an individual's PHI,[209] and patient controls over the extent of the data that may be used or disclosed,[210] may have a chilling effect on the portability of PHR industry. The severity, complexity, and inflexibility of some ARRA provisions may "cause many physicians, hospitals, laboratories, and other parties to reevaluate their participation in fledgling [regional health information organizations] and health information exchange efforts, leaving them dependent on exchange of paper records."[211]

The current HIPAA framework fails to strike a balance between accessibility, privacy, and innovation. The next section seeks to correct the imbalance and proposes that Congress should amend HIPAA to require all PHR system providers to comply with HIPAA.

Model Legislation

Kirk J. Nahra, an attorney who specializes in privacy and information security litigation and counseling, concluded that: "[t]he market for health information technology is not waiting for final rules to develop [and] most of the relevant questions will need to be resolved through legislation, as there is no obvious regulatory vehicle to institute broad changes."[212] In other words, Congress should act diligently to bring all PHRs within government regulation before the infrastructure of PHR systems is solidified. If Congress waits until PHR system providers are anchored in their ways, Congress will create unnecessary costs and further disrupt consumer confidence in the stability of PHRs. Worse, if Congress waits to react to a major PHR privacy or security breach, consumer trust in the PHR industry could be irreparably damaged.

This Article proposes model legislation that Congress should adopt to require all PHR system providers to

HOME BACK NEXT

comply with HIPAA. The purpose of the model legislation is to allow the U.S. health care system to fully exploit the benefits offered by PHRs, while facilitating trust between PHRs and consumers by establishing minimum privacy and security standards.

The model legislation contains two primary components—(1) redefining "personal health record" and "electronic health record," and adding the definition "personal health record system provider," and (2) adding "personal health record system provider" to HIPAA's list of entities that are defined as "covered entities."

First, Congress or HHS should redefine "personal health record," "electronic health record," and add the definition of a "personal health record system provider." HHS may be a more effective author of the definitions because it is more adept at collaborating with the PHR industry and consumer groups and the definition is easier to amend in light of the ever-evolving characteristics of PHRs. When drafting the definition, lawmakers should adopt a broad definition because it will ensure that all PHR system providers will fall under HIPAA. Too narrow or vague of a definition, like the one adopted by Congress, could create loopholes in which PHR system providers try to avoid falling under HIPAA. Allowing some PHR system providers to fall outside HIPAA could have negative consequences on the entire PHR industry because it creates consumer confusion and mistrust. Therefore, the following definitions should be added to HIPAA:

> The term "personal health record" means any electronic record, other than an "electronic health record," that allows an individual to view one or more of the following:
>
> (1) Individually identifiable health information[213] created or maintained by a covered entity; or
>
> (2) Individually identifiable health information created or maintained by any individual.
>
> The term "electronic health record" means any electronic record created or maintained by any health care provider.
>
> The term "personal health record system provider" means any entity, other than (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered under the Privacy Rule (as defined under 45 C.F.R. § 160.103), that provides individuals the ability to access "personal health records."

Second, Congress should amend HIPAA to add "personal health record system providers" to the list of entities that are defined as "covered entities."[214] Because all PHR system providers are considered covered entities, this would eliminate the need to rely on business associates to interface with consumers. Eliminating business associates would allow consumers more freedom and flexibility to choose their PHR system providers because covered entities are not forced into contracts with business associates.

If this model legislation is enacted, all PHR system providers that satisfy the broad definitions of PHRs would be required to comply with HIPAA's privacy and security safeguards. This would allow the U.S. health system to exploit the advantages of PHRs by making PHRs accessible, interoperable, and portable, while minimizing their potential adverse impacts on an individual's privacy.

Weaknesses in the Model Legislation: Is Expanding HIPAA Coverage a Good Idea?

This Article proposes to expand the scope of HIPAA to regulate all PHR system providers. Expanding HIPAA's scope, however, may not be prudent because the agencies in charge of enforcement, OCR and CMS, are already overburdened, and in some cases, ineffective in their ability to deter and detect HIPAA violations.

In 2008, the Office of the Inspector General reported that CMS, the agency in charge of enforcing the Security Rule,[215] was failing to satisfy its duties. First, "CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities."[216] Second, "CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant covered entities that it might investigate."[217] Third, "CMS had not implemented proactive compliance reviews and therefore had no effective way to determine whether covered entities were complying with HIPAA Security Rule provisions . . . [n]or did CMS know how vulnerable protected health information was to attack by individuals intent on accessing and misusing protected health information."[218] Because CMS's enforcement mechanisms are inadequate, an expansion of HIPAA's scope may not be a prudent action.

Personal Health Records. . .

Continued from page 15

OCR, the agency in charge of enforcing the Privacy Rule,[219] also may not be in a position increase the number of entities that it must regulate. Although the OIG has not investigated OCR's enforcement of the Privacy Rule, several statistics indicate that the OCR could not handle an increase in the number of cases. For example, the number of complaints has increased from 6,534 in 2004 to 8,142 in 2007;[220] the total number of resolutions has drastically increased from 1,516 in 2003 to 9,280 in 2008;[221] and 14% of all complaints remain open.[222] Expanding the number of entities that must be regulated by both CMS and OCR may dilute their ability to detect and deter HIPAA violations.

Alternatives to Amending HIPAA to Regulate Personal Health Records

If Congress decides not to amend HIPAA to cover all PHR system providers, there are several other alternatives that strike a balance between accessibility and privacy.

Administrative-led Solutions

Although HIPAA may need to be amended, the Center for Democracy and Technology ("CDT"), a non-profit organization that promotes internet openness, warns that Congress should not have a dominant role in regulating PHRs because PHRs are continually evolving and innovating.[223] If Congress enacted broad legislation that brings all PHRs under HIPAA, it could exacerbate privacy and security concerns because it can not flexibly respond to new PHR industry developments.[224]

Rather than Congress dictating "one size fits all" terms, CDT proposed that government agencies be tasked with the responsibility to implement "precisely tailored policy solutions that are context and role-based and flexible enough to both encourage and respond to innovation."[225] For example, HIPAA was intended to apply to EHRs, "which are created and controlled by health care providers for purposes of treatment and care management."[226] As a result, HIPAA may not be effective in regulating PHRs "which are often created by and controlled by consumers and held by third party data stewards outside the health care system."[227]

To achieve this, Congress could enact legislation that gives a broad mandate to agencies to promulgate privacy and security regulations for different "technology platforms and business models."[228] For example, Congress could delegate HHS to strengthen the privacy and security regulations that apply to covered entities as defined under HIPAA, while the Federal Trade Commission could set the privacy and security regulations that govern internet-based PHR system providers.[229]

Self-Regulatory Organizations or Certification

Uncovered PHR system providers currently regulate themselves using their internally-adopted privacy policies. The problem is that these privacy policies can be easily modified to suit their means. Two alternatives that provide more accountability than self-regulation, but are less intrusive than government regulation is for uncovered PHR system providers to either establish a self-regulatory organization ("SRO") or a certification process.

First, PHR system providers could establish an SRO that requires its members to comply with standards that are identical or similar to HIPAA.[230] The ideal SRO would also have teeth. Like the federal government's civil and criminal penalties, the SRO must have the ability to impose corrective actions, money sanctions, suspension orders, or expulsion orders on members who do not comply with the SRO's standards. The benefits of an SRO are that it reduces government regulatory costs, uses regulators that are more familiar with industry practices, and provides more flexible regulation. On the other hand, there is a risk that an SRO will cater to the PHR industry's interests and provide lax regulations.

Second, similar to creating an SRO, an independent organization could certify PHR system providers that comply with certain standards that are similar or identical to HIPAA.[231] For example, the certifying organization could require that the PHR system providers adopt a privacy policy that parallels HIPAA's standards to receive certification.[232] The certifying organization should also have an audit and inspection function to ensure that PHR system providers are complying in practice and not just on-paper. As long as there is a continuous audit and inspection

function, consumers and providers would be able to trust the PHR system providers that satisfied the requirements for certification.

