Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | April 2015

Introduction

In this month's issue, Congress continues to move forward with new proposals dealing with privacy and data security. On the House side, Shawn Chang looks at developments related to federal legislation related to data breach notification and overall data security practices. I review a recent initiative within the Energy and Commerce Committee to revise the privacy rules related to health care research. Megan L. Brown, Caroline Rose Van Wie and Kathleen E. Scott look at the new role NIST is playing in the development of privacy policy. Nova J. Daly, Timothy C. Brightbill, and Alexandra E. Landis also explore a recent development in law enforcement action against cyber criminals.

We have a number of upcoming events, including the annual Blue National Summit, the PLUS Professional Risk Symposium, the Medical Informatics World Conference and HITRUST 2015. We'll be covering privacy and data security litigation, likely changes to health care privacy rules for big data, top privacy and security developments for 2015, and insurance coverage issues for privacy and security breaches. Please attend these sessions, or contact me if you would like materials from these events. If you have issues you'd like us to address in future editions of Privacy in Focus—or areas where we can be helpful to you on these issues—please let me know at knahra@wileyrein.com or 202.719.7335. Thank you for reading. ■

Kirk Nahra, Privacy Practice Chair.

ALSO IN THIS ISSUE

2 Bipartisan Data Security and Breach Notification Legislation on Fast Track in the House

4 NIST Plays Increasingly Prominent Role in Privacy Policy

6 New Executive Order Authorizes Sanctions on Cyber Attackers

10 Speeches & Events

Congress, Privacy and Health Care Research

Congress is looking at ways to strengthen privacy and data security protections in various situations, evaluating new legislation related to data security, data breach notification, a consumer bill of rights and educational privacy, among others. Most of these provisions will expand existing protections and create new obligations for a broader range of companies across a wider range of personal data.

But there is also one area where Congress is looking at whether there are means of reducing some of the complexity of existing privacy laws, for overall public benefit. Through an ongoing project called 21st Century Cures, the Energy and Commerce Committee of the U.S. House of Representatives has been developing looking at ways to "accelerate the pace of cures in America," by "looking at the full arc of this process – from the discovery of clues in basic science, to streamlining the drug and device development process, to unleashing the power of digital medicine and social media at the treatment delivery phase." See http://energycommerce.house.gov/cures.

continued on page 7

Bipartisan Data Security and Breach Notification Legislation on Fast Track in the House

On March 25th, the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade marked up a discussion draft of the "Data Security and Breach Notification Act of 2015" with strong support from Subcommittee Republicans, including Chairman Michael Burgess (R-TX), and some Democrats. The markup came a week after the bill's circulation and legislative hearing and less than two months after the Subcommittee held its first hearing for the 114th Congress – an indication of the House leadership's determination to pass a data security and breach notification bill this year.

The discussion draft, authored by Energy and Commerce Committee Vice Chair Marsha Blackburn (R-TN) and Peter Welch (D-VT), represents the first bipartisan legislative effort in the House to enact a federal information security and breach notification framework since 2009. It seeks to balance granting the Federal Trade Commission (FTC) broad and explicit authority over data security and breach notification requirements with ensuring regulatory certainty through a single national standard subject to non-duplicative federal and state enforcement. While the legislative hearing and markup helped identify the divide between Republican and Democrats, and between business interests and privacy advocates, the gaps that were exposed did not seem insurmountable, and members from both sides of the aisle seem willing to entertain further compromises in order to move the legislation through the House on a bipartisan basis.

Key Issues Remain As Legislation Progresses Through Hearing & Subcommittee Markup

As the draft bill moves through the legislative process, the sponsors of the bill consistently described their effort as a carefully crafted, narrow proposal aimed to vest the FTC with the authority to enforce a singular, national standard for securing electronic personal information as well as to notify affected customers and law enforcement authorities when breaches of such information do occur. While the overarching goals of the legislation were generally endorsed by members of the Subcommittee from both sides of the aisle, the debate that ensued at the legislative hearing and markup helped shed light on a number of key issues dividing the parties and key stakeholders. They include:

- *Preemption*: A violation of the data security and breach notification requirements imposed by the draft bill constitutes an unfair or deceptive act or practice subject to enforcement by the FTC and state attorneys general but not through any private right of action. However, similar to the previous bipartisan legislation that passed the House in 2009, the draft bill also preempts state information security laws, although a bracketed provision in the discussion draft seems to indicate that a covered entity's liability under common law is not affected by the bill. During markup, amendments were offered either to remove the preemption of state law, or to remove the bracketed language exempting common law from preemption, indicating wide partisan divide on this issue.

