Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | November 2018

As privacy and security law expands into a broader range of areas, our issue this month addresses some of this array of topics. Steve Claeys writes about the impact of the U.S.-Mexico-Canada Agreement (USMCA) on data privacy issues. Lee Goodman continues his analysis of the First Amendment right to political privacy. I evaluate the potential for Health Insurance Portability and Accountability Act (HIPAA) changes as part of the Administration's regulatory agenda. Lastly, Michael Diakiwski reviews the upcoming Federal Trade Commission (FTC) Hearings on Privacy and Data Security Enforcement as part of a broader set of FTC activities. As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or **knahra@wileyrein.com**. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

Will We See HIPAA Changes Anytime Soon?

By Kirk J. Nahra

While many industries have been focused on reducing the regulatory burdens imposed upon their participants, the health care industry – which certainly has important areas of regulatory concern – has not been pushing for changes to the general Health Insurance Portability and Accountability Act (HIPAA) structure or for reductions in HIPAA burdens. At the same time, there has been little change to the HIPAA rules since the implementation of the final HITECH omnibus rule issued in January 2013.

This may be changing somewhat – although both the fact and scope of future changes is very much up in the air. As part of its semi-annual regulatory agenda (and supplemented by various speeches and presentations from senior Office for Civil Rights (OCR) leadership), the U.S. Department of Health and Human Services (HHS) announced that it will be moving forward to start various processes to consider certain changes to the HIPAA rules. (Note that I will

continued on page 2

be participating in an event in December hosted by the Future of Privacy Forum on "The HIPAA Privacy Rule 15 Years Later: What's Next?" For information on this event, please see **https://privacycalendar.org/event/hipaa-privacy-rule-15-years-later-whats-next-workshop/?instance_id=1318)**. These potential changes are driven by three motivating factors. First, there still remain several holdover changes from the HITECH statute (passed in 2009). Second, there are potential changes driven by a concern (primarily from the Administration) about reducing regulatory burdens. Third, and perhaps most important in terms of the potential for broader change, there is an ongoing concern that the HIPAA rules as currently structured may create impediments to improved coordinated care, driven by concerns about the opioid crisis and more broadly.

Funds Sharing

Some of the steps being considered are remaining holdovers from the HITECH law. For a variety of reasons, these provisions were not adopted as part of the "omnibus" rule that implemented most of the HITECH requirements.

For example, HHS has indicated that it will be requesting public input for how OCR may share funds collected from HIPAA enforcement actions with affected individuals. This step is required by the HITECH statute. However, despite this announcement, this step may still be a long time in coming, as OCR has announced similar plans at least 12 previous times, all without any actual activity. There is no obvious reason why this year should be any different.

This issue is a challenging one, and there is likely to be a lot of controversy about any proposal. Defining "harm" in the context of a regulatory enforcement proceeding is extremely difficult and will put additional pressure on OCR's already tight resources. There also will be a concern from industry that this provision will lead to higher demands for monetary payments – to "compensate" these individuals while also permitting OCR to obtain significant amounts for its own purposes. In addition, courts across the country continue to struggle with definitions of "harm" in class action litigation. There likely will be reasonable concerns that any OCR definition of harm will spill over to a litigation context.

Accounting Rule

Next (and perhaps more significant depending on the result), HHS OCR continues to evaluate the HITECH requirement to modify the HIPAA accounting rule. The accounting rule has been one of the primary "individual rights" in the Privacy Rule since it first went into effect. As part of the HITECH statute, Congress directed that certain changes be made to the accounting rule, primarily to broaden the scope of the rule in connection with electronic health records. While the statutory language created meaningful concerns in the health care industry, these concerns exploded when HHS – in May 2011 – issued a proposed rule on the accounting provisions. This proposal was met with widespread and virtually universal criticism. At this point, HHS seems to be starting over with the accounting rule, having formally abandoned the earlier proposal.

The health care industry will be firmly supportive of this abandonment. The earlier accounting rule proposal wildly

continued on page 11

Impact of the United States-Mexico-Canada Agreement on Data Privacy Rules

By Stephen J. Claeys

On September 30, the United States, Mexico and Canada reached agreement on the United States-Mexico-Canada Agreement (USMCA) to replace the North American Free Trade Agreement (NAFTA). The agreement also significantly updates NAFTA with new rules, including rules regarding data privacy. The Administration intends to use the USMCA as a template for future potential trade agreements with Japan, the United Kingdom, the European Union (EU), and others. Therefore, the new rules in the USMCA potentially will impact not just doing business in Canada and Mexico, but potentially also in other significant markets.

