The Top Ten Health-Care Privacy and Security Issues to Watch in 2014

BY KIRK J. NAHRA

As the business of health care continues to grow, it also becomes more complicated. While some of the problems change, it is always clear that more data and better data is at the heart of many health-care problems, both in terms of managing actual health and in operating a health-care business. So, it is not at all surprising that data privacy and security remains a critical challenge for any health-care business. The business opportunity from effectively utilizing data coupled with the compliance challenges and regulatory risks from voluminous privacy and security rules creates a compliance and operational perfect storm. Health-care businesses need to learn what they can do with data, how they can gather it, where it can be used and disclosed and how best to protect it.

So, we look ahead to 2014. It is clear that health-care companies (and their wide range of business partners) face an ever growing range of legal requirements, business pressures and operational challenges related to privacy and data security. Chief privacy officers, who exist and participate in senior management at more and more companies, face an increasing array of concrete problems. For many, the biggest issue may not be how to comply with everything (which may not be possible, particularly in a global environment), but rather how to make reasonable sense of this mix of legal, operational and contractual challenges while at the same time effectively running an actual business. What data security and privacy issues should health-care companies and their chief privacy officers, information security officials, compliance officers, general counsels, CEOs and boards of directors be paying the most attention to in 2014?

1. Security Breaches

While there was lots of debate in 2013 about various aspects of the new Health Insurance Portability and Accountability Act rules (stemming from the January 2013 publication of the Health Information Technology omnibus rules), it is clear that the provision with the most immediate and widespread impact has been the new breach notification rule, due to the continuing volume of security breaches. These breaches, large and small, affect every kind of health-care business and their business partners. Without risk of overstatement, the only companies that have not had security breaches of some kind are those who are not looking for them.

Therefore, regulatory details aside, the biggest single challenge for the health-care industry in 2013 is to improve security practices and therefore try to reduce the extent of security breaches plaguing the industry. Obviously, as the massive Target and growing Neiman-Marcus breaches indicate, the health-care industry is not alone on these breach issues. However, the combination of enormously sensitive personal information (where identity theft protections do not necessarily address many of the privacy risks), detailed regulatory notification requirements and detailed security obligations under the HIPAA Security Rule lead to a situation where health-care companies and their business partners need to pay closer attention to their overall security practices, in order to minimize the growing risks related to security breaches.

All health-care companies should undertake a reasonable review of prominent security breaches in 2013 and in recent past years, and evaluate their own security practices with appropriate consideration of where others have faced real problems. It is clear that (1) every business faces realistic risks of security breaches; (2) these breaches result in complicated analysis and regulatory and operational challenges, resulting from contractual entanglements and numerous state laws; and (3) many of these breaches could have been prevented through more effective security practices.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington and a member of the advisory board for BNA’s Health Law Reporter. He provides privacy, data security and cybersecurity advice to companies in a wide range of industries around the country and the world. He can be reached at (202) 719-7335 or knahra@wileyrein.com. Follow him on Twitter @KirkJNahrawork.
2. Insider Access
One key area that requires specific and aggressive focus is the security breach risk due to insider access. We are seeing, in all sorts of industries and particularly in health care, actual breaches resulting from improper behavior by employees who need access to data to do their jobs but then misuse this data for an inappropriate purpose. While this risk can apply to any industry where there are lower level employees, such as those who work in customer service, intake, and data entry, we are seeing a broad spectrum of problems in the health-care industry, ranging from review of medical records of celebrities or other individuals with personal connections to an employee to more malicious situations where employees misuse data to commit identity theft, engage in fraud or otherwise misuse or wrongfully disclose sensitive personal information. As with any kind of security control, companies are faced with the need to take steps up front to reduce risks, and then engage in ongoing activities to monitor and investigate.

In this situation, it often is difficult to properly control front end access to data. Customer service representatives, for example, need access to information about every customer, because they never know who will call. Companies should always look to streamline this access in any way reasonably possible, especially to sensitive data. However, where this is not a complete solution (which will typically be the case), it is crucial to have the tools for both ongoing monitoring and effective investigation in the event of a specific problem. This is a problem that is facing companies in virtually every industry and that is creating actual ongoing risks to personal information, with a large enough number of specific identifiable situation to require aggressive action. 2014 will be a year of improving data control efforts and improving the ability of companies, in real time, to stay on top of employee behavior and act quickly in the event of identifiable concerns.

3. BYOD/Mobile Devices
The other key technology development to watch in 2014 is the ongoing evaluation of how to regulate mobile devices and the related concerns about how companies can effectively manage how their data are used on mobile devices. From a regulation perspective, the effort to regulate mobile devices is caught up in the same swift development of technology, with capabilities well beyond what went before, and a late blooming and continually lagging effort to develop appropriate regulation without stifling economic and technological opportunity. These concerns in the United States are magnified by the regulatory vacuum (which the FTC is trying to fill, along with others) and the nonstop growth in capabilities of mobile devices.

