Bloomberg BNA

Privacy and Security Law Report®

2017 Health Privacy

The world of health-care privacy in 2017 is relatively stable, but it will also be confronted with a new Donald Trump administration that will be focused on health-care issues. The author reviews the top issues in health-care privacy that companies will face in 2017.

The Top Ten Health Care Privacy and Security Concerns for 2017

BY KIRK J. NAHRA

As we look into 2017 the world of health-care privacy is in a bit of a strange place (and obviously it isn't alone). On the one hand we have relative stability. The Health Information Technology for Economic and Clinical Health Act (HITECH) rules are fully in place, a broad range of business associates should be in compliance and the enforcement process, while resulting in modestly growing actions, seems reasonable and focused on meaningful problems. At the same time, there are far too many security breaches, new concerns like ransomware are threatening overall health-care operations, and the business developments involving big data and a broad range of new health-care technologies (such as mobile applications and wearables) threaten to break apart the protections of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules and expose the long-existing gaps in individual rights. Placed on top of this is a new administration with no expressed positions whatsoever on any of the key health-care privacy and security issues, creating additional complexity and potential concern. So what are the major issues to watch in this area as we move into 2017?

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, where he specializes in privacy, data security and cybersecurity issues for the health-care are industry and a broad variety of industries across the country and the globe. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

1. The Impact of the New Administration and a Focus on Health-Care Reform

The first area of concern and interest is one we have not had to consider for a while—the impact of a new Donald Trump administration on privacy and security. This topic is of particular importance today for two reasons—the likely repeal of the Accountable Care Act (ACA) and the overall disruption of the broader health-care industry on the one hand, along with the fact that the administration has essentially no expressed positions of any kind on the primary issues facing the health-care industry in connection with privacy and security. Let's take these issues separately.

First, it is clear that the ACA is on its last legs. The repeal of the ACA stands as one of the few expressed positions of the new administration during both the campaign and the post-campaign period. Increasingly, however, there is a recognition that simple repeal is not sufficient or appropriate—there needs to be a replacement of some kind. Much less thought has gone into this replacement, and there is extensive and significant disagreement among the administration and among legislators on appropriate solutions. The impact on privacy and security is indirect—we can expect that the primary focus of attention from the health-care leadership in government will be focused on the repeal of the ACA and development of its replacement for a signifi-

 ISSN 1538-3423

cant part of 2017 and perhaps beyond. This means that far less attention will be given to privacy and security while this assessment is ongoing. Moreover, this effort likely will occupy significant resources, both financially and in staffing.

Second, we have three broad philosophical elements of the new administration that could eventually impact privacy and security. First, there is a recognition of the relative weak state of the country's cybersecurity efforts (with health care simply part of a broader problem). As with many other issues, there is criticism of the status quo without any meaningful solution yet. Nonetheless, that effort to address cybersecurity has its implications for the health-care field. Second, there is a willingness in the new administration to engage in broad surveillance of individuals in connection with national security activities. Again, the health-care industry is not a particular focus, but this effort will drive certain behavior in the administration. The impact may be felt most broadly in connection with international privacy issues, where the more aggressive the U.S. is in connection with surveillance the less flexible we may find the European authorities and others in connection with international data flows. Third, we will watch the impact of two other themes of the new Administration—less government regulation and expenditure of less government money. This likely means no new regulations and somewhat less enforcement, rather than broader changes and a rollback on existing privacy rights, but this is clearly an area to watch carefully.

The privacy implications of the 21st Century Cures Actare modest, but will certainly be worth watching.

