

Health Care Privacy and Security in 2009: What's Hot on the Horizon?

BY KIRK J. NAHRA

While health care reform is at the forefront of everyone's mind as we enter 2009, health care companies and others who use health care information also should be prepared to deal with a significantly different environment for health care privacy and security in the year ahead. Here are a few of the top areas to be paying attention to in the next year.

1. *Health Care Privacy Legislation in the New Congress*

After several years of inaction, there were significant movements in 2008 toward new health care privacy legislation, driven at least in part by the desire to expand the use of electronic medical records. This push—and the related concern of many that these electronic records need new privacy rules—led committees in both houses of Congress to move significant health care privacy legislation through committee, typically as part of a larger bill to increase the incentives for and the use of health information technology and electronic medical records. For better or worse, these efforts fell victim to three related problems—the disagreement about the substance of new privacy legislation, the focus on the November election, and then the abandonment of all legislative activity except that related to the economy. But now, with the advent of the Obama administration on the horizon, we once again see substantial interest in legislation encouraging more use of health information technology. In fact, in a Dec. 6 radio address, President-elect Obama focused on the benefits to the overall economy of electronic medical records and more efficient health information technology. In this address, President-elect Obama said: We must also ensure that our hospitals are connected to each other through the Internet. That is why the economic recovery plan I'm proposing will help modernize our health care system—and that won't just save jobs, it will save lives. We will make sure that every doctor's office and hospital in this country is using cutting edge technology and electronic medical records so that we can cut red tape, prevent medical mistakes, and help save billions of dollars each year. (A transcript of this address is available at http://change.gov/newsroom/entry/the_key_parts_of_the_jobs_plan/).

This position is not at all surprising, given that improved utilization of health information technology has been a key component of the Obama health care plan from the start. In fact, the campaign's original health care position paper contained the following element:

Obama will lower health care costs: The Obama plan will lower health care costs by \$2,500 for a typical family by investing in health information technology, prevention and care coordination. *See* <http://www.barackobama.com/issues/healthcare/>.

Close on the heels of these pronouncements, the Bush administration also unleashed its final effort related to these technological developments for the healthcare industry. On Dec. 15, Health and Human Services Secretary Michael O. Leavitt, head of the American Health Information Community group that has been overseeing efforts to expand the use of health information technology, released the Health and Human Services Department "Privacy and Security Framework" for the electronic exchange of health care information. *See* http://www.hhs.gov/healthit/documents/NationwidePS_Framework.pdf. This document was intended to set a baseline standard for privacy and security controls related to electronic health records.

Taken together, these efforts, by two administrations, represent a continuing push toward expanded use of health information technology. For health care companies (and others that use, disclose or otherwise rely on health care information), the biggest questions for the privacy debate in 2009 will be whether the legislation encouraging health information technology will include health care privacy provisions and, if so, whether these provisions will advance or retard these significant economic opportunities.

So far, in 2008, Congress has seemed more interested in passing *something* to change the health care privacy environment than in ensuring that changes—even if arguably "pro-privacy"—would in fact make the health care system more productive and efficient (or even support the use of health information technology). Some of the proposed changes actually seemed designed to discourage use of certain health care technology, by imposing significant new obligations only on those health care companies that adopted this new technology (for example, by imposing new customer consent and individual rights obligations where companies adopt electronic medical records). Other provisions, some with substantial anti-efficiency implications, had nothing apparent to do with any efforts related to health care

technology. So, as the legislation moved forward in 2008, there were real concerns as to whether the legislation would cause more problems than it solved.

So, for 2009, the debate will focus on the positive benefits of health information technology for the economic and health care systems, along with an evaluation of whether there is a concrete need for new privacy legislation that may impose significant costs without

providing clear benefits. If privacy provisions are included, this proposed health information technology legislation likely will have an impact not only on the core members of the health care industry who currently are covered by the health care privacy rules, but also

will affect an enormous number of other companies who gather, use and disclose health care data.

Many companies that are not covered by the existing Health Insurance Portability and Accountability Act (HIPAA) rules may find themselves facing significant compliance obligations, while current covered entities may need to re-do their overall HIPAA compliance plan. Accordingly, companies need to be paying close attention to this debate, and should begin preparing for the most significant implications of these proposed changes. Companies also need to factor this debate into their ongoing business planning, particularly for any business efforts related to health care or health information technology.