- *Definition of Personal Information:* Many Democrats and public interest stakeholders point out that the bill does not grant the FTC any rulemaking authority to define or modify the term "personal information" that could take into account the emergence of new technologies or evolving expectations of what information should be considered private and thus subject to the bill's definition of "personal information." Opponents of this change argue that the changes to definition should only be made by Congress and giving the FTC too much flexibility through rulemaking undermines the goals of uniformity and predictability. During the markup Congresswoman Yvette Clarke (D-NY) introduced an amendment that would grant the FTC rulemaking authority over the definition of "personal information" but it was defeated in a party-line vote.

- *Third-Party Duty to Notify*: A bipartisan amendment adopted during the markup amends the draft bill to ensure a breached covered entity who handles data for another covered entity whose data was breached should be held responsible for providing the breach notification to the affected individuals while avoiding over-notification. The sponsor of the amendment, Mr. Pompeo, stated that the new language attempts to require all breached entities to have the same legal burden to provide notification, although he also acknowledged that the amendment language is not perfect and more work needs to be done to refine it.

continued on page 3

- *Treatment of FCC Authority:* In creating a single national data breach and notification regime, the sponsors of the bill also sought to remove duplicative enforcement authorities among federal agencies. As a result, the Federal Communications Commission's authority to regulate data security and breach notification practices over common carriers, cable, and satellite providers is eliminated under the bill. Supporters of the provision argue that the FCC's authority is redundant and those regulated entities should be treated no differently than entities in any other covered sectors subject only to the FTC's case-by-case enforcement regime. Opponents, on the other hand, point to the lack of rulemaking authority at the FTC and the loss of certain safeguards for call-related information (such as the numbers called or particular services used such as call forwarding) known as "customer proprietary network information" (CPNI) currently protected by the FCC's rules.

- *Definition of CPNI:* With the elimination of FCC authority over the security of CPNI, the sponsors of the draft bill added a slightly modified definition of CPNI to the list of "personal information" protected by the bill's requirements to ensure there are no unintended gaps in the jurisdictional shift from FCC to the FTC. Opponents of the current language argued, however, that the modified definition of CPNI fails to capture the full scope of the FCC's existing rules. During markup Congressman Bobby Rush (D-IL) introduced an amendment that would add to the definition of "personal information": (1) proprietary information of other carriers, equipment manufacturers, and customers; (2) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service or interconnected VoIP service; (3) personally identifiable information concerning any subscriber to a cable service, satellite service, or any other wire or radio communications service provided using any of the cable or satellite facilities, including any viewing-related information. The amendment was defeated along party lines as well.

- *Privacy versus Data Security:* Throughout the hearing and markup, the chief Democratic sponsor Peter Welch repeatedly emphasized the narrowly tailored nature of the draft proposal. One such example is the sponsors' effort to preserve the FCC's existing authority over privacy matters. Nevertheless, the FCC testified, and several Democrats agreed, during the hearing that it is impossible to separate privacy protection from data security. At the markup, supporters of the legislation argued that privacy-related obligations such as providing notice of personal information collected or to be collected to subscribers, seeking customer consent for disclosure of such information, or allowing subscriber access to such information, are outside the scope of the bill. To further support their point, the sponsors of the bill put in a bracketed provision that could help clarify the preservation of the FCC's existing regulatory power over privacy under the draft bill, should the bracket be removed.

Aside from those key issues, concerns over notification procedure and trigger as well as penalties that may be imposed by state Attorneys General further divided proponents and opponents of the bill.