The USMCA data privacy rules are included in the digital trade chapter. This is an important update to NAFTA, which does not contain any rules on data privacy or digital trade in general. This also means that the data privacy rules should be viewed along with the overall objectives of the USMCA's digital trade chapter to reduce cross-border data flow barriers and limit domestic data storage requirements. Thus, while the USMCA's data privacy rules are not a trade-off per se for liberalizing cross-border data flows, they certainly help address concerns about the impact on individuals of allowing such data flows.

The USMCA requires the United States, Canada, and Mexico to maintain a legal framework to protect personal data but leaves the content and enforceability of such laws up to each country. Specifically, the agreement creates only two hard commitments: 1) to adopt or maintain a legal framework that protects the personal information of the users of digital trade; and 2) to publish information on the personal information protections the country provides to users of digital trade, including how individuals can pursue remedies and businesses can comply with any legal requirements.

While the remaining data privacy rules are not obligatory, importantly they encourage the United States, Canada, and Mexico to have their respective privacy regimes reflect a common set of principles and be compatible. These principles include limitation on collection and use of data; security safeguards; transparency; individual participation; and accountability. Moreover, each country is urged to consider principles and guidelines of relevant international bodies, such as the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the Organisation for Economic Co-operation and Development (OECD). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Finally, the United States, Canada, and Mexico jointly recognize in the agreement that compliance with data privacy protections and any restrictions on cross-border flows of personal information should be necessary and proportionate to the risks presented and should not discriminate against parties from the other USMCA countries.

Regardless of the above, the USMCA specifically recognizes that there are different legal approaches to protecting personal information, including comprehensive privacy, personal information, or personal data protection laws; sector-specific laws covering privacy; or laws that provide for the enforcement of voluntary private sector undertakings. However, the United States,

continued on page 4

FTC Sets Hearings on Privacy and Data Security Enforcement

By Michael L. Diakiwski

On October 26, the Federal Trade Commission (FTC or Commission) announced it will address privacy and data security enforcement as part of its ongoing "Hearings on Competition and Consumer Protection in the 21st Century."[1] It will hold four days of hearings examining "the FTC's authority to deter unfair and deceptive conduct in data security and privacy matters."[2] A Wiley Rein Client Alert on the hearings and their importance to the tech sector is available **here**.

The FTC's primary enforcement authority is found in Section 5 of the FTC Act and prohibits unfair or deceptive practices in the marketplace.[3] This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge from the development of new technologies and business models. Under this authority, the FTC has brought dozens of enforcement cases against companies that have engaged in practices that the agency determined failed to adequately protect consumers' data.[4]

The hearings on data security are slated for December 11-12, 2018, and will examine private-sector incentives to invest in data security and the FTC's data security enforcement program, among other topics.[5] Related to consumer privacy, the FTC has scheduled hearings for February 12-13, 2019.[6] According to the Commission, it will be the first comprehensive re-examination of its approach to consumer privacy since 2012. Through December 21, 2018, the FTC staff is seeking comment on what the privacy hearings should cover specifically.

Wiley Rein has actively engaged with the FTC's privacy and data security initiatives. In

continued on page 5

Impact of the United States-Mexico-Canada Agreement on Data Privacy Rules

continued from page 3

Canada, and Mexico agreed to promote compatibility and exchange information on their respective mechanisms. The USMCA specifically identifies the APEC Cross-Border Privacy Rules system as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

The USMCA's data privacy rules appear to be supported by most stakeholders and commenters. While some may wish that the rules were stricter, they recognize that the USMCA's rules go farther than those in the Trans-Pacific Partnership agreement in requiring data protection and promoting compatibility. There is particular support for the USMCA allowing different approaches to data privacy while also promoting the APEC Cross-Border Privacy Rules.

The next steps are for the three countries to sign the USMCA, likely by the end of November, and then for Congress to pass legislation to approve and implement the agreement. Congressional consideration of the USMCA probably will not occur until next year. The combination of Congress' full schedule after the midterm elections and various procedural and reporting requirements that apply to USMCA legislation prevent it from being voted on this year. ■

For more information, please contact:

Stephen J. Claeys
202.719.3540
sclaeys@wileyrein.com

continued from page 4

September, as part of its **Outlook on Cyber** series, the firm hosted Bilal Sayeed, Director of the FTC's Office of Policy Planning, and James Cooper, Deputy Director for Economic Analysis in the FTC's Bureau of Consumer Protection. Both FTC officials play key roles in driving the hearings. At the Outlook event, the FTC encouraged stakeholders to submit comments with tangible, data-driven analysis on the topics of privacy and cyber harm.