The Certification Commission for Healthcare Information Technology, a non-profit organization that already certifies EHR systems used by providers, has developed draft criteria to certify PHRs.[233] The criteria for certification has not been finalized, but would most likely have to meet seven privacy safeguards (consent, controlling access to your information, conditions of use, amending the record, account management, document import, and data availability) and standards in three other categories (security, interoperability, and functionality)."[234]

On one hand, certification may provide consumers with the assurances that they need to overcome their privacy and security fears about PHRs.[235] In addition, certification may promote certain industry-wide goals, such as interoperability.[236] On the other hand, certification may not be a good idea for two main reasons. First, certification might "stifle innovation" because it would narrowly define the essential characteristics of a certified PHR.[237] Second, certification is a costly process that may create high barriers of entry, especially for small start-ups.[238]

State Law Preemption

If Congress fails to act, states have the authority to set privacy and security standards that are more stringent than the minimum federal standards under HIPAA.[239] States have used their right to enact more stringent standards to fill in HIPAA's gaps in other places, such as prohibiting the use and disclosure of PHI pertaining to HIV/AIDs, mental health, and genetic information, and could use it again to prohibit the disclosure of PHI held by third parties.[240]

Two states, Arkansas and California, have enacted legislation that protects the information contained on PHRs.[241] In 2007, California enacted legislation that prohibits third parties from using or disclosing health information without the individual's consent.[242] Specifically, under California's Confidentiality of Medical Information Act:[243]

> [a]ny business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of [the Act].[244]

At first glance, some PHR system providers that are considered noncovered entities under HIPAA may fall within this definition and would be subject to the confidentiality and enforcement provisions under the Act.[245] If the PHR provider does not comply, California also prescribes civil and criminal penalties.[246] However, the California HealthCare Foundation pointed out that the Act applies only to entities "organized *for the purpose* of maintaining medical information" which means "[i]n the context of personal health information custodians, this means it is possible—even likely—that some custodian models would fall wholly outside of existing regulatory authority."[247] In sum, if Congress is unwilling, states could take legislative action to bring PHR system providers under state privacy and security regulations.

Health Record Banking

Another emerging approach to consumer-oriented health record management is health record banking.[248] Health record banking is when a consumer selects an organization to serve as the custodian for a consumer's health records EHRs.[249] The consumer elects the personal health information that the provider may transmit into the account.[250] The consumer has a right to access the consumer's account anytime and anywhere, in addition to determining which providers may access all or part of their records.[251]

Because health record banking uses a trustee-based model, the consumer is given stronger privacy assurances.[252] Like PHRs, health record banking gives the consumer control over their personal health information—consumers can choose which medical records are deposited in their account and which medical records a certain provider may view. Unlike PHRs, however, health record banking presents less privacy concerns because "[c]onfidentiality is protected by a trust agreement that governs further distribution of data, but is assured only to the extent that the trustee lives up to its fiduciary responsibilities."[253] Security issues, however, remain because "trustees of large data sets may be attractive targets for hackers."[254]

Given the amount of money that the PHR system providers have invested, PHR systems are likely here to stay. The best solution is to provide consumers with the most options and allow commercial Darwinism to choose the victor. Increased competition may force PHR system

Continued from page 17

providers and health record banks to engage in a race-to-the-top for offering privacy and security protections to consumers.

Conclusion

The U.S. health care system presents an interesting dichotomy: it uses some of the most state-of-the-art technology and equipment, yet its medical records system is still paper-based. Although PHRs can both increase the health care system's efficiency and empower consumers, they also expose consumers to the risk of privacy breaches. In 2009, Congress finally recognized that health care privacy and security needed to be strengthened, but failed to provide the full privacy and security protections needed by consumers. To adequately combat privacy and security threats, Congress should amend HIPAA to extend to all PHR system providers. ▪

** J.D. Candidate, 2009, The George Washington University Law School; B.A., 2006, The George Washington University.*

Endnotes

1 Barack Obama, President-elect, American Recovery and Reinvestment (Jan. 8, 2009), link at http://change.gov/newsroom/entry/dramatic_action .

2 This narrative has been fictionalized, but seeks to portray elements of the lack of collaboration, communication, and information sharing present in health care settings today.

3 For the purposes of this Article, the term "provider" shall refer to persons and entities providing health care services to consumers (i.e., hospitals, doctors, nurses, laboratory technicians); the term "consumer" shall refer to the person receiving health care services (i.e., patients); and the term "payer" shall refer to persons and entities that pay providers for the health care services they provide to consumers (i.e., private health insurers, Medicare and Medicaid, out-of-pocket consumers).

4 Exec. Order No. 13,335, 69 Fed. Reg. 24,059 (Apr. 27, 2004) (establishing the position of National Health Information Technology Coordinator who is responsible for "guid[ing] the nationwide implementation of interoperable health information technology in both the public and private health care sectors"); David J. Brailer, *Presidential Leadership and Health Information Technology*, 28 Health Affairs 392 (Mar. 2009).

5 Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, 360 New Eng. J. Med. 1, 1 (2009) (finding that only 9% of U.S. hospitals use electronic health records); Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care—A National Survey of Physicians*, 359 New Eng. J. Med. 50, 50 (2008) (finding that only 17% of U.S. doctors use electronic health records).

6 Electronic medical records ("EMRs") are "[a]n electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization." The Nat'l Alliance for Health Info. Tech., Defining Key Health Information Technology Terms 15 (2008), link at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848133_0_0_18/10_2_hit_terms.pdf [hereinafter Defining Key Terms].

7 Electronic health records ("EHRs") are "[a]n electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization." *Id.*

8 Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 Health Affairs 1103, 1103–1117 (2005) ("It is widely believed that broad adoption of electronic medical record (EMR) systems will lead to major health care savings, reduce medical errors, and improve health."); Samuel J. Wang et al., *A Cost-benefit Analysis of Electronic Medical Records in Primary Care*, 114 Am. J. Med. 397, 397-403 (2003) ("In the 5-year cost-benefit model, the net benefit of implementing a full electronic medical record system was $86,400 per provider."); U.S. Dep't of Health & Human Servs., Health Information Technology, link at http://www.hhs.gov/healthit/ (last visited Mar. 4, 2009) (citing the benefits of health information technology: (1) improve health care quality; (2) prevent medical errors; (3) reduce health care costs; (4) increase administrative efficiencies; (5) decrease paperwork; and (6) Expand access to affordable care); *see, e.g.*, Stephen D. Persell et al., *Electronic Health* Record-Based Cardiac Risk

HOME BACK NEXT

Assessment and Identification of Unmet Preventive Needs, 47 Med. Care 4 (2009) (finding EHR data can be used to automatically perform cardiovascular risk stratification and identify patients in need of risk-lowering interventions which could improve detection of high-risk patients whom physicians would otherwise be unaware); Dwight C. Evans et al., *Effect of the Implementation of an Enterprise-wide Electronic Health Record on Productivity in the Veterans Health Administration*, 1 Health Econ., Pol'y & L. 163, 163-69 (2006) (finding the VHA has been able to increase its productivity by nearly 6 percent per year since full EHR implementation in 1999). For a full analysis of the benefits (and costs) of PHRs, see *infra* Part I.B–C.

9 Paul C. Tang et al., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. Am. Med. Informatics Ass'n 121, 122 (2006) ("[A]ll the advantages of PHRs for providers depend on the PHR being integrated with the provider's EHR.").

10 For example of scenarios illustrating the PHR's potential for integrating the U.S. health care system, see Markle Found., Health Decision Making Circa 2015 1–8 (2007), link at http://connectingforhealth.org/resources/Decision_Cases_FINAL_9-21-07.pdf; Markle Found., Connecting Americans to Their Healthcare 32–43 (2004), link at http://www.connectingforhealth.org/resources/wg_eis_final_report_0704.pdf.

11 Defining Key Terms, *supra* note 6. For a full discussion of the definition of PHRs, see *infra* Part I.A.

12 *See* Markle Found., Common Framework for Networked Personal Health Information 2 (2008), link at http://www.connectingforhealth.org/phti/docs/Overview.pdf .

13 Press Release, Secretary Leavitt Announces New Principles, Tools to Protect Privacy, Encourage More Effective Use of Patient Information to Improve Care (Dec. 15, 2008), link at http://www.hhs.gov/news/press/2008pres/12/20081215a.html (HHS Secretary Leavitt stated "[f]inding the balance between increased access to information and privacy is very important. If we don't have it, we won't succeed."); Robert Pear, *Privacy Issue Complicates Push to Link Medical Data*, N.Y. Times, Jan. 18, 2009, at D1. Privacy refers to "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." Altarum Inst., Review of the Personal Health Record (PHR) Service Provider Market 2 (2007), link at http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf [hereinafter Altarum Report]. In general, the health care data privacy laws seek to protect this right. For a full explanation of the health care data privacy laws, see *infra* Part II.B. Security refers to "physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure." Altarum Report, *supra* note 13. In general, the health care data security laws require certain safeguards to prevent to protect identifiable health data from unwarranted access or disclosure. For a full explanation of the health care data security laws, see *infra* Part II.C.

14 "Protected health information" means individually identifiable health information that is: (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium. 45 C.F.R. § 160.103 (2009). "Individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. *Id.* As discussed more in-depth *infra* Part II, most health care providers are prohibited from sharing a consumer's PHI, unless certain requirements are satisfied. Most providers, however, are required to disclose the consumer's PHI with the consumer and provide the consumer with access to the PHI generally in the form or format requested by the consumer. *See* 45 C.F.R. § 164.502(a)(1)(i), 164.524.