Next Up: More Negotiations and Markup

Bipartisan legislation carefully negotiated to reflect the middle ground may be disappointing to some interests from both the left and the right, but there remains much to like in the Blackburn-Welch legislation for lawmakers facing pressure at home for visible action in response to near-daily discovery of significant data breaches. The fact that the bill was voice voted out of the Subcommittee was a positive sign that both Democrats and Republicans continue to hold out hope for a broader consensus that may be reached through further negotiation. The bill will likely be marked up by the full Energy and Commerce Committee after Congress returns from its two-week April recess. A floor vote in the House soon after is also likely. The extent to which the two parties can further narrow their differences between now and then will serve as a good indication whether the bill is on track to the President's desk before the end of the year. ■

For more information, please contact:

Shawn H. Chang
202.719.4456
schang@wileyrein.com

NIST Plays Increasingly Prominent Role in Privacy Policy

A technical agency within the Department of Commerce is poised to have a substantial impact on American businesses, through efforts on cybersecurity, data security, and privacy. The National Institute of Standards and Technology has taken a leadership role on technology issues by producing guidance documents that are broad in scope and may influence regulatory agendas and expectations about private sector operations and policies. The private sector should be engaged and watchful, as NIST's work generally is not bound by notice and comment procedures and is rarely subject to judicial review, but could become de facto obligations or expectations for private behavior.

NIST Produces Guidance and Standards by Consensus, Outside Familiar Administrative Law Procedures

NIST, housed within the U.S. Department of Commerce, is a non-regulatory agency. Since its inception in 1901, the agency has been charged with, among other things, "stimulating cooperative work among private industrial organizations in efforts to surmount technological hurdles." NIST's stated mission is to "[t]o promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST has core responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 et seq., Public Law 107-347, "for developing information security standards and guidelines, including minimum requirements for federal information systems."

NIST performs several functions, including developing standards and guidelines for federal information systems; supporting Commerce in facilitating trade; and cooperating in international- and private- efforts to establish standard practices and voluntary, consensus-based standards. Much of NIST's work is spread among six internal research laboratories, including the Information Technology Laboratory (ITL).

In carrying out its functions, NIST publishes a variety of guidance, including handbooks, NIST interagency or internal reports (NISTIRs), special publications, technical notes, and bulletins, among others. "While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted throughout the world." NIST's work has been influential in government procurement policy by, for example, setting security standards for federal contractors and others that store controlled unclassified information (CUI) on their systems.

NIST is a non-regulatory agency and its procedures are often unlike the notice-and-comment procedures of regulatory agencies dictated by the Administrative Procedures Act (APA). In some instances, NIST will follow procedures "modeled after" the APA, but for other work, such as special publications, NIST tends toward the creation of voluntary, consensus-based standards via workshops and meetings rather than formal rulemakings. NIST explains that "standards and guidelines are developed in an open and transparent manner that enlists broad industry and academia expertise from around the world." NIST's development of the Framework for Improving Critical Infrastructure Cybersecurity, discussed below, illustrates the collaborative, workshop-based approach NIST often uses. NIST's substantive work is not often subject to judicial review , though its efforts often are used by other agencies as a standard or benchmark.

The legal impact of NIST guidance and expertise outside the federal government is not well developed, but NIST's work has been used in a variety of ways by courts and litigants. NIST studies and standards have been cited by litigants and analyzed by courts in cases concerning products liability, patent infringement and false advertising.

Litigants also cite NIST guidance in their advocacy. For example, NIST's activities were raised in a key case challenging the Federal Trade Commission's authority to regulate data security. In *FTC v. Wyndham Worldwide Corporation*, a federal court upheld the FTC's authority to bring an enforcement action against a hotel company for failing to use reasonable and appropriate data security practices. There, Wyndham and amici had argued that the FTC could not develop or enforce general data security standards, and cited NIST's then-pending Framework efforts as an example of appropriate standard-setting.

NIST Is a Leader on Data Security, Privacy and Cybersecurity

NIST supports federal network security standards, guidelines, and best practices. Its work feeds into national and international consensus standards,

continued on page 5

and informs state and local governments, along with private industry.

> The framework provides broad cybersecurity guidance using a risk-based approach that can be adapted to the needs of different CI sectors.