2. Expanded Enforcement of the Health Care Privacy and Security Rules

While there are substantial questions as to the shape of any future health care privacy legislation, there is virtually no doubt that there will be increased enforcement of the current HIPAA rules in the new administration. There are significant reasons to anticipate new enforcement in the year ahead. First, even in 2008, there started to be some movement toward additional enforcement.

In the health care industry, for example, we saw the first HIPAA penalty, brought against Providence Health Systems. *See* Nahra, “The HIPAA Enforcement Era Begins,” *Privacy in Focus* (August 2008), available at

http://www.wileyrein.com/publication_newsletters.cfm?sp=newsletter&year=2008&ID=10&publication_id=13717&keyword=providence.

We also saw the beginning of a more proactive effort at HIPAA Security Rule compliance, through an organized compliance assessment process. There also are continued calls for additional enforcement, from Congress and a wide range of privacy advocates.

In the Obama administration, enforcement of privacy laws is likely to be a significant priority. Additional enforcement resources for the Federal Trade Commission were a component of the campaign platform. There is a virtual guarantee that the new administration will take a more aggressive approach on enforcement of the HIPAA rules. Moreover, given the potential tension between the incentives for health information technology and the possibility that enhanced privacy protections will lessen any resulting efficiency gains, additional enforcement of the current privacy rules creates a “winwin” possibility for the new administration, since a lack of enforcement of the current rules has been a significant cause of advocate pressure for “better” privacy rules.

Accordingly, we can expect a general increase in HIPAA enforcement activity in 2009. Because of this risk, companies should be paying special attention to any complaints or other reports of problems, and should conduct additional auditing and monitoring of high risk areas.

3. Red Flag and Medical Identity Theft

The Federal Trade Commission’s “red flag” rule, the last substantial rule remaining from the 2004 passage of the Fair and Accurate Credit Transactions (FACT) Act law, stands far and away as the most broadly applicable and challenging new privacy regulation on the horizon.

For health care companies, particularly health care providers, this Rule came out of nowhere, creating widespread concerns across the industry. The outcry from the health care industry (and those in other industries) has resulted in an extension of the compliance date from Nov. 1, 2008 to May 1, 2009, to give companies an additional opportunity to meet their compliance obligations on the “identity theft program” aspects of this rule (other components still have a Nov. 1, 2008 compliance date).

So, why is this rule creating so much concern for health care companies? This rule—as with much of FACT Act—is designed to deal with the problem of identity theft. It requires covered companies to develop an “identity theft red flags program,” designed to evaluate and mitigate identity theft risks. The challenge for the health care industry (and certainly for other industries) involves the covered category of “creditors,” a term that, in the FACT Act statute and the rule itself, seems to have a somewhat restricted definition; the FTC, however, in various

public comments, has taken a surprisingly broad view of its own rule, such that virtually any company—in any industry—who provides services in advance of payment may face obligations under this rule.

For companies in the health care industry, there are two critical issues. First, companies will need to assess whether they meet the definition of “creditors.” (Health insurers and a limited range of others may also need to evaluate whether they are considered “financial institutions” under this rule.) Once a company is considered a “creditor,” then the company must review its business relationships with customers to determine whether there are “covered accounts” that require an identity theft program. Many companies may find that they do not have accounts that trigger identity theft risks—but will need to conduct an evaluation and document their rationale. Other companies will have “covered accounts” and will need to implement a full identity theft red flags program.

Second, companies in the health care industry need to focus on a related issue—the growing problem of medical identity theft. It is clear that there is increasing attention being paid to medical identity theft; at the same time, however, it also seems clear that there are few effective “solutions” in sight. For example, the Department of Health and Human Services Office of the National Coordinator for Health Information Technology and the FTC recently held a “Town Hall” meeting on medical identity theft. The general conclusion of the meeting is that there is ongoing confusion about, and few effective means of fighting, medical identity theft. (A “report and roadmap” from this Town Hall meeting is expected to be published this winter). In addition, the movement toward electronic medical records creates the possibility that the problem with medical identity theft will get worse (although there clearly are some who think that electronic medical records can help solve this problem in the health care industry). As a general matter, the industry concerns with identity theft, whether medical or otherwise, must remain high, as identity theft is the main potential and concrete “harm” that can be suffered as a result of security breaches.