15 PHR system providers can, however, be held accountable under other laws. For example, the Federal Trade Commission requires that websites comply with their privacy policies. *See infra* note 91.

16 HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26, 29, and 42 U.S.C. (2006)). part at (2006)).

17 42 U.S.C. § 1320d-1(a) (discussing HIPAA's applicability); 45 C.F.R. § 160.103 (defining "covered entities").

18 HIPPA, § 262 (codified at 42 U.S.C. §§ 1320d to 1320d-8).

19 42 U.S.C. § 1320d-2(d) (giving the Secretary authority to adopt privacy and security standards).

20 Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164 (2009)) [hereinafter Privacy Rule]. The main sections of the Privacy Rule can be found at 45 C.F.R. §§ 164.501 to 164.534.

21 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) [hereinafter Security Rule]. The

main sections of the Security Rule can be found at 45 C.F.R. §§ 164.302 to 164.318.

22 HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390, (Feb. 16, 2006) (codified at 45 C.F.R. pts. 160 & 164) [hereinafter Enforcement Rule]. The main sections of the Enforcement Rule can be found at §§ 160.300 to 160.316.

23 *See infra* Part II.C–E.

24 Off. of Civ. Rts., Personal Health Records and the HIPAA Privacy Rule 7 (2008), link at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf [hereinafter OCR Guidance]. This disparity has the potential to create consumer confusion because it is difficult to determine whether a PHR system provider is required to comply with HIPAA or a consumer may assume (wrongly) that all PHR system providers must comply with HIPAA. Robert Gellman, World Privacy F., Personal Health Records: Why Many PHRs Threaten Privacy (2008), link at http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf [hereinafter World Privacy F.].

25 Markle Found., Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve Their Health 1, (2008), link at http://www.connectingforhealth.org/resources/ResearchBrief-200806.pdf [hereinafter Markle Found. Survey] ("Only 2.7 percent of adults have an electronic PHR today (representing about 6.1 million persons). Most (57.3 percent) do not keep any form of personal health records, and 40 percent keep some paper health records.")

26 The Markle Foundation conducted a survey of 1,580 U.S. adults and found that:

> Consumers cite privacy concerns as a significant barrier to PHR adoption. Of the people who said they were not interested in having a PHR, more than half (57 percent) cited privacy concerns as a reason for not wanting one. "Regarding health privacy, we found that 24 percent of the public have high concerns; 49 percent to 56 percent have moderate concerns, and only 20 percent to 27 percent have low concerns," [Professor Emeritus Alan F.] Westin said. "This pattern of health privacy intensity suggests that 73 percent to 80 percent of the public will want to be assured of robust privacy and security practices by online PHR services, if they are to join those offerings."
>
> Press Release, Markle Found., Technology Companies, Providers, Health Insurers and Consumer Groups Agree on Framework for Increasing Privacy and Consumer Control Over Personal Health Records (June 25, 2008), link at http://www.connectingforhealth.org/news/pressrelease_062508.html. Another Markle Foundation survey of 1,003 U.S. adults found that "Americans express strong concern that their information may be used for purposes other than their own care. Eight in 10 Americans (80%) say they are very concerned about identity theft or fraud or the possibility of their information getting into the hands of marketers (77%)." Markle Found., National Survey on Electronic Personal Health Records 1, (2006), link at http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

27 Robert L. Coffield & Gerald E. DeLoss, *The Rise of the Personal Health Record: Panacea or Pitfall for Health Information*, 12 Health Law. News 8, 10–13 (2008) (discussing legal issues created by PHRs).

28 *See, e.g.*, Rebecca Walton, HealthNote: An Easy, Do-It-Yourself Guide to Managing Your Health Information (2007); Melissa Kahn, Personal Health Care Passport (2004); So Tell Me Organizer, http://sotellmeorganizer.com/ (last visited Mar. 5, 2009) (personal health record organizers).

29 Some of the weaknesses may cut both ways. First, paper-based PHRs may be more convenient for some populations. For example, elderly consumers may feel more comfortable with a paper-based PHR than an electronic PHR. Second, paper-based PHRs may be more accessible to providers when providers do not have the technology to view electronic PHRs.

30 Nicholas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic*

> *Health Records*, 2007 U. Ill. L. Rev. 681, 722 (2007) (stating that patient-provided health data is "less likely to be viewed as reliable by providers").

31 *See, e.g.*, CheckUp, link at http://www.checkupsoftware.com/Overview.html (last visited Mar. 5, 2009); HealthFrame, link at http://www.recordsforliving.com/HealthFrame (last visited Mar. 5, 2009); MyMeds, link at https://www.my-meds.com/index.html (last visited Mar. 5, 2009).

32 To increase accessibility, some software-based PHRs allow the user to print-out a medical summary.

33 *See, e.g.*, HealthFile, link at http://www.wakefieldsoft.com/healthfile (last visited Mar. 5, 2009) (PDAs); ICER-2-Go, link at http://www.icer-2-go.com (last visited Mar. 5, 2009) (flash drive); My Medical CD, link at http://www.mymedicalcd.com/about.asp (last visited Mar. 5, 2009) (mini CD); VitalKey, link at http://www.vitalkey.com/site/info_on_vitalkey (last visited Mar. 5, 2009). It is interesting to note how as user accessibility and convenience increases, privacy and security risks also increase. Most PIDs are password-protected.

34 Don Long, *Google CEO: 'Cloud Computing' Is Key to Patient-Owned PHR's*, Medical Device Wk., Mar. 3, 2008.

35 Bob Brown, *The Number of Online Personal Health Records Is Growing, But Is the Data in These Records Adequately Protected*, 9 No. 3 J. Health Care

Compliance 35, 35 (2007). It is important to keep in mind that HIPAA was passed in 1996, so the crafters of HIPAA may not have foreseen the internet-based PHR.

36 *See* Steve Lohr, *Dr. Google and Dr. Microsoft*, N.Y. TIMES, Aug. 14, 2007, at C1; Microsoft HealthVault, link at http://www.healthvault.com (last visited Jan. 16, 2009); Google Health, link at http://www.google.com/health (last visited Jan. 16, 2009).

37 This Article focuses on the internet-based PHR and the regulation of internet-based PHR system providers because they impose the most risks on privacy and security.

38 *See* James S. Kahn et al., *What It Takes: Characteristics of the Ideal Personal Health Record*, 28 Health Affairs 369, 369 (2009) (stating that there is still a need for PHR innovation and improvement).

39 *See, e.g.*, Nat'l Comm. on Vital & Health Statistics, Personal Health Records and Personal Health Record Systems 14 (2006), link at http://ncvhs.hhs.gov/0602nhiirpt.pdf. ("[T]he term 'personal health record' to refer to the collection of information about an individual's health and health care, stored in electronic format."); Markle Found., The Personal Health Working Group 3 (2003), link at http://www.connectingforhealth.org/resources/final_phwg_report1.pdf ("The Personal Health Record (PHR) is an Internet-based set of tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it.").

40 American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, § 13400(11), 123 Stat. 115 (2009). The term "PHR identifiable health information" means individually identifiable health information . . . and includes, with respect to an individual, information—(A) that is provided by or on behalf of the individual; and (B) 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. ARRA § 13407(f)(2).

41 Terry & Francis, *supra* note 30, at 721. In contrast, physicians are the dominant managers and custodians of EHRs. "The idea of electronic medical records is simple: take the records that doctors, hospitals and other health care providers have traditionally maintained, and move them from paper to electronic formats." Kirk J. Nahra, *How Health Information Exchange Is Driving a New Health Care Privacy Debate*, 17 Health L. Rep. (BNA) 825, 826 (June. 12, 2008).

42 Terry & Francis, *supra* note 30, at 721; *see, e.g.*, myHealthFolders, link at https://myhealthfolders.com/features.aspx (Mar. 5, 2009) (allowing the user to insert and access their health care data over the internet, but cannot import EHRs).

43 *Id.*; *see, e.g.*, Kaiser Permanente, My Health Manager, link at https://members.kaiserpermanente.org/kpweb/toc.do?theme=myhealthmanager_members (last visited Mar. 5, 2009) (allowing patient to view EHRs, but does not allow a consumer to add or supplement information).