Of late, NIST has been taking on an increasingly high profile on issues related to privacy and security, principally through its ITL, which "has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics." The ITL contains the Computer Security Division (CSD), which is responsible for developing standards, guidelines, tests, and metrics for the protection of non-national security federal information and communications infrastructure. CSD includes the Computer Security Resource Center, which facilitates "sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia."

As shown in a recent Annual Report, the CSD is addressing a variety of issues, as diverse as smart-grid cybersecurity, health information technology security, supply chain risk management, cloud computing, and identity verification. NIST is proud of its role in developing "scalable and sustainable information security standards and practices in areas such as cyber-physical and industrial control systems, privacy engineering, security automation, and mobile technologies." These areas are all emerging as major challenges for government and the private sector.

NIST Has Taken a Lead Role in Federal Cybersecurity Efforts, and is Impacting Regulatory Activities Throughout the Federal Government

In February 2013, President Obama issued an Executive Order (EO) on Improving Critical Infrastructure (CI) Cybersecurity. The EO tasked NIST with developing a voluntary cybersecurity framework through an open, consultative process. To implement its responsibilities under the EO, NIST held several open planning sessions for the voluntary cybersecurity framework during 2013-2014. NIST released a proposed framework, on which it accepted comments from interested parties, and finalized the framework in February 2014.

The framework provides broad cybersecurity guidance using a risk-based approach that can be adapted to the needs of different CI sectors. It consists of three parts: the core, profile and implementation tiers. The core is a set of activities and outcomes NIST found applicable to all CI sectors. It is organized into five functions-identify, protect, detect, respond, and recover-that are recognized components of a cybersecurity management lifecycle, along with associated programmatic and technical outcomes. The profile describes an entity's current and target cybersecurity postures, based on business needs. And the implementation tiers characterize an entity's current and intended practices. The framework is not intended to be mandatory or static, and NIST explicitly states that it can updated.

Industry has been generally supportive of NIST's efforts on the cybersecurity framework, in particular the agency's open and collaborative approach, and its commitment to keep the resulting Framework voluntary and non-regulatory.

NIST's cybersecurity activities are influencing initiatives at other government agencies:

- The Food and Drug Administration incorporated the framework into recent guidance related to cybersecurity on medical devices.
- The National Highway Traffic Safety Administration is using the framework to analyze cybersecurity risk management in the automotive sector.
- The Securities and Exchange Commission's Office of Compliance Inspections and Examinations has undertaken a cybersecurity initiative that includes conducting examinations of registered broker-dealers and registered investment advisors focused, among other things, on identification and assessment of cybersecurity risks and protection of networks and information. The inquiry largely tracks the framework.
- The Federal Trade Commission, which has asserted broad authority over private sector data

continued on page 6

NIST Plays Increasingly Prominent Role in Privacy Policy *continued from page 5*

security issues, will consider the framework in its data security activities and investigations.

- The Federal Communications Commission's Communications Security, Reliability, and Interoperability Council is looking at mechanisms to provide macro-level assurance that communications providers are reducing cybersecurity risks through the application of the framework, or an equivalent construct.
- The Department of Defense and the General Services Administration used the framework in its development of cybersecurity guidelines for government acquisition.

A full version of this article is available here.

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Caroline Rose Van Wie
202.719.7550
cvanwie@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

New Executive Order Authorizes Sanctions on Cyber Attackers

To address the increasing and damaging tide of what the Administration considers "malicious cyber-enabled activities" originating from abroad, the President issued an Executive Order on April 1 authorizing the imposition of broad economic sanctions on individuals and entities deemed responsible for or complicit in cyber attacks.

The Executive Order empowers the Secretary of Treasury, in consultation with the Attorney General and Secretary of State, to sanction individuals and entities responsible for cyber-enabled activities that are reasonably likely to result in or have materially contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The Order addresses harm to critical infrastructure, as well as significant disruptions to computers or their networks and the misappropriation of funds or economic resources, personal or financial information, and trade secrets, among others.