2. 21st Century Cures

The lame duck legislative session following the election featured passage of an enormous health-care technology bill called the 21st Century Cures Act. This bill is designed, primarily, to accelerate the approval of new drug products, improve overall health-care research capabilities and provide additional support for various mental health issues. The breadth of the bill is staggering, and the health-care industry (and their lawyers and lobbyists) will be spending the next several months and years dealing with all of the provisions of this massive bill. The privacy implications are modest—but will certainly be worth watching. The worst provisions of this bill for privacy disappeared between the passage of the original bill in the House and the final package. Two provisions in the House bill in particular would have created substantial privacy concerns—a provision that greatly expanded the opportunities to broadly disclose for research activities to virtually anyone with few controls, and the ability of pharmaceutical companies to buy protected health information without financial limits for research and public health purposes. *See generally* Nahra, ''Privacy, Research and the Evolution of Health Care in the 21st Century,'' Bloomberg BNA Medical Research Law & Policy Report (March 18, 2015).

What remained had much less impact—but still can be significant. First, the original House research provision morphed into a new work group to study healthcare research issues involving privacy (and other elements of research). While this will take time, there certainly are areas where the loosely connected areas of HIPAA regulation of research and the Common Rule can be better integrated and streamlined, while still protecting privacy. At the same time, the legislation seemed to ignore the fact that there is a pending rulemaking proceeding designed to do exactly the same thing (although the fate of any pending rulemaking in the new Administration is unclear). The legislation directs the Department of Health and Human Services' Office for Civil Rights (OCR) to make protected health information (PHI) more available to caregivers of mental health patients—although the instructions seem to address issues that already are part of the HIPAA rules and where health care entities—if they struggle at all—struggle to apply the Privacy Rule's reasonable flexibility in specific complicated situations. The major impact of these provisions on HIPAA may be that OCR is instructed to make certain revisions to the Privacy Rule in the future, and that these revisions will require a rulemaking proceeding that could result in a re-opening of the HIPAA rules on a broader basis. *See* Nahra, ''Privacy and Security Impacts from the 21st Century Cures Legislation,'' .

In addition, the 21st Century Cures bill creates a new set of regulatory obligations and reporting activities in connection with meaningful use and interoperability. Despite a broader concern that regulations are impeding technological innovation, the new law directs a new working group to address interoperability and related standards. How this working group will be different from the previous groups addressing these identical topics is not made clear at all in the legislation. But, because of the importance of electronic health records to both health care technology and data analytics more generally, how these issues are addressed will impact a broad array of privacy challenges involving how personal health data can be gathered, analyzed and used.

3. HHS and OCR Leadership

In any new Administration, there is a shuffling of leadership, both in political positions and in other senior leaders who take the opportunity to move on. This year, we will see more of these changes than in many transitions. For privacy and security, the key issue will be the senior leadership of the HHS Office for Civil Rights, as well as the fate of the primary ''day to day'' senior staff who constitute the bulk of the thought leadership and institutional memory of the office. In general, we can expect to see a new Director of the Office for Civil Rights, with a likely ''interim'' leader'' as well. No names have surfaced in the gossipy world of the presidential transition.

  PVLR ISSN 1538-3423

The most important issue for privacy in the transition of administration will be the senior leadership of the Health and Human Services Office for Civil Rights, as well as the fate of the primary "day to day" senior staff.

As for senior staff, we have the rare situation where it will be beneficial for both individuals and the industry to maintain as much of the senior leadership of the office as possible (with a reasonable expectation that this will actually take place). OCR has always been a thoughtful enforcement agency—through two very different administrations so far (at least as far as HIPAA is concerned). They have built up strong knowledge of how the health-care industry operates, and have used that knowledge to evaluate when companies are trying to comply and when they are not. While individual companies may disagree, and the pace of enforcement has picked up somewhat, the health-care industry should generally be happy that there is a responsible and knowledgeable enforcement agency leading this charge. For individuals, while there clearly are some advocates who would like to see more enforcement, the office has operated in a way that has both generally ensured appropriate privacy rights and that the necessary data flow to operate the health-care system has worked effectively. Individuals should care not just about privacy but also about the overall operation of the health-care system. This office has done a strong job of balancing these interests.

The bigger issue with OCR is whether the new administration will force or lead any different directions in enforcement or otherwise. We certainly have seen no discussion of these issues as part of the campaign or the transition. My expectation is that we will see few new rules, little or no rollback of existing rights, and a generally similar enforcement policy going forward, coupled with the budgetary wild card that could reduce enforcement simply through reduced staff.