The Commission is seeking new thinking on these subjects and will weigh stakeholder feedback with an open mind. As Chairman Joe Simons said in announcing this effort, the FTC plans to engage in "serious reflection and evaluation" so that the agency is "better able to promote competition and innovation, protect consumers, and shape the law, so that free markets continue to thrive."[7]

Industry and stakeholder comments on both data security and privacy may be submitted through March 13, 2019. ■

For more information, please contact:

Michael L. Diakiwski
202.719.7031
mdiakiwski@wileyrein.com

[1]See FTC, *"Hearings on Competition and Consumer Protection in the 21st Century,"* available at: **https://www.ftc.gov/policy/hearings-competition-consumer-protection**.

[2]See FTC, *"FTC Announces Sessions on Consumer Privacy and Data Security As Part of its Hearings on Competition and Consumer Protection in the 21st Century"* (Oct. 26, 2018) available at: **https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its**.

[3]15 U.S.C. § 45.

[4]See FTC, Privacy & Data Security Update: 2017, 2 (Jan. 18, 2018), available at: **https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf**.

[5]See FTC, *"FTC Hearing on Competition and Consumer Protection in the 21st Century – December 2018,"* available at: **https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018**.

[6]See FTC, *"FTC Hearing on Competition and Consumer Protection in the 21st Century – February 2019,"* available at: **https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019**.

[7]See FTC, *"FTC Announces Hearings on Competition and Consumer Protection in the 21st Century"* (Jun. 20, 2018) available at: **https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st?utm_source=slider**.

The First Amendment Right to Political Privacy
Chapter 2 – The New Deal Witch Hunt

By Lee E. Goodman

Introduction

The opening chapter in this series revealed the seed of First Amendment protection for anonymous political speech and association in the 1940s Red Scare cases of *Barsky v. United States* and the "Hollywood Ten" in the U.S. Court of Appeals for the District of Columbia Circuit. In *Barsky*, Judge E. Barrett Prettyman authored the 2-1 majority opinion elevating Congress' right to investigate American communists over any vague "private right" to political belief and association. That opinion was met by Judge Edgerton's dissent, an early articulation of the First Amendment right to political privacy. In 1950, the Supreme Court of the United States chose not to wade into the debate and denied review. Although the Edgerton Dissent did not protect the Hollywood Ten, the legal concept reverberated as a powerful jurisprudential idea. And the Edgerton Dissent would impress judges in future cases – including Judge E. Barrett Prettyman and a number of Supreme Court Justices.

The New Dealers Investigate Conservatives, Too

After the Supreme Court denied certiorari to the Hollywood Ten, congressional investigations of communists resumed and indeed intensified. At the House Un-American Activities Committee (HUAC), conservative Georgia Democrat John Wood had assumed the chairmanship. In the U.S. Senate, a new Republican Senator from Wisconsin named Joseph McCarthy entered the enterprise, focused principally on communist spies within the federal government.

While conservatives of both political parties investigated progressives from Hollywood to the U.S. Department of State, New Deal liberals in Congress exercised their subpoena powers to investigate conservative antagonists, too, proving that the use of government subpoenas and compelled exposure was an ecumenical political weapon.

New Deal Democrats had won control of the House of Representatives in the 1950 election, and in 1951 the House Select Committee on Lobbying Activities, also known as the Buchanan Committee (after the name of its Chairman, Frank Buchanan, a New Deal Democrat from Pennsylvania), turned its investigative sights on the political activities of Edward Rumely, an American anti-communist and free marketer, an outspoken opponent of New Deal economic policy, and Executive Secretary of the Committee for Constitutional Government, Inc. (CCG) a conservative free market advocacy organization.

The Buchanan Committee purported to investigate the CCG not in the name of national security, as in the case of communists, but in the name of good government and the regulation of money, influence, and lobbying.