While the jurisdiction of the President's Executive Order will likely be reserved for the most significant cyber attacks, the issuance of the Order represents an important expansion of the enforcement tools available to the U.S. government in pursuing the perpetrators of malicious cyber-enabled activities. The Order gives the Administration greater flexibility to deal with harmful cyber attacks, such as the now infamous Sony Pictures hacking incident and also certain state-sponsored cyber attacks, such as the infiltrations of Westinghouse, U.S. Steel, Alcoa, SolarWorld, and the United Steelworkers, which led to the May 2014 Department of Justice indictment of several military officers from China's People's Liberation Army.

Once designated pursuant to the Executive Order, sanctioned parties will appear on the U.S. Department of the Treasury's Office of Foreign Assets Control's (OFAC) Specially Designated Nationals (SDN) List, which features entities whose assets have been frozen and are barred from engaging in commercial transactions with U.S. companies. While no entities have yet been designated under these new sanctions, U.S. persons should continue to monitor the U.S. government prohibited parties lists and remain vigilant in conducting due diligence research and compliance checks.

The text of the President's Executive Order can be found here.

For more information, please contact:

Nova J. Daly
202.719.3282
ndaly@wileyrein.com

Timothy C. Brightbill
202.719.3138
tbrightbill@wileyrein.com

Alexandra E. Landis
202.719.3381
alandis@wileyrein.com

One key area for this proposal involves whether the existing privacy rules for health care research – which stem from both the "Common Rule" and the HIPAA Privacy Rule - can be streamlined to facilitate better research opportunities. The idea is to improve the ability of health care researchers to use and disclose personal data, to facilitate research that will improve overall conditions across the population. While these proposals are still being developed, this idea is an important one with a broad range of implications – can we make changes that will improve important public goals, while still providing appropriate protections for individual privacy? And, are there situations where the population can benefit on a broad scale and therefore minor impacts on privacy protections are worth the trade-off?

As Congress evaluates the 21st Century Cures initiative, some of the key issue to watch are:

- **Generalizable Knowledge**
  The current HIPAA rules permit data analytics where a covered entity uses these analytics for its own benefit, but appears to restrict any external communication of these results, even if no personal data is included in the research results. By restricting use and disclosure of Protected Health Information (PHI) when a covered entity is "Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines" if the "primary purpose" of the activity is "generalizable knowledge," the current rules – without any real explanation - seem to impede communication of research results. These provisions permit the use of data for internal purposes, but seem to prohibit communication of these findings to others. Moreover, in practice, HIPAA covered entities often have been conservative in their view of this language, even though the rule may give more flexibility than current activities seem to indicate (for example, if internal data analysis leads to results that may be worth publishing, this publication was likely not the "primary purpose" of the initial data analysis).

  Congress should fix this restriction, so that useful analytical conclusions can be disclosed on a broader basis, rather than solely used to benefit one entity. First, Congress should consider removing this "generalizable knowledge" restriction. If a hospital conducts "quality assessment and improvement" activities, and learns through its analysis some conclusion of general value to the community or other entities, the HIPAA rules should not prevent communication of these results and conclusions. Since the "use" of the patient data would be the same, there should be no additional privacy concerns in this use. Obviously, whether driven by a minimum necessary analysis or otherwise, specific PHI should not be publicly disclosed in publishing any research findings, but this would be normal behavior in any event (and could certainly be included in any regulatory revision if deemed necessary).

  Second, Congress should look at how this provision is applied in practice – and may simply wish to instruct HHS to make clear (in guidance) what kinds of disclosures are in fact permitted here – by redefining or explaining when "the primary purpose" of an activity is generalizable knowledge, or clarifying that analysis for other elements of this definition (e.g., population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination) can be conducted even if there is generalizable knowledge at the end.