44 Patient-provided health data typically includes:

> personal identification, including name and birth date; emergency contacts; names, addresses, and phone numbers of physicians, dentists, and specialists; health insurance information; living wills, advance directives, or medical power of attorney; organ donor authorization; a list and dates of significant illnesses and surgical procedures; current medications and dosages; immunizations and their dates; allergies or sensitivities to drugs or materials; important events, dates, and hereditary conditions in the family history; results from a recent physical examination; opinions of specialists; important test results; eye and dental records; correspondence between the patient and the provider(s); educational materials; and any other information the patient wishes to include.
>
> Gina Marie Stevens, Electronic Personal Health Records 3–4 (Cong. Research Serv., CRS Report for Congress Order Code RS22760, Nov. 15, 2007), link at http://leahy.senate.gov/issues/medprivacy/CRSemedprivacy.pdf; *see, e.g.*, CapMed, link at http://www.capmed.com (last visited Jan. 16, 2009); Google Health, link at http://www.google.com/health (last visited Jan. 16, 2009); Microsoft HealthVault, link at http://www.healthvault.com (last visited Jan. 16, 2009); Revolution Health, link at http://www.revolutionhealth.com (last visited Jan. 16, 2009); WebMD Personal Health Manager, link at http://www.webmd.com/phr (last visited Jan. 16, 2009). Patient-provided health data is "less likely to be viewed as reliable by providers." Terry & Francis, *supra* note 30, at 722.

45 Pursuant to HIPAA requirements, this option is only available when the PHR system provider has an agreement with a covered entity. OCR Guidance, supra note 24, at 4–7. For example, Microsoft HealthVault has agreements with Kaiser Permanente, Aetna, the Mayo Clinic and New York-Presbyterian Hospital. Steve Lohr, *Kaiser Endorses Microsoft's Health Records Plan*, N.Y. Times, June 10, 2008, at C4. Google has agreements with the Cleveland Clinic and Beth Israel Deaconess Medical Center. *Id.*

46 Salomeh Keyhani, *Electronic Health Record Components and the Quality of Care*, 46 Med. Care 1267, 1267 (2008); *see, e.g.*, Health Butler, link at http://healthbutler.com (last visited Mar. 5, 2009) (allowing the user to set alerts and reminders for cancer screenings, immunizations, and other preventive measures); WebMD, link at http://www.webmd.com (last visited

Mar. 5, 2009) (allowing the obtain health information and advice).

47 Nat'l Comm. on Vital & Health Statistics, *supra* note 39, at 14.

48 *Id.*

49 OCR Guidance, *supra* note 24, at 2; *see, e.g.*, Kaiser Permanente, My Health Manager, link at https://members.kaiserpermanente.org/kpweb/toc.do?theme=myhealthmanager_members (last visited Mar. 5, 2009); Aetna's Personal Health Record, http://www.aetna.com/showcase/phr/ (last visited Mar. 5, 2009).

50 For the purposes of this Article, the term "PHR" shall refer to the internet-based PHR and the term "PHR system provider" shall refer to the commercial PHR system provider. Although Google Health and Microsoft HealthVault are the two high-profile PHR system providers, there are many others. *See, e.g.*, myOptumHealth, link at http://www.myoptumhealth.com/portal (last visited Jan. 16, 2009); Revolution Health, link at http://www.revolutionhealth.com (last visited Jan. 16, 2009).

51 Congress defines entities that offer or maintain PHRs, but are not covered entities as "vendors of personal health records." ARRA, § 13400(18).

52 *See generally* Robert Gellman, World Privacy Forum, Personal Health Records: Why Many PHRs Threaten Privacy (2008), link at http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

53 Google Health Frequently Asked Questions, link at http://www.google.com/intl/en-US/health/faq.html#free (last visited Jan. 12, 2009) (answering the question "If it's free, how does Google make money off Google Health?").

54 Jessica E. Vascellaro, *Google Helps Organize Medical Records*, Wall St. J., May 20, 2008, at D2. The same holds true for Microsoft HealthVault. Jay Greene, *Microsoft Wants Your Health Records*, Bus. Week, Oct. 15, 2007, at 44 (discussing how "Microsoft is hoping it can make money on the service—which is free to patients—with help from a little box inside HealthVault's page, where consumers can search the Web").

55 Google Health Privacy Policy, link at http://www.google.com/intl/en-US/health/privacy.html (last visited Mar. 27, 2009) (stating that "Google will not sell, rent, or share your information (identified or de-identified) without your explicit consent, except in the limited situations described in the Google Privacy Policy"); Google Privacy Policy, link at http://www.google.com/intl/en/privacypolicy.html (last visited Mar. 27, 2009) (explaining when a user's information will be shared with other parties and reserving Google's right to make changes to the privacy policy in the future); *see also* Gellman, *supra* note 52, at 15–16 (stating that privacy policies may be amended at any time without notice to the user).

56 *See* Google Health, link at http://www.google.com/health (last visited Mar. 27, 2009).

57 Inst. of Med., Preventing Medication Errors 3–6 (2007), link at http://www.nap.edu/catalog.php?record_id=11623#toc.

Inst. of Med., Crossing the Quality Chasm 1–4 (2001), link at http://www.nap.edu/catalog.php?record_id=10027#toc; Inst. of Med., To Err Is Human: Building a Safer Health System 1–2 (2000), link at http://www.nap.edu/catalog.php?record_id=9728#toc; *see also* Lisa L. Dahm, *Healthcare Systems and Quality of Care: Do International Measurement Standards Exist?*, 20 Temp. Int'l & Comp. L.J. 395 (2006) (finding that the U.S. health care system spends more money than other OECD countries and that the quality of health care is poor compared to other OECD countries).

58 U.S. Gen. Accounting Office, Pub. No. GAO-04-793SP, Health Care: Unsustainable Trends Necessitate Comprehensive and Fundamental Reforms to Control Spending and Improve Value 3–6 (2004), link at http://www.gao.gov/new.items/d04793sp.pdf [hereinafter Unsustainable Trends].

59 Micah Hartman et al., *National Health Spending In 2007: Slower Drug Spending Contributes to Lowest Rate of Overall Growth Since 1998*, 28 Health Affairs 246, 246 (2009); Kaiser Family Found., Health Care Spending in the United States and OECD Countries, link at http://www.kff.org/insurance/snapshot/chcm010307oth.cfm (last visited Jan. 14, 2009); Kaiser Family Found., U.S. Health Care Costs: Background Brief, link at http://www.kaiseredu.org/topics_im.asp?imID=1&parentID=61&id=358#3b (last visited Jan. 12, 2009).

60 Aaron Catlin et al., *National Health Spending in 2006: A Year of Change for Prescription Drugs*, 27 Health Affairs 14, 14 (2008); Hartman, *supra* note 59 (noting that historically in economic downturns health care expenditures has increased its share of GDP); Kaiser Family Foundation, U.S. Health Care Costs: Background Brief, link at http://www.kaiseredu.org/topics_im.asp?imID=1&parentID=61&id=358#3b (last visited Jan. 12, 2009).

61 Unsustainable Trends, *supra* note 58, at 4–5.

62 Editorial, *The High Cost of Health Care*, N.Y. Times, Nov. 25, 2007, at 49. 45 million Americans are uninsured. *See* McKinsey & Co., Accounting for the Cost of U.S. Health Care: A New Look at Why Americans Spend More 11 (2008), link at http://www.mckinsey.com/mgi/reports/pdfs/healthcare/US_healthcare_Executive_summary.pdf.

63 Even if a consumer's employer provides health care insurance, increased insurance costs will most likely

be passed onto the consumer in the form of lower wages or foregone benefits. *See* David Blumenthal, *Employer-Sponsored Health Insurance in the United States—Origins and Implications*, 355 New Eng. J. Med. 82, 85 (2006) ("[E]conomists . . . argue that ultimately employers pass the costs of health care on to workers who pay for their own health insurance in the form of wages or other benefits foregone.").

64 Unsustainable Trends, *supra* note 58, at 9. There are many other reasons why health care costs are increasing, such as expensive health care technology with modest benefits. *See* Catherine Arnst, *Behind Rising Health-Care Costs*, Bus. Wk., July 14, 2008, at 12. This Article focuses on costs associated with the U.S. health care system's lack of information sharing because PHRs are well-suited to decreases these costs.

65 *Id.*

66 Ctr. for Info. Tech. Leadership, The Value of Personal Health Records 77 (2008), link at http://www.citl.org/_pdf/CITL_PHR_Report.pdf. The report limited the cost-saving benefits to sharing of complete test results, sharing of complete medication lists, smoking cessation management, congestive heart failure (CHF) monitoring, appointment scheduling, medication renewals, preencounter questionnaires, and e-visits.