The CCG was formed in 1937 for the purpose of resisting New Deal thought and policies.[1] It was very active, for example, in opposing President Roosevelt's court-packing plan in 1938. According to historian David Beito, the organization "in mobilizing against 'court packing' (a term it did much to popularize), led perhaps the first successful political offensive against the New Deal and pioneered the use of direct mail to gain

continued on page 7

continued from page 6

supporters. Over the next seven years, the group distributed more than 82 million pieces of literature declaiming such policies as expanded government medical insurance, public housing, and labor legislation."[2]

The CCG's outspoken advocacy made it a perennial target of Democratic investigative interest. In 1938, Democratic Senator Sherman Minton of Indiana announced that the Senate Select Committee on Lobbying would conduct an investigation into the CCG's advocacy activities. In addition to dispatching staffers to rummage through CCG records at its headquarters, Minton obtained Rumely's tax returns from the U.S. Department of the Treasury. Like communist sympathizers, the CCG would remain "subject to almost constant investigation over the next twelve years" by New Deal officials in government and liberal organizations.[3] CCG's liberal critics accused it of being pro-Nazi and seditious.[4]

Since the early 1940s, one of the CCG's principal communications strategies had been to influence public opinion through the publication and distribution of pointed ideological books.[5] The CCG sold books in bulk to ideological supporters who would direct the CCG to distribute the books to certain audiences. In 1950 and 1951, CCG was distributing nearly a million copies of the book *The Road Ahead: America's Creeping Revolution* by John Flynn. The book "warned that leftist pressure groups were edging the United States into socialism through a Fabian strategy of incremental change."[6]

Democrats developed a good government reform plan and promised to scrutinize – exclusively – pro-business lobbies. The Buchanan Committee "sent out a probing questionnaire to more than 170 businesses and organizations," defining lobbying in the broadest possible terms to include efforts to influence public opinion, and inquiring about the funding of such efforts.[7]

In June 1950, the Buchanan Committee subpoenaed Rumely to, among other things, name the people or organizations that purchased books and pamphlets from CCG.[8] Rumely answered 25 questions, but declined to disclose the names of the people and organizations that purchased books and pamphlets.[9] "I am perfectly willing to give everything except one thing," Rumely testified before the Buchanan Committee on June 28, 1950. "I haven't withheld anything, except the names of the buyers of our books. Those you can't have."[10] The Committee was persistent and continued to press him to disclose the names. Again on June 29,[11] Rumely repeated:

> "I certainly refuse to disclose those names – not contemptuously, but respectfully, because I feel it is my duty to uphold the fundamental principles of the Bill of Rights. I think there is no power to require of a publisher the names of the people who buy his products, and that you are exceeding your right."[12]

For that Rumely was prosecuted and convicted of contempt of Congress in the U.S. District Court for the District of Columbia. Rumely appealed.

Prettyman Turns for Rumely and the CCG

So, in 1952, the First Amendment right to private association was back before the U.S. Court of Appeals for the District of Columbia and Judge E. Barrett Prettyman in a case styled *Rumely v. United States*.[13]

continued on page 8

continued from page 7

Rumely asserted two defenses similar to the arguments asserted unsuccessfully by the Hollywood Ten. First, he argued the Buchanan Committee violated the First Amendment by forcing him to disclose the names of book purchasers. Second, he contended that the Buchanan Committee was acting beyond its legitimate writ to investigate "lobbying" when it inquired about the CCG's efforts to influence public opinion by communicating directly with citizens.[14] The government argued that the Buchanan Committee was well within its rights to investigate "subterfuges to evade the Federal Regulation of Lobbying Act, i.e., to mask contributions as purchases," because the Lobbying Act required lobbying organizations like CCG to disclose their donors.[15]

The appeal came before a panel of the Court of Appeals that included Judge Prettyman, who had rejected similar First Amendment arguments asserted by communists in *Barsky* four years earlier. Neither Judge Edgerton nor Judge Clark (author of the Hollywood Ten decision) was on the panel.

In a 2 to 1 opinion,[16] a newly enlightened Judge Prettyman (perhaps channeling Judge Edgerton), ruled that the publication, sale, and distribution of books discussing national issues was protected speech under the First Amendment. He rejected the argument that the names were pertinent to the Committee's investigation "since the Committee might wish to question those persons as to possible subterfuges," finding that "so slim a semblance of pertinency is not enough to justify inquisition violative of the First Amendment."[17] Sounding more like the Edgerton Dissent (though not acknowledging it), Judge Prettyman found that publicizing the names and addresses of book purchasers "is a realistic interference with the publication and sale of those writings," and that "the realistic effect of public embarrassment is a powerful interference with the free expression of views."[18]

Judge Prettyman moved from his prior opinion in *Barsky* in two distinct ways. First, in somewhat revisionist style, he interpreted *Barsky*, with clarity missing in the original opinion, to have ruled that public inquiry and disclosure of names "was an impingement upon free speech."[19] Second, the judge distinguished *Barsky* on the grounds that it allowed the inquisition into the names of communists for the "public necessity" of national security.[20]

> In that case it was shown that the President and other responsible Government officials had, with supporting