From a corporate perspective, the question of what new regulations are coming for mobile devices probably is less important than the current issue of how to manage the use of these devices. Physicians and many others find mobile devices to be incredibly useful means of quickly and efficiently accessing critical data, for important, time sensitive reasons. They also are useful for quick access for no reason other than pure convenience.

Companies that have not yet developed an appropriate policy for the use of mobile devices have in fact adopted a policy: they are letting data be used and disclosed in largely unpoliced ways. Every company needs to review their overall strategy for mobile devices, whether through a formal “BYOD” [bring your own device] program that provides and supports particular technology, and/or a broader program that addresses how employees and others use mobile devices, with or without the company’s formal support. These devices create a broad range of concerns, ranging from theft of personal and corporate data, overall employee monitoring strategies, new and expanding risks from security breaches, the need to investigate and mitigate security breaches and a wide variety of lesser concerns about how employees use devices to perform their jobs and use and disclose data. While there are few “right” answers, companies must evaluate this issue and develop an approach that appropriately balances the enormous risks with an environment that (1) recognizes the reality that these devices will be used by a growing number of employees and (2) the benefits of a mobile work force.

4. Health-Care Reform
The ongoing saga of the health insurance exchange Web site has dominated the debate about health-care reform for the past several months. We will see, in 2014, the initial feedback about whether the status has improved and whether the exchange program is actually working (or not).

A related issue for the privacy and security community is how the security issues involving the exchange Web site will be resolved. Last summer, before the overall problems with the Web site surfaced, politicians (mainly Republicans) were raising real concerns about the security of the exchange environment. These complaints were put aside when the overall operational issues emerged, but have now been revived. The House recently passed a bill requiring two-day notification for security breaches involving the exchange Web site. The various sets of proposed regulations for the Web site, which for the most part are not yet final, require strict security controls well beyond the details of the HIPAA Security Rule.

So, in 2014, we will watch three related developments. First, what controls and rules will be applied to the Web site itself? Second, how far downstream will these requirements flow (meaning how many participants in exchange related requirements will need to follow the eventual rules)? Third, will the rules for exchanges, such as an exceedingly difficult to meet two-day notification period, apply in any other contexts in the health-care industry?

5. HIPAA Application to Business Associates
Aside from the HITECH breach notification rule, the other major impact of the new HIPAA rules is on the enormous category of “business associates”—the services providers to the health-care industry and those downstream contractors from the service providers. While nothing in the new HITECH rules should be news to this community, since the rules simply implemented the direction of the HITECH law from 2009, the reality is that, in 2014, for the first time, all HIPAA business associates will face the full obligation to follow the HIPAA rules.

This means that all HIPAA business associates, and all downstream subcontractors, must have effective
6. Enforcement

HIPAA enforcement, while growing slightly in recent years, remains quite limited. The Office for Civil Rights, which has acted reasonably and responsibly throughout the HIPAA era, has faced criticism for its enforcement approach in recent years, including recent criticism from the HHS Inspector General. Moreover, with a likely leadership change in 2014, there is the reasonable possibility that the enforcement approach will change.

In general, while there are many predictions that HIPAA enforcement will expand significantly (which seem to arise after every enforcement development), we can expect that there likely will be an evolution toward somewhat increased enforcement, not a revolution that will bring HIPAA enforcement on par with areas like health-care fraud. Nonetheless, because of the obligation to report security breaches, we can expect that the OCR will have numerous opportunities with which to conduct investigations. These investigations are growing in number and expanding in detail with a meaningful burden added to covered entities and business associates, even if there is no formal enforcement at the end. Moreover, the OCR will need to develop a reasonable approach to handling enforcement for business associates now that it has the authority to act against these entities. In addition, state attorneys general remain an important wild card. Despite having broad general authority on consumer protection, specific authority in many states under data breach notification laws and explicit new authority to enforce the HIPAA rules, AG enforcement has been noticeably and surprisingly absent in connection with their HIPAA/HITECH authority. Watch closely for any meaningful enforcement developments, particularly any early cases involving business associates.

7. The FTC’s Role in Health Care

At the same time that the OCR is re-evaluating its enforcement approach, we also are seeing tentative steps by the Federal Trade Commission to enter the world of privacy enforcement for the health-care industry. The FTC’s overall authority as the United States’s “default” regulator for data security practices is facing a direct challenge this year, in two separate proceedings involving Wyndham Hotels and a company called Lab MD.

Both cases directly present the question of whether the FTC is authorized to engage in enforcement activity related to data security independent of specific data security statutory authority, relying on its general consumer protection authority. For the Lab MD case, where Lab MD appears to be a HIPAA covered entity, the enforcement action presents the additional question of whether the FTC can act in a situation where the Department of Health and Human Services has primary enforcement authority under HIPAA. This would be major news for the health-care industry if in fact this is what the FTC is trying to do.

In addition, it is clear that the FTC is exploring its authority in situations where there are “gaps” to privacy and security protection resulting from the structure of the HIPAA rules. Much as it did with the breach notification rule for personal health records (in situations where the PHRs were not regulated under HIPAA), the FTC also is exploring the regulatory environment for mobile devices and mobile applications, including a wide range of applications that utilize health-care data outside the HIPAA structure.