67 Curtis P. McLaughlin & Arnold D. Kaluzny, Continuous Quality Improvement in Health Care 604 (3d ed. 2005).

68 Preventing Medication Errors, *supra* note 57, at 3–6; To Err Is Human, *supra* note 57, at 1–2 (finding there are 1.5 million cases of preventable adverse drug event a year); Agency for Healthcare Research and Quality, Reducing and Preventing Adverse Drug Events to Decrease Hospital Costs, link at http://www.ahrq.gov/qual/aderia/aderia.htm#4 (last visited Jan. 18, 2009).

69 Editorial, *The High Cost of Health Care*, N.Y. Times, Nov. 25, 2007, at 49 ("The American health care system lags well behind other sectors of the economy—and behind foreign medical systems—in adopting computers, electronic health records and information-sharing technologies.").

70 *See supra* notes 59–60 and accompanying text.

71 World Health Org., The World Health Report 152–55 (2000), link at http://www.who.int/whr/2000/en/whr00_en.pdf. To assess a health system, the World Health Organization used five factors: (1) the overall level of health; (2) the distribution of health in the population; (3) the overall level of responsiveness; (4) the distribution of responsiveness; and (5) the distribution of financial contribution. *Id.* at 27.

72 *See generally* To Err Is Human, *supra* note 57. The Agency for Healthcare Quality and Research, the agency tasked for evaluating health care quality and disparity in the U.S. health care system, reports annually on health care quality indicators. *See* Agency for Healthcare Quality and Research, Health Care: Measuring Healthcare Quality Subdirectory Page, link at http://www.ahrq.gov/qual/measurix.htm (last visited Mar. 10, 2009) (reporting on health care quality indicators in the U.S. health care system).

73 *See generally* Inst. of Med., Crossing the Quality Chasm, *supra* note 57.

74 *See generally* Preventing Medication Errors, *supra* note 57.

75 Victoria E. Knight, *Patient Records Need Reviews*, Wall St. J., Aug. 30, 2007, at D2 ("Errors in medical records aren't uncommon.").

76 Paul C. Tang & David Lansky, *The Missing Link: Bridging The Patient–Provider Health Information Gap*, 24 Health Affairs 1290, 1291 (2005).

77 Paul C. Tang et al., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. Am. Med. Info. Ass'n 121, 124 (2006).

78 Rajeev Chaudhry et al., *Web-Based Proactive System to Improve Breast Cancer Screening: A Randomized Controlled Trial*. 167 Archives of Internal Med. 606, 606 (2007); Maria Staroselsky et al., *Improving Electronic Health Record (EHR) Accuracy and Increasing Compliance with Health Maintenance Clinical Guidelines Through Patient Access and Input*, 75 Int'l J. Med. Info. 693, 693 (2006).

79 Ctr. for Info. Tech. Leadership, *supra* note 66, at 30-32; S.N. Selvachandran et al., *Prediction of Colorectal Cancer by a Patient Consultation Questionnaire and Scoring System: A Prospective Study*, 360 Lancet 278, 278–83 (2002).

80 Tang & Lansky, *supra* note 76.

81 Lynn A. Volk et al., *Patients' Perceptions of a Web Portal Offering Clinic Messaging and Personal Health Information*, AMIA Ann. Symp. Proc. 1147 (2005); Eung-Hun Kim et al., *Application and Evaluation of Personal Health Information Management System*, 2004 Conf. Proceedings IEEE 3159–62 (2004); Maisie Wang et al., *Personal Health Information Management System and Its Application in Referral Management*, 8 IEEE Transactions Info. Tech. Biomedicine 287–97 (2004); Barbara A. Walters & Kim Danis, *Patient Online at Dartmouth-Hitchcock—Interactive Patient Care Web Site*, AMIA Ann. Symp. Proc. 1044 (2003).

82 Senator Patrick Leahy, Chairman, Senate Judiciary Committee, Introduction of The Health Information Privacy and Security Act of 2007 (July 18, 2007), link at http://leahy.senate.gov/press/200707/071807c.html.

83 Markle Found. Survey, *supra* note 25, at 1.

84 The physician-patient privilege often prevents a physician from disclosing confidential information.

Disclosing confidential information to a PHR system provider may waive the physician-patient privilege. Gellman, *supra* note 52, at 5–6.

85 Under HIPAA, when PHI is to be released in response to a subpoena or discovery request, the covered entity must receive satisfactory assurance that: (1) there have been good faith attempts to notify the subject of the protected health information in writing of the request and that subject has been given the opportunity to object; or (2) reasonable efforts have been made by the requesting party to obtain a qualified protective order. 45 C.F.R. § 164.512(e)(1)(ii)(A)–(B). Information disclosed to uncovered PHR system providers will not be subject to this stringent privacy standard and could be more easily obtained by third parties. *See generally* A. Michael Froomkin, Project HealthDesign ELSI Group, Forced Sharing of Patient-Controlled Health Records (2007), link at http://www.projecthealthdesign.org/media/file/Forced-sharing.pdf.

86 Gellman, *supra* note 52, at 2.

87 Federal Trade Commission Act, 15 U.S.C. § 45 (2006) (declaring "deceptive acts or practices in or affecting commerce" to be unlawful); *see, e.g.*, FTC, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), link at http://www.ftc.gov/opa/2000/07/toysmart2.htm (prosecuting Toysmart under Section 5 of the FTC Act by misrepresenting to consumers that personal information would never be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company's own privacy statement.).

88 Altarum Inst., Review of the Personal Health Record (PHR) Service Provider Market 17 (2007), link at http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf.

89 *Id.*

90 U.S. Dep't of Health & Human Servs., Health Info. Tech., Draft Model Personal Health Record (PHR) Privacy Notice & Facts-At-A-Glance, link at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1176&parentname=CommunityPage&parentid=11&mode=2&in_hi_userid=10732&cached=true (last visited Mar. 7, 2009); *see also* Daniel Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. Ill. L. Rev. 357 (2006) (proposing model regime for privacy protection); Federal Trade Commission, Fair Information Practice Principles, link at http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Mar. 7, 2009) (listing practices that provide adequate privacy protection).

91 Consumers may still have mechanisms for recourse against PHR system providers that are not subject to HIPAA's baseline privacy and security standards. For example, PHR system providers could be held legally accountable to comply with their privacy policies under Section 5 of the FTC Act. 15 U.S.C. § 45 (2006) (declaring "deceptive acts or practices in or affecting commerce" to be unlawful). Consumers may also have recourse in contract law, tort law, or state law. *See* Daniel Solove, The Digital Person: Technology and Privacy in the Information Age 56-75 (2004); *see also* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn St. L. Rev. 587, 597–609 (2007); Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. Intell. Prop. L. 57, 71–78 (1999).

92 Nat'l Comm. on Vital & Health Statistics, *supra* note 39, at 19.

93 *See* Off. of the Nat'l Coordinator for Health Info. Tech., Medical Identity Theft Final Report 1 (2009), link at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1239&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true.

Off. of the Nat'l Coordinator for Health Info. Tech., Medical Identity Theft Environmental Scan 7 (2008), link at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1239&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true.

94 Nahra, *supra* note 41. "If an Internet company offers a consumer a product to gather and store health care information, that activity is outside the scope of HIPAA unless the offering entity happens to be a health care provider or a health insurer. Clearly, some providers and insurers are offering these products; at least as often, however, these products are being offered by companies with no effective control under HIPAA." *Id.*

95 Nat'l Comm. on Vital & Health Statistics, *supra* note 39, at 25.

96 *See* Lohr, *supra* note 45.

97 Nat'l Comm. on Vital & Health Statistics, *supra* note 39, at 25.

98 Ctr. for Info. Tech. Leadership, *supra* note 66, at 47.

99 *Id.* at 13.

100 *Id.*

101 *Id.* at 17–20.

102 *Id.* at 55–70.

103 Coffield & DeLoss, *supra* note 27, at 10–13.

104 *See supra* note 26.

105 *See supra* Parts I.B–C.

106 Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, 110 Stat. 1936 (codified in part at 42 U.S.C. §§ 1320d to 1320d-8 (2006)).

107 *Id.*; *see also* H.R. Rep. No. 104-496, at 1, 66-67, *as reprinted in* 1996 U.S.C.C.A.N. 1865, 1865-66.

108 HIPAA §§ 261–264 (codified at 42 U.S.C. §§ 1320d to 1320d-8).

109 HIPAA § 261.

110 *See* 45 C.F.R. § 160.103 (2009).

111 42 U.S.C. § 1320d-2(a)–(d) (giving the HHS Secretary authority to promulgate privacy and security requirements and standards); *Id.* § 1320d-5 (providing general penalties for failure to comply with privacy and security requirements and standards); *Id.* § 1320d-6 (providing penalties for the wrongful disclosure of individually identifiable health information).

112 *See infra* Part II.C–E.

113 "Health plan" means "an individual or group plan that provides, or pays the cost of, medical care." 45 C.F.R. § 160.103 (defining "health plan").