4. *Controlling Access to Information*

With security breaches still in the news on an almost daily basis, health care companies need to pay particularly close attention to one key security issue—inappropriate access to and use of information by corporate insiders. As data has

become more extensive, it is clear that many identity theft cases stem from insider breaches. In addition, as highly publicized incidents have revealed (primarily those at the UCLA Medical Center), at least some employees can be expected to misuse information if given the chance.

These access problems fall into three categories. First, the most publicized incidents have involved celebrities. Health care personnel with access to information have reviewed the medical details of celebrity patients, whether out of curiosity or for more malicious motives (such as selling information to the media). Second, insiders have used their access to information to engage in acts of identity theft or other inappropriate behavior for personal gain—usually involving serious consequences for a small number of people. These incidents don't generate the same kind of publicity as a hacker incident involving millions of records, but these smaller scale incidents are designed specifically to result in identity theft or other identifiable harms. Third, insiders are using their access to review information about friends, family or other personal acquaintances. Again, this motive can be “merely” curiosity or something worse, but, unlike celebrities, there is no meaningful way for companies to isolate the records of these individuals.

Accordingly, as these incidents become more visible, health care companies have been put on notice that they must deal aggressively with this specific problem.

The solution will involve a complicated mixture of activities, focusing on front-end access to information (where it may be difficult to impose meaningful controls, given customer service needs), along with aggressive back-end monitoring and oversight, increased education and significant sanctions for employees who engage in these activities. However, despite this difficulty, companies must take action in this area, and face higher risks of enforcement along with litigation risk in the event that this problem is not corralled.

5. Creative State Laws Involving Health Care Information (As goes New Hampshire, so goes Vermont and . . .)

The last critical issue for the health care industry involves a wild card—the minor trend in several states to restrict the sharing of doctor-focused prescription records. The key issue here is not the impact of this specific category of law, but, more importantly, whether states will use the opportunity presented by this law to impose new restrictions on the use and disclosure of certain kinds of information.

First, the background. New Hampshire passed, in 2006, a law that prohibited the disclosure of certain kinds of prescription data when that data was to be used by pharmaceutical firms to tailor their marketing efforts based on physician prescribing habits. New Hampshire initially focused on privacy concerns as part of its justification for the law, but eventually conceded that its primary goal was to have an impact on health care costs by controlling certain kinds of marketing activities that (the state argued) resulted in higher pharmaceutical costs. The law was immediately challenged by two companies whose primary business involved the sale of this information to pharmaceutical companies. The District Court upheld the challenge. In November, the U.S. Court of Appeals for the First Circuit reversed the judgment, and upheld the New Hampshire law, finding that the law regulated conduct, not speech, and therefore passed constitutional scrutiny. (Similar laws have been passed in Maine and Vermont, and have been proposed in many other states). While much has been written about this case and its impact on health care costs, privacy and the First Amendment, health care companies will want to watch how the states react to the court's decision, first in the narrow area currently regulated by these laws (*e.g.*, will more states pass laws restricting the sale of prescribing data?). More significantly, will states take this opportunity to pass laws regulating the use, disclosure or sale of other kinds of information, based on health care cost control issues or on other public policy goals? With the costs of health care rising at the same time as concerns about privacy and the number of security breaches, we can expect the states to continue to explore means of solving real or perceived health care problems through new compliance obligations for the health care industry. For many companies, particularly if there is no new federal legislation and federal enforcement remains modest, the growing morass of state laws may in fact prove the biggest compliance challenge for the health care industry and its business partners.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, where he specializes in privacy and information security litigation and counseling for the health care industry and others. He is chair of the firm's Privacy Practice, has served on the IAPP Board of Directors and is the editor of Privacy Advisor. He is a Certified Information Privacy Professional. He can be reached at 202.719.7335 or knahra@wileyrein.com.