Therefore, we can expect in 2014 that the FTC will become a much more active participant in activity involving the privacy and security of health-care data, expanding both the volume of enforcement and the reach of enforcement into areas of the health-care industry that are not regulated by HIPAA.

8. Health Information Exchanges

While the government’s health insurance exchange site got all the headlines in 2013, the longstanding effort to develop effective health information exchanges continues in 2014. This may be an important make or break year. These information exchanges—a corollary to the HITECH effort to implement electronic health records—provides the unusual possibility of better care and lower cost, through the promise of better and more complete information on a usable timeframe.

However, the development of health information exchanges has gotten bogged down in repetitious state-wide developments (with each state or region reinventing its own wheel), regulatory confusion and pri-
privacy and security complications. These changes are taking longer to build, are more costly than anticipated and, because of the privacy and security rules being applied, likely will not provide better care or more savings.

Watch this year carefully. There is a new head at the Office of the National Coordinator for Health Information Technology, the office that has general federal oversight of these efforts. Absent significant movement on the privacy and security front, along with development of reasonable business plans, we may see 2014 as the year that these efforts collapse. While this would be a shame, as the opportunities are significant, it may make more sense to reduce or eliminate these efforts if they are being built in a way that will not work effectively or achieve the desired goals.

9. De-identification

The “big data” revolution is alive and well in the health-care industry. The enormous volumes of data being generated across the industry create realistic possibilities for better health, more effective research, improved provider protocols and an overall more engaged patient population. At the same time, given privacy concerns, there are real limits on how patient information can be used for these purposes in a meaningful way that will benefit large populations.

Enter the concept of de-identification. The concept, which is spelled out in significant detail in the HIPAA Privacy Rule, is that once patient information has been “de-identified” according to proper protocols, it no longer is traceable to a patient, and privacy concerns essentially disappear. This “de-identified” data can be used for any purpose. While this idea of anonymous or de-identified data has uses in many industries beyond health care, we have seen the most regulatory definition and analysis in health care.

The big data discussion has made clear that there is enormous economic value in de-identified data, along with enormous potential benefits for various important public purposes. The debate in 2014 will focus on the principles behind de-identified data, to examine whether the current HIPAA framework is appropriate, and to review whether there are additional means of developing de-identified data that can achieve important goals without threatening patient privacy.

10. Cybersecurity

The last big privacy and security issue for the health-care industry to watch in 2014 involves cybersecurity. Beginning in 2012 and continuing into 2013, Congress and the Obama Administration have attempted (with little success) to develop a legislative and regulatory approach to cybersecurity issues. While Congress developed a series of legislative proposals, none of these moved forward, leaving the Administration to issue an executive order addressing the development of an overall cybersecurity framework.

The overlaps between “cybersecurity” and “data security” are important for any company to understand. Data security principles—stemming from statutes such as HIPAA (for the health-care industry) and the Gramm-Leach-Bliley Act (for financial services), coupled with the FTC’s enforcement directives on data security (for everybody)—have existed for many years, and have focused on technical, administrative and physical safeguards for effective protection of personal information, whether in paper or electronic form (or any other form). These laws typically were a follow-on corollary to privacy principles dictating how this data can be used and disclosed.

Cybersecurity, by contrast, is less of a “personal information” issue and more of a “protection of our national infrastructure” issue, with undertones of national security. As noted in the executive order, “[t]he cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats.”

This means that cybersecurity concerns address how infrastructure works, how companies work together and with government, and applies to all kinds of information and operations, with no particular focus on personal data. Similarly, the critical industries involved in this executive order include not only industries that already face significant information security regulation (such as health care and financial services), but also other industries that have little personal information and therefore are being regulated or instructed on security issues for the first time (such as manufacturing, utilities and chemicals).

The health-care industry will need to watch these developments carefully. To the extent that the new program focuses on “information sharing,” there may be new areas of obligation and/or opportunity for health-care companies. From the regulatory perspective, the primary goal of the industry seems to be to avoid the need for duplicative, overlapping and/or inconsistent regulation that differs from the key elements of the HIPAA Security Rule. In addition, as many recent “hacking” incidents demonstrate, no company is immune from cybersecurity threats that create risks for both personal and corporate information as well as ongoing business operations.

Conclusions

While 2013 finally brought us the HITECH omnibus rules, 2014 will be a year of progress and challenge for the health-care industry. Any honeymoon period for the new rules is over, whether for covered entities or business associates. And the continuing challenges from security breaches mean that these issues will need to be front and center for any health-care business.

At the same time, there are substantial opportunities for health-care businesses to benefit, both economically and operationally, from better use and analysis of the volumes of data that are created by the industry. The challenge—for privacy officers, security professionals, counsel, compliance leaders and business executives—is to understand the risks and opportunities presented by the complicated regulatory and risk structure, and to use these principles appropriately, efficiently and effectively, to both protect individual privacy interests and facilitate the goals of a better health-care system.