114 Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. *Id.* § 160.103 (defining "health care clearinghouse").

115 42 U.S.C. § 1320d-1(a) (discussing HIPAA's applicability); 42 U.S.C. § 1320d-2(a)(1) (describing transactions covered under HIPAA for purposes of the third element of the term "covered entity"); 45 C.F.R. § 160.103 (defining "covered entity"); *see also* C. Stephen Redhead, Medical Records Privacy: Questions and Answers on the HIPAA Rule 2 (Cong. Research Serv., CRS Report for Congress Order Code RS20500, Feb. 4, 2005), link at http://leahy.senate.gov/issues/medprivacy/CRSQandAonHIPAA.pdf.

116 OCR Guidance, *supra* note 24, at 7; *see also* Gellman, *supra* note 86, at 3–4. Dr. Reid Cushman of Project HealthDesign has suggested that a PHR may actually be a covered entity because it is a health care clearinghouse. Reid Cushman, Project HealthDesign ELSI Group, Primer: HIPAA and PHRs 1–2 (2007), link at http://www.projecthealthdesign.org/media/file/primer_hipaa_and_PHRs.pdf. However, HHS likely does not share the same point of view because HHS has not brought enforcement actions against PHR system providers and this theory has not been tested in courts.

117 HIPAA § 264(c) (enacted Aug. 21, 1996).

118 *Id.* § 264(a), (d).

119 Privacy Rule, *supra* note 20, at 53,182.

120 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

121 Privacy Rule, *supra* note 20, at 53,182.

122 Citizens for Health v. Leavitt, 428 F.3d 167, 172 (3rd Cir. 2005) (upholding the Privacy Rule against a challenge that the rule violated due process rights).

123 Privacy Rule, *supra* note 20, at 53,182.

124 *Id.* at 53,209.

125 *Id.* at 53,182.

126 45 C.F.R. § 164.502(a) (2009).

127 *Id.* § 164.502(a)(1)(i).

128 *Id.* § 164.506.

129 *Id.* § 164.502(d).

130 *Id.* § 164.502(e).

131 *Id.* § 164.512(a)–(b), (e).

132 *See generally id.* § 164.502(a)(1).

133 *Id.* §§ 164.508, 164.510.

134 *Id.* § 164.502(a)(2)(i); *see also id.* §§ 164.524, 164.528.

135 *Id.* § 164.502(a)(2)(ii).

136 *Id.* § 164.502(b).

137 "Business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement . . . in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by [the Privacy Rule]; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation . . . management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or

arrangement, or from another business associate of such covered entity or arrangement, to the person." 45 C.F.R. § 160.103.

138 *Id.* § 164.502(e)(1).

139 *Id.* § 164.502(e)(1)–(2).

140 Off. of Civ. Rts., *HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information*, July 16, 2008, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/providenceresolutionagreement.html To view the Office of Civil Rights' case examples and resolution agreements for violations of HIPAA's Privacy Rule, see Off. of Civ. Rts., Case Examples and Resolution Agreements, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Mar. 8, 2009).

141 45 C.F.R. § 164.530(b).

142 *Id.* § 164.530(c).

143 *Id.* § 164.530(e); *see generally* 45 C.F.R. § 164.530.

144 Off. of Civ. Rts., *CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case*, Jan. 16, 2009, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html.

145 42 U.S.C. § 1320d-2 (2006).

146 Security Rule, *supra* note 21.

147 Ctrs. for Medicare & Medicaid Servs., HIPAA Security Series: Security 101 for Covered Entities 4–5 (2007), link at http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf.

148 Ctrs. for Medicare & Medicaid Servs., HIPAA Security Series: Security 101 for Covered Entities 4–5 (2007), link at http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf.

149 45 C.F.R. § 164.306(a)(1)–(4).

150 *Id.* § 164.306(b)(1).

151 *Id.* § 164.306(b)(2).

152 *Id.* § 164.306(c).

153 *Id.* § 164.304; *see also id.* § 164.308 (discussing the standards and implementation specifications for the administrative safeguards element). Half of the Security Rule's regulations are administrative safeguards. Ctrs. for Medicare & Medicaid Servs., HIPAA Security Series: Security Standards: Administrative Safeguards 2 (2007), link at http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsAdministrativeSafeguards.pdf.

154 *Id.* § 164.308(a)(1)(i).

155 *Id.* § 164.308(a)(1)(ii).

156 *Id.* § 164.308(a)(2).

157 *Id.* § 164.308(a)(3).

158 *See generally id.* § 164.308(a).

159 *Id.* § 160.103 (defining "business associate"); *Id.* § 164.308(b).

160 *Id.* § 164.308(b).

161 *Id.* § 164.308(b)(1)–(2).

162 *Id.* § 164.304; *see also id.* § 164.310 (discussing the standards and implementation specifications for the physical safeguards element).

163 *Id.* § 164.310(a).

164 *Id.* § 164.310(b).

165 *Id.* § 164.310(c).

166 *Id.* § 164.310(d).

167 *Id.* § 164.304; *see also id.* § 164.312 (discussing the standards and implementation specifications for the technical safeguards element).

168 *Id.* § 164.312(a).

169 *Id.* § 164.312(b).

170 *Id.* § 164.312(c).

171 *Id.* § 164.312(d).

172 *Id.* § 164.312(e).

173 42 U.S.C. § 1320d-5 (2006) (civil money penalties); *Id.* § 1320d-6 (criminal penalties).

174 Enforcement Rule, *supra* note 22, at 8390.

175 *Id.* at 8391; Statement of Delegation of Authority, 65 Fed. Reg. 82,381, 82,381 (Dec. 28, 2000). As of May 2007, 27,778 Privacy Rule complaints have been made in OCR—21,801 are closed, 5,997 are open. Office of Civil Rights, Compliance and Enforcement, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/05312007.html (last visited Jan. 15, 2009).

176 Enforcement Rule, *supra* note 22, at 8391; Statement of Organization, Functions, and Delegations of Authority, 68 Fed. Reg. 60,694, 60,694 (Oct. 23, 2003). As of December 31, 2008, 392 Security Rule complaints have been made to CMS—305 are closed, 87 are open. Ctrs. for Medicare & Medicaid Servs., CMS Enforcement Statistics Report 1 (2008), link at http://www.cms.hhs.gov/Enforcement/11_HIPAAEnforcementStatistics.asp; *see generally* Ctrs. for Medicare & Medicaid Servs., HIPAA Enforcement Statistics, link at http://www.cms.hhs.gov/Enforcement/11_HIPAAEnforcementStatistics.asp#TopOfPage (last visited Jan. 15, 2009).

177 When there is a violation of both the Privacy Rule and a nonprivacy rule, OCR coordinates an investigation with CMS. *See* U.S. Dep't of Health & Human Servs., Compliance and Enforcement: How OCR Enforces

the HIPAA Privacy Rule, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html (last visited Mar. 9, 2009).

178 Jamie Lund, Comment, *ERISA Enforcement of the HIPAA Privacy Rules*, 72 U. Chi. L. Rev. 1413, 1413 (2005) (citing University of Colorado Hospital Authority v Denver Publishing Co, 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004) ("[L]egal commentators appear to unanimously assume that there is no private right of action under HIPAA, including to enforce the 'privacy rule' of § 1320d-6.")).

179 Enforcement Rule, *supra* note 22, at 8390.

180 45 C.F.R. § 160.304(a)–(b).

181 *Id.* §§ 160.306(a), (c).

182 *Id.* § 160.308.

183 *Id.* § 160.310.

184 *Id.* § 160.312; *Id.* §§ 160.400 to 160.426.

185 42 U.S.C. § 1320d-5 (2006) ("[T]he Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.").

186 American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 115 (2009).

187 *Id.* § 13410.

188 42 U.S.C. § 1320d-6. Very few criminal cases have been brought under HIPAA. *See* Stevens, *supra* note 44, at 11–13.

189 OCR Guidance, *supra* note 24, at 4.

190 *Id.*

191 Steve Lohr, *Google Health Begins Its Preseason at Cleveland Clinic*, N.Y. Times, Feb. 21, 2008, link at http://bits.blogs.nytimes.com/2008/02/21/google-health-begins-its-preseason-at-cleveland-clinic/?ref=technology.

192 OCR Guidance, *supra* note 24, at 4.

193 *Id.* at 7–9; *see also* 45 C.F.R. §§ 164.502(e),164.504(e).

194 ARRA §§ 13401, 13404.

195 *Id.* § 13402.

196 *Id.* § 13405(a).

197 *Id.* § 13405(c).

198 *Id.* § 13405(d).

199 *Id.* § 13406.