4. The Federal Trade Commission

A related issue to OCR's future involves the future of the Federal Trade Commission. While OCR has had the lead on HIPAA enforcement, the FTC has a much broader overall role in enforcement and setting policy for privacy and data security enforcement. The FTC has also made clear (although this position is being challenged in court currently) that the FTC can take action under its own standards against entities who are covered by other privacy and security rules, including covered entities and business associates under HIPAA. The appointment of future FTC commissioners is very much a first or second tier priority for the new administration. There is a realistic likelihood that new commissioners will have a distinctly different view on ongoing enforcement in many areas, with the realistic possibility that this will include data security. We also are much more likely to see the FTC take a lesser role in overall thought leadership on privacy and security issues generally (although many of the existing staff will remain in place and will continue to bring their strong expertise to these issues). We will need to watch whether the FTC really does change, and whether OCR (or anyone else) steps in the void that is created.

5. Big Data and Non-HIPAA Health-Care Data

In the privacy world, we are seeing an intensifying debate about how best to regulate big data—whether directly connected to HIPAA or not. This debate is blending with a parallel discussion about the regulation of ''non-HIPAA health care data,'' health-care data that is being generated, used and disclosed by entities that are outside the HIPAA regulatory structure (think web sites, mobile applications and wearables, for example). We are seeing a blurring of HIPAA/Non-HIPAA lines (think wellness programs and the interest of employers in evaluating the health of their workforce). We also are seeing the related developments of HIPAA entities bringing into their systems a broad variety of data that is not normally thought of as ''health'' data, but where data analytics folks at these companies are finding relevant health-care connections (such as income, marital status, number of cars, shopping habits, etc.). This debate has been building—there is a growing consensus that something should be done about these concerns (and the broader concerns about big data as well), but little consensus on what this reform or new regulation should look like. *See generally*, Nahra, ''Moving Toward a New Health Care Privacy Paradigm,'' *Privacy in Focus* (November 2014).

The appointment of future Federal Trade Commission commissioners is very much a first or second tier priority for the new administration.

In 2017, we can expect this debate to slow down and become significantly quieter. I don't think it will go away, but there is little reason to believe that Congress or any relevant regulatory agency will be using 2017 to develop reasonable new regulations or legislative proposals on these points. As with other areas (and as discussed below), this means that there is a significant opportunity for the private sector to build out appropriate standards for this industry, and to develop best practices to fill in the current gaps in the regulatory structure since the likelihood of a regulatory solution clearly has decreased.

6. Research and De-Identification

We also can expect to see an ongoing debate about two inter-related issues—improving research and effective de-identification of data. The research issues under law are complicated—this is a part of the issue that the 21st Century Cures law is trying to address, as well as the ongoing rulemaking about revising the Common Rule. The primary purpose of the Common Rule proposals is to streamline the provisions of the rule, and to permit broader access to data particularly in situations

where privacy issues are minimized. The proposal would have brought the Common Rule more in line with the HIPAA provisions—but not entirely. Now, following almost a year of reviewing comments, the fate of this rule in a new administration is unknown. Nonetheless, there clearly will be more interest going forward in making personal data available for research purposes—coinciding with the goal of getting faster approval of new drugs and treatment protocols.

Whenever there is talk about research, we also hear the discussion about de-identification. De-identification—in theory—presents a win-win for a broad variety of public purposes, including research, public health and overall data analytics. The HIPAA de-identification structure remains the ''gold standard'' for de-identification—the most robust set of practices defining how personal data can be transformed into de-identified data. However, there remains a significant ongoing debate about whether these de-identification practices work in today's environment (where there is a broader array of data available and better technologies available to potentially re-identify).