- **Access to Information to Develop Research Protocols**
  It often is difficult for researchers to identify individuals whose data should be included in research studies. Improving this matching process will make research more productive and less expensive, but can certainly come with a privacy cost. While the HIPAA rules provide some flexibility to permit researchers to identify potential research subjects, the current provision is quite limited because it is restricted to situations where a researcher reviews records on the premises of a covered entity. Congress should explore whether there are ways to replicate the protections for this "on-site" review in an electronic environment. For example, if a researcher implements appropriate security practices, reviews records and then returns them, research opportunities can be expanded with a limited impact on any privacy rights (particularly since the same records are subject to review on site). In general, this "pre-research" phase clearly can benefit from additional flexibility.

continued on page 8

- **Encouraging Use of Limited Data Sets and De-Identified Data**
  In connection with research, the HIPAA rules address three categories of data – protected health information, limited data sets and de-identified data. De-identified data is PHI that has been stripped of sufficient individual identifiers (using one of the two methods spelled out in the rules) so that the information is longer "individually identifiable" and therefore is no longer subject to the HIPAA rules. De-identified data has real value in certain research contexts, and both the Committee and HHS should continue to explore means of enhancing the use and disclosure of de-identified health care data.

  There also are substantial opportunities in connection with limited data sets. Limited data sets are a carefully defined term in the HIPAA rules, meaning information that has been almost de-identified, but by inclusion of certain limited data fields, remains PHI. Under the current rules, covered entities can use and disclose limited data sets for research and certain other purposes, as long as there is an appropriate data use agreement in place. The Committee should explore (or instruct HHS to explore) whether there are additional means (including additional remuneration) of encouraging covered entities to disclose limited data sets for research purposes.

- **Expand Use of Data Use Agreements Outside of Limited Data Set Context**
  The data use agreement concept also can be expanded. A data use agreement mirrors – in most ways – the terms of a business associate agreement. Most researchers are acting on their own, rather than as a service provider to a covered entity, and therefore are not business associates under the HIPAA rules. Currently, researchers can only receive a limited data set using this data use agreement. The Committee should encourage HHS to implement a broader disclosure rule that permits broader PHI to be disclosed to researchers consistent with the protections of a data use agreement. This data use agreement, for example, would provide appropriate protections for any "pre-research" evaluation of potential research subjects. This expansion should be explored as a viable means of expanding research opportunities, particularly for "data research," without raising many of the privacy and security concerns that accompany many other modifications to the HIPAA rules.

- **Improved Guidance on Privacy Waivers**
  As a general matter, while the HIPAA rules on research have been in place since 2003, there remains significant confusion about them. Most researchers are neither covered entities nor business associates, so they may have little understanding of how these rules work. In the research community, there often is little focus on how best to obtain such a waiver, little attention to the steps that should lead to a waiver, and little incentive for institutional review boards to approve waivers without clear protections. Everyone involved in this process – covered entities, researchers, IRBs and Privacy Review Boards – all would benefit from additional guidance from HHS on when a waiver of patient authorization is appropriate. HHS could consider whether there are "safe harbors" where a waiver would be presumed or automatic (e.g., data research only in a controlled and secure environment). For Congress, rather than try to define these details, Congress should direct HHS to issue additional guidance and/or clarifications to make this waiver process more efficient and to improve the ability of researchers to obtain and use data (for the benefit of the overall healthcare system) where privacy risks are small or otherwise controlled.

- **Authorization Issues**
  Various HHS components have been reviewing patient authorization requirements in connection with research, to streamline the elements that are required to permit PHI to be used in research. The Committee draft includes an element establishing a "one time" authorization for PHI generally. This idea makes sense, and should move forward in the legislation. This step gives patients more effective control of their data, if they wish to permit use of their data for research activities on a broad basis.

- **Harmonization of HIPAA, the Common Rule and Other Research Principles**
  It is clear that one of the key challenges for health care research in the United States (without even considering international opportunities and complications) is that there are multiple rules and approaches that must be addressed and understood for many projects. As with many other areas of privacy law, the mere existence of multiple overlapping, inconsistent and ambiguous regulatory requirements creates its own problems and clearly

continued on page 9

About the Practice

With the explosion in information technology, privacy and information security issues have risen to the forefront of legal developments affecting every business. New and emerging privacy and security laws produce challenges for any business that collects, utilizes, or distributes information about individuals. Wide media attention, tort litigation brought by private parties (often as class actions), and governmental enforcement actions have made privacy a major risk area for businesses. Wiley Rein's goal is to provide companies with a thorough understanding of the current and potential rules on privacy and security and to provide legal solutions that harmonize businesses' needs with emerging information access restrictions.