200 *Id.* § 13400(18).

201 *Id.* § 13407.

202 *See id.* § 13400(11).

203 *See id.* § 13407.

204 *See id.* §§ 13401, 13404.

205 Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 Harv. L.J. & Tech. 103, 152–53 (2008).

206 *Id.* at 153–54 ("EHR system vendors may also find interoperability unappealing because it makes it easier for providers who have one EHR system to switch to another by enabling patient EHRs to be easily transferred between systems. Without interoperability, the difficulty of transferring hundreds or thousand of EHRs between different systems may deter providers from changing their EHR vendors.").

207 *See* ARRA § 13410.

208 *See id.* § 13409.

209 *See id.* § 13405(c).

210 *See id.* § 13410(a).

211 Brailer, *supra* note 4.

212 Nahra, *supra* note 41.

213 "Individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

214 *See* 45 C.F.R. § 160.103 (defining "covered entity").

215 *See supra* note 176 and accompanying text.

216 U.S. Dep't of Health & Human Servs., Off. of the Inspector General, Nationwide Review of the Centers for Medicate & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight 3 (2008), link at http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf.

217 *Id.*

218 *Id.* at 5.

219 *See supra* note 175 and accompanying text.

220 Office of Civil Rights, Health Information Privacy Complaints Received by Calendar Year, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html (last visited Mar. 11, 2009).

221 Office of Civil Rights, Enforcement Results by Year, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html#resol (last visited Mar. 11, 2009).

222 Office of Civil Rights, Numbers at a Glance, link at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/numbersglance0209.html (last visited Mar. 11, 2009).

223 Ctr. for Democracy & Tech., Comprehensive Privacy and Security: Critical for Health Information Technology 12–13 (2008), link at http://www.cdt.org/healthprivacy/20080514HPframe.pdf.

224 *Id.*

225 *Id.* at 12.

226 *Id.*

227 *Id.*

228 *Id.*

229 *Id.*

230 For example, Congress required that SROs for national securities exchanges enforce the Exchange Act on its members. 15 U.S.C. § 78f(b)(1) (2006).

231 The independent organization could be private or governmental. Professor Murphy recommends using a private organization because they are less costly and more flexible than governmental organizations. Tobi M. Murphy, Comment, *Enforcement of the HIPAA Privacy Rule: Moving from Illusory Compliance to Continuous Compliance Through Private Accreditation*, 54 Loy. L. Rev. 155, 197 (2008).

232 A good place to start would be HHS Secretary Leavitt's model privacy policy. *See* U.S. Dep't of Health & Human Servs., Draft Model Personal Health Record (PHR) Privacy Notice & Facts-At-A-Glance, link at http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1176&PageID=15440 (last visited Jan. 16, 2009).

233 Certification Comm'n for Healthcare Info. Tech., Consumer's Guide to Certification of Personal Health Records 3 (2008), link at http://cchit.org/files/CCHITPHRConsumerGuide08.pdf.

234 *Id.* at 5–6

235 Letter from Rose Marie Robertson & Nancy Davenport-Ennis, Co-chairs, Consumer Empowerment Workgroup, to The Honorable Michael O. Leavitt, Chairman, American Health Information Community (Jan. 23, 2007), link at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848182_0_0_18/2008%20AHIC%20CDS%20Recommendations%20-%20FINAL.pdf.

236 Increasing interoperability would also increase efficiency. Murphy, *supra* note 231, at 196.

237 Dissenting Statement on PHR Certification Process from Stephen Downs et al., to The Honorable Michael O. Leavitt, Chairman, American Health Information Community (Mar. 13, 2007), link at http://www.connectingforhealth.org/resources/cew_certification_dissent_final_22707.pdf.

238 *Id.*

239 42 U.S.C. § 1320d-7 (2006).

240 Ctr. for Democracy & Tech., *supra* note 225, at 8.

241 Kory Mertz, *Personal Health Data on the Net: States Address Privacy Concerns*, 29 State Health Notes (2008), link at http://www.ncsl.org/programs/health/shn/2008/sn517b.htm.

242 A.B. 1298 (Cal. 2007) (codified as amended at Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82), link at http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf.

243 Cal. Civ. Code §§ 56-56.37 (West 2009).

244 *Id.* § 56.06.

245 *Id.* §§ 56.10-56.265 (stating use and disclosure requirements for medical information); *Id.* §§ 56.35-56.36 (describing civil and criminal penalties for violating the Act).

246 *Id.* §§ 56.35-56.36.

247 Cal. HealthCare Found., Whose Data Is It Anyway? 5–6 (2008), link at http://www.chcf.org/documents/chronicdisease/WhoseDataIsItAnywayIB.pdf.

248 Health record banking was proposed in Congress in the Independent Health Record Bank Act of 2006. *See* S. 3454, 109th Cong. (2006); H.R. 5559, 109th Cong. (2006). Health record banking was proposed again in the House of Representatives in The Health Record Trust Act of 2007. *See* H.R. 2991, 110th Cong. (2007).

249 *See, e.g.*, eHealth Trust, link at http://www.ehealthtrust.com (last visited Jan. 16, 2009) (health record bank).

250 William A. Yasnoff, Health Record Banking Alliance 1–3 (2006), link at http://www.louhie.org/Downloads/HRBA%20Principles%20Final%20Draft%20May%2007.pdf; *see generally* William A. Yasnoff, *Electronic Records Are Key to Health-Care Reform*, Bus. Wk., Dec. 19, 2008; Health Record Banking Alliance, http://www.healthbanking.org (last visited Jan. 16, 2009).

251 Yasnoff, *supra* note 250, at 1–3.

252 Terry & Francis, *supra* note 30, at 723.

253 *Id.*; Paul T. Kostyack, Note, *The Emergence of the Healthcare Information Trust*, 12 Health Matrix 393, 435–47 (2002) ("The concept of fiduciary is central to the concept of a Healthcare Information Trust [(i.e. health record bank)] and is its major advantage over other market players that might play this role. The trustee, when assigned the assets of the trust (i.e., individually identifiable healthcare information) would be obligated to make the trust property productive for the benefit of the trust beneficiary. The trustee's obligation . . . is oriented only toward the interests of the beneficiary.").

254 Terry & Francis, *supra* note 30, at 723.

Not Quite to Copyright? Your Idea May Still Be Entitled to Protection

By Brian A. Hall and John Di Giacomo

Unfortunately, it is difficult to find laws supporting the proposition that ideas, in and of themselves, deserve protection. It appears even more difficult to find mechanisms for enforcement of an idea. Although difficult, it is not impossible, and it may be time to enact further protections for ideas and more stringent causes of action to enforce them. In order to do so, however, a question must be answered – what's in an idea?

Traditionalists may agree with Arnold H. Glasgow, who said: "An idea not coupled with action will never get any bigger than the brain cell it occupied." Copyright law's requirement that there be an expression of the idea in a tangible form seems to support such a view. However, let's face it – we are an idea economy. As such, I tend to agree with Owen Laughlin, who said: "Money never starts an idea. It is always the idea that starts the money." To this end, every aspiring artist fears that his or her creative idea will be stolen. Often, aspiring artists will submit their ideas to established television studios, authors, or musicians without fully developing the idea into a completed form, whether that form is a screenplay, novel, or demo tape. While media companies often state that they do not accept unsolicited ideas, artists often later notice, to their horror, that their idea has been used to create a profitable television show, book, or song. Since the idea has yet to be fully realized into a tangible form, the idea is not protected by common law copyright, sometimes known as a "poor man's copyright."

Clients often ask me whether copyright law protects against the misappropriation of their ideas. Unfortunately, and often to their dismay, I must explain that copyright law does not protect against the theft of ideas, but rather only the theft of the expression of those ideas. Many states, however, have tort or contract causes of action that can help protect a creative artist against the theft of an idea that has been sufficiently developed and presented to a producer or company for sale. These causes of action include misappropriation, implied-in-fact contracts, and breach of confidence or confidentiality.

The first of these causes of action is the tort of misappropriation. A claim for misappropriation typically exists where a defendant takes an original or novel idea from another. The idea must be original or novel because non-novel or unoriginal ideas are not considered protectable as "property." *See Nadel v. Play-By-Play Toys & Novelties, Inc.*, 208 F.3d 368, 378 (2d Cir. 2000). Additionally, there must be a legal relationship between the parties, in essence, a fiduciary relationship of trust or a relationship based on an express or implied-in-fact contract. *See McGhan v. Ebersol*, 608 F. Supp. 277, 284 (S.D.N.Y. 1985), *citing Vantage Point, Inc. v. Parker Bros.*, 529 F. Supp. 1204, 1216-1217 (E.D.N.Y. 1981), *aff'd mem. sub nom., Vantage Point, Inc. v. Milton Bradley*, 697 F.2d 301 (2d Cir. 1982). As New York courts have recognized, the states will "afford protection to persons who… have disclosed their ideas to others in the expectation that the idea would be used, and the use compensated." *Vantage Point, Inc. v. Parker Brother, Inc*., 529 F. Supp. 1204, 1216 (E.D.N.Y. 1981), *aff'd without op. sub. nom. Vantage Point, Inc. v. Milton Bradley*, 697 F.2d 301 (2d Cir. 1982). Since a misappropriation claim requires a relationship between the parties, it is unclear what benefit, if any, this separate cause of action presents outside of a typical implied-in-fact contact claim.