We are seeing de-identification frameworks being developed both in other segments of the U.S. regulatory structure (including an approach modeled on the FTC de-identification framework for the telecommunications industry), as well as various models around the globe (some of which effectively do not permit de-identification or permit it only in very limited circumstances). There is a challenge for the health-care industry in this area—to demonstrate the value in de-identified information, and to evaluate and educate the public and relevant regulators and advocates on how best to protect the data that has been effectively de-identified. There is significant value here—and some of it is being lost because of bad examples of re-identification (where relevant de-identification frameworks were not followed) or misperceptions about how this data is used. This debate will continue—but it will be important for the health-care industry and the public at large to support strong, risk-based de-identification methods and a broader understanding of how de-identified data can benefit the public at large in a variety of ways.

De-identification—in theory—presents a win-win for a broad variety of public purposes, including research, public health and overall data analytics.

7. International Developments

Health-care entities—particularly health care providers such as physicians and hospitals—often do not focus on international developments. However, the rest of the world is focusing on two related developments—the implementation over the next two years in Europe of the European Union General Data Protection Regulation, covering all personal data across Europe, and the EU-U.S. Privacy Shield program, permitting (for the time being) the transfer of personal data from the EU to the U.S. The health-care industry needs to be thinking about both of these issues as well as the broad and growing morass of other international privacy laws.

For the GDPR (effective in 2018), the new rules require time, attention and resources. The regulation will implement a broader range of controls across Europe, and will have a material impact on individual consents, the use and disclosure of health-care information and the collection of a broad variety of other information that increasingly is being used by health-care entities. Medical research will be more challenging. And companies interested in new products and services will be challenged by the need to comply with this broad regulation (which brings with it the potential for enormous fines).

The Privacy Shield program deals with another component of the international privacy regime—the transfer of personal data from the EU to a country (the U.S.) which—in the EU's mind—does not have adequate safeguards for this personal data. Privacy Shield replaces the Safe Harbor program, which had survived for almost 15 years but was brought down by the new information (the Snowden revelations) about how the U.S. government collected and analyzed personal data. Privacy Shield strengthens the protections for this data, but there is little confidence that the Privacy Shield program is free from future legal challenge, particularly with a new administration that does not seem bound by prior agreements and has an interest in mass data surveillance.

Moreover, significant portions of the health-care industry cannot rely on Privacy Shield as a means of bringing data to the U.S. (although there are other data transfer options as well). Privacy Shield depends on whether a company is subject to the jurisdiction of the Federal Trade Commission. Insurers—generally speaking—are not subject to the FTC and therefore cannot take advantage of Privacy Shield. The same for not-for-profit entities—including many hospitals. So, even if this program stands, it is not a solution for many health-care entities. *See generally* Nahra, ''Impact of the EU-U.S. Privacy Shield on Health-Care Data Transfers,'' Bloomberg BNA Privacy and Security Law Report (Aug. 1, 2016). But, with the business of health care becoming increasingly global—through research, multinational employers, wellness programs, vendors around the world, patients traveling around the globe and a broad variety of creative programs across country lines—these international privacy challenges cannot be ignored.

8. Security Breach Class Action Litigation

On a different path, class action litigation continues to be a major challenge for any company subject to a large data breach. Cases now are brought routinely when there is a large reported breach. While this issue is not limited to the health-care industry, this industry faces significant and enhanced concerns due to both the volume of reported breaches (because of the HITECH notification rules) and the sensitivity of the information involved in many breaches. While the plaintiffs' bar continues to face substantial challenges in proving actual injury (which is a threshold legal issue to get a case started (standing), as well as a meaningful element of causation and damages), they haven't stopped trying. And there are just enough large and small wins to keep these cases coming. We are seeing theories concerning

  PVLR ISSN 1538-3423

''breach of contract'' injury, where there are allegations that a portion of an insurance premium, for example, goes towards data security protections. We are seeing arguments about the ''assumed'' risks associated with sensitive health-care information. We are seeing a new range of claims related generally to weak data security practices. In general, the cases keep coming, even without major victories. It won't take many big wins for the current wall of protection for defendants to come tumbling down.