Wiley Rein's Privacy Practice, named one of the best privacy consultancies by *Computerworld* magazine and recognized as a national leader in Privacy and Data Security law by *Chambers USA*, includes more than 20 attorneys who provide experience in more than a dozen substantive areas. The Group is chaired by Kirk J. Nahra, who is ranked among the top tier of attorneys nationwide in Privacy and Data Security by *Chambers*, and is considered by sources to be in "the top echelon" of data privacy lawyers and "highly knowledgeable and sensitive to both costs and delivering results on time" (2013). The directory notes that the Practice "has been stellar in giving spot-on advice that combines the legal perspective with the practical implications" (2014).

We represent domestic and international businesses, as well as major trade associations, in many industries including communications, Internet, health care and insurance, financial services, online advertising, biometrics, information security, manufacturing, retailing, franchising, and distribution. In recommending the Practice, *Chambers* reports that sources say "They are very strong because they have the subject matter expertise combined with proactiveness" (2014), and say that Kirk Nahra is "the guy you need to call" (2014). ■

Congress, Privacy and Health Care Research *continued from page 8*

increases overall transaction costs, to the detriment of both the industry and patients. The current legislative proposal does not address this overall confusion and tension. Moreover, it likely is not an appropriate or feasible legislative step to make legislative changes to an entire series of current regulations to attempt to bring them all together under a single framework. Instead, the Energy and Commerce Committee should consider directing the Department of Health and Human Services – which oversees many of these frameworks through various different sub-agencies – to study this question of harmonization and provide to Congress a report on how a more integrated and harmonious framework can be developed, to permit research projects to be developed in a more streamlined and efficient manner. Today's rules create impediments to research based on confusion, without addressing the potential benefits of these projects. HHS should be instructed to evaluate how these confusion-oriented and duplicative impediments can be reduced or eliminated, through development of a more efficient and clearer overall process for developing beneficial research projects.

Conclusions

It is clear that there are substantial benefits to better and more efficient research. The goal – for Congress and HHS – should be to facilitate more opportunities for research, provide complete opportunities for patients to agree for their data to be included in research and to provide clear guidance on how the existing rules can be used most effectively. Additional improvements also can be made to the structure of the rules to improve consistency and reduce tensions and ambiguities. On a broader level, the debate about health care research also focuses key attention on the public benefits of better research, and the opportunities tor e-evaluate the balance between aggressive protection of privacy interests at the potential expense of broader societal benefits, particularly where there are opportunities to have better research without sacrificing privacy interests.

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

SPEECHES & EVENTS

Privacy Litigation and Enforcement for Health Plans

Kirk J. Nahra
2015 Blue National Summit
April 20, 2015 | Phoenix, AZ

The New Paradigm for Health Care Privacy & Why It Matters to You

Kirk J. Nahra
2015 Blue National Summit
April 21, 2015 | Phoenix, AZ

Top Ten Healthcare Privacy and Security Developments to Watch

Kirk J. Nahra
2015 Blue National Summit
April 21, 2015 | Phoenix, AZ

The Wild Wild West: Cyber Risks, Data Security and Privacy

Kirk J. Nahra
2015 PLUS Professional Risk Symposium
April 28, 2015 | Atlanta, GA

The New Paradigm for Health Care Privacy

Kirk J. Nahra, Moderator
Third Annual Medical Informatics World Conference 2015
May 4, 2015 | Boston, MA

The Coming New World Order on Health Care Privacy and Data Security

Kirk J. Nahra, Speaker
Third Annual Medical Informatics World Conference 2015
May 5, 2015 | Boston, MA

The Evolving World of Privacy and Security – What's it mean to you?

Kirk J. Nahra, Panelist
HITRUST 2015
May 21, 2015 | Grapevine, TX

Contributing Authors

Timothy C. Brightbill	202.719.3138	tbrightbill@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Shawn H. Chang	202.719.4456	schang@wileyrein.com
Nova J. Daly	202.719.3282	ndaly@wileyrein.com
Alexandra E. Landis	202.719.3381	alandis@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Caroline Rose Van Wie	202.719.7550	cvanwie@wileyrein.com