A number of cases have also found protection for ideas through contract law. Most notably, Justice Traynor's dissent in *Stanley v. Columbia Broadcasting System* stated that "[t]he policy that precludes protection of an abstract idea by copyright does not prevent its protection by contract." The California Supreme Court in *Desny v. Wilder* later adopted Traynor's *Stanley* dissent as law. Subsequent case law iterations of the law of contracts as applied to ideas have limited the protection of ideas to implied-in-fact contracts and not implied-in-law contracts. This distinction exists because implied-in-fact contracts are actual agreements between two parties that are established by looking to the conduct of the parties, as opposed to implied-in-law contracts that are simply imposed to prevent the unjust enrichment of a party.

Wrench, LLC v. Taco Bell is one such implied-in-fact contract case. In *Wrench*, Thomas Rinks and Joseph Shields, members of Wrench, created a cartoon character named "Psycho Chihuahua." This character was

Not Quite to Copyright?

Continued from page 29

described as a "clever feisty dog with an attitude." Rinks and Shields attended a licensing trade show in 1996 where two Taco Bell employees approached them and expressed an interest in the character.

After the trade show, the Taco Bell employees began promoting the Psycho Chihuahua character within Taco Bell. Rinks and Shields sent a number of promotional items to the company, including t-shirts, hats, stickers, and art boards. The two Taco Bell employees soon decided that it would be better to use a live dog that would be manipulated by computer graphics, instead of the cartoon character, and they discussed what it would cost Taco Bell to license and use the character. Wrench eventually sent a licensing proposal to Taco Bell, which was ultimately rejected.

In 1997, Taco Bell hired a new advertising agency, which presented an idea for a new commercial in which a male Chihuahua would pass up a female for a burrito from Taco Bell. The agency said that it had conceived of the idea when a few of its employees were eating Mexican food at a café and saw a Chihuahua walk by. Taco Bell ultimately aired its commercials containing the now famous Chihuahua in the United States in 1997, and Wrench brought suit against Taco Bell in Michigan shortly thereafter, alleging an implied contact in fact.

The decision in this case hinged upon whether Wrench's idea could properly be considered "property." The 6th Circuit Court of Appeals found that the Copyright Act did not preempt Wrench's state law claims. More importantly, the court found that an implied contact claim for the theft of an idea does not require the plaintiff to prove the novelty of the idea. Prior to this decision and as stated above, cases from other circuits had held that a plaintiff must prove the novelty of his idea because there can be no consideration for an implied promise to pay if the idea is not, in fact, "property." The 6th Circuit Court of Appeals found that an idea does not have to be novel or unique in order to constitute consideration for an implied-in-fact contract and, therefore, the trial court erred in dismissing the suit on the grounds that the plaintiff's idea was not novel.

Additionally, courts have recognized a cause of action for a breach of confidentiality to protect ideas. The principle case that established this doctrine is *Thompson v. California Brewing Co.* 150 Cal. App. 2d 469, 310 P.2d 436 (1957). In *Thompson*, the plaintiff submitted a letter to the California Brewing Company that recommended that they market beer under two different labels to two different audiences: one for men and the other for women. The court held that while the letter did not create a fiduciary relationship between the two parties, a fiduciary relationship is not necessary to assert a cause of action for a breach of confidence. Under *Thompson*'s reasoning, a cause of action for a breach of confidentiality can be established by showing (1) that the idea was disclosed in confidence under circumstances that show that the recipient of the idea knew that it was intended to be confidential, (2) that the recipient of the idea accepted the idea on the basis that it was confidential and consented to keep it confidential, and (3) that the recipient violated that confidence. *See* 4-19D Nimmer on Copyright § 19D.05. As with misappropriation law, some commentators have argued that a cause of action for breach of confidentiality or confidence is unnecessary because the situations to which this cause of action would be applicable also support a claim for an implied-in-fact contact. Regardless, the breach of confidentiality cause of action is another method by which individuals can protect their ideas outside of copyright law.

Even though copyright law cannot protect ideas, plaintiffs can still seek redress for the theft of their ideas under state tort or contract law. Whether through theories of misappropriation, implied-in-fact contracts, or breach of confidentiality, plaintiffs may have a remedy that lies outside of the traditional intellectual property realms of trademark law, copyright law, trade secret law, and patent law. While I remain of the belief that these traditional laws and the benefits they provide should remain, I want you to be aware of the protections available to ideas under the right circumstances. ▪

Brian Hall is a Partner at Traverse Legal, PLC in Traverse City, MI, and John Di Giacomo is an Associate with Traverse Legal, PLC. Mr. Hall and Mr. Di Giacomo practice in the areas of trademark, copyright, trade secret, and Internet law. Mr. Hall and Mr. Di Giacomo can be reached at (231) 932-0411, or by email at brianhall@traverselegal.com *and* john@traverselegal.com *respectively.*

Meet a Section Member: Jeanne M. Dunk

Jeanne M. Dunk

VP & Assoc General Counsel
Health Alliance Plan
2850 W Grand Blvd
Detroit, MI 48202

P: (313) 664-8106
E: jdunk@hap.org

- **What is the name of your firm/corporation/employer?** Health Alliance Plan of Michigan
- **What is your area of practice?** Corporate and regulatory health care; insurance; information technology
- **When did you first become involved with the Section?** 2009
- **Where did you grow up?** Brighton, MI when Brighton was a very small town.
- **Where else have you lived?** Detroit and Steubenville, Ohio (home of Dean Martin for those of you who went to grade school with the dinosaurs).
- **Where did you attend undergraduate and law school?** Undergrad – Michigan State; law school – MSU Law School (when it was called Detroit College of Law).
- **What was your undergraduate major?** Accounting and Finance
- **What are your hobbies, other interests?** Running, golf, reading, and cross stitch
- **Favorite restaurant?** Carrabba's
- **Last vacation?** Trinidad, Colorado
- **Who is your hero?** (a parent, a celebrity, an influential person in one's life) My brother Bill who passed away in 2008
- **If you had to describe yourself using four words, they would be…** determined to be happy!
- **What is your favorite movie of the past ten years?** *Love Actually*
- **What do you like to do most with a free hour?** Run or read
- **What e-mail can Section members use to contact you?** jdunk@hap.org
- **A short comment on why you became involved with the Information Law Technology Section:** Information Technology work is my favorite part of my practice. I enjoy the complexity of the technology, using my knowledge to help clients through complex contract development and post contract issues. The section offers support to my practice and it's nice to know there are other "geeks" out there like me who enjoy the work.

Publicly Available Websites for IT Lawyers

Following are some publicly available websites relating to varying aspects of information technology law practice. Some of these websites require payment for certain services. Neither the State Bar of Michigan nor the IT Law Section endorses these websites, the providers of the website, or the goods or services offered in connection therewith. Rather these websites are provided for information purposes only and as possible useful tools for your law practice.

Please provide any feedback or recommendations for additional websites to *brianhall@traverselegal.com* or *michael@gallo.us.com*.

Copyright Resources

- http://www.copyright.gov/ - Provides access to the United States Copyright Office and includes information relating to copyright law, access to registration services, and other information
- http://copyright.cornell.edu/resources/public-domain.cfm - Offers a table outlining they type of copyright, the copyright term, and what is in the public domain
- http://www.utsystem.edu/ogc/intellectualProperty/dmcaisp.htm - Provides instructions regarding compliance with the Digital Millennium Copyright Act
- http://www.copyscape.com/ - Allows a user to search for copies of a web page and plagiarism of the same
- http://www.tineye.com/ - Allows a user to submit an image and learn information relating to it, including where it might be used on the Internet
- http://fairuse.stanford.edu/ - Contains information relating to copyright fair use law, especially as it pertains to the educational and library services

2010 Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to three student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law.
2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.
3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top, and bottom margins of one inch.
4. Essay must include the submitter's name, e-mail address, mailing address, telephone number, and school attended.
5. A total of $1,500 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.
6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the *Michigan IT Lawyer*.
7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2010, and emailed to ***dsyrowik@brookskushman.com***.