Class action litigation continues to be a major challenge for any company subject to a large data breach.

We also may see over the next few years an enhanced role for these cases as a substitute privacy regulator—if we see a diminishment of the activity of government regulators. We may see privacy advocates being willing to step into more situations where, today, they might lobby the FTC or HHS to bring an enforcement action. If those agencies slow down in their efforts, we are likely to see policy oriented privacy and security litigation growing as a concern across the health-care industry.

9. Breach Notification Legislation

We have seen half a decade of legislative proposals from Congress about breach notification legislation—to create a consistent federal standard on top of on instead of at least 47 state laws. Many of these proposals are roughly similar, and there is a consensus in Congress on many (but not all) of the key issues. And, with each major breach—Target Corp., Sony Corp., Anthem, Yahoo! Inc., Yahoo! again—many of us think that ''this one or the next one'' will finally be the tipping point for actual legislation. Some of these bills also address general data security standards as well.

So, it will be critical to see if any of the latest breaches—or any new ones in 2017—finally lead Congress to act in this area. A parallel impetus for legislation could be significant court rulings (in contrast to the *Wyndham* litigation) where the FTC's overall authority to act in data security cases is cut back. For the health-care industry, this issue is more important than the industry has realized so far. To date, the health-care industry generally has tried to stay out of this legislative debate—by encouraging a carve-out of HIPAA covered entities and business associates from any new legislation. For data security, this position makes sense—there's no reason to impose another set of data security standards on the same industry (even though the FTC currently believes that it can impose its own standards on health-care entities as well).

This carve-out position is more complicated on data breach notification. Yes, there already is a HIPAA/HITECH standard. And there's generally no need for another rule for the health-care industry. However, most of the federal proposals to date have involved preemption of the existing morass of state laws across the country. If the health-care industry gets carved out of the main federal standard, it won't get the benefit of preemption as well. That's a tricky issue—and one that the industry has not really grappled with so far. Watch this one carefully if legislation moves forward on this point.

10. Managing Compliance with Less Enforcement

Last, there is a real possibility that the relevant enforcement agencies—due to budget cuts, staffing cuts, leadership changes, overall philosophy or distraction from other activities—will significantly reduce enforcement activity. Already, in many situations, there is no realistic threat of enforcement. This may only get worse over the next few years. There also is a reduced likelihood of new legislation addressing some of the concerns that have been raised (and discussed above) about big data and non-HIPAA data and the like.

Therefore, health-care companies and business associates face a real challenge—how to maintain a focus on compliance and good business practices in the wake of a reduced likelihood of enforcement. We see these pressures regularly—will a company push the envelope more? Will marketing have a louder voice while compliance and legal isn't listened to? Will company leaders—facing budget and revenue pressures—be willing to cut more corners, particularly in situations where it is unlikely something bad will become visible? All in all, this will be a challenging time for privacy officials. There will be a need for forceful leadership, and creative strategies to address this likely reduction of attention across companies. Part of this message needs to be that many people are watching even if it isn't tied to enforcement—the news media, consumers, customers and class action lawyers all aren't going away. Nonetheless, privacy officials need to be cognizant of this possibility, and have a realistic plan for addressing potential changes in attitude towards privacy and security compliance.

Conclusions

We are living in interesting times. The commercial privacy and security issues that are so important to the health-care industry and their consumers have not been a focus of any material discussion for the new administration, but there is no doubt that data and the ability to manage and analyze data has never been more important for the health-care industry. Any new health care reform program will require privacy principles. Health-care businesses will not stop using data just because there is less enforcement. So, for any health-care entity (or related service provider) looking to be competitive and responsible in the 21st Century and in the years ahead, the ability to recognize and understand these key developments will be critical. This requires thought, and time, and attention, and planning. It also requires the ability to think beyond the pressures of the day, to develop thoughtful and responsible approaches to the collection, analysis, use and disclosure of the increasingly volume of personal information and related data that is driving success in the health-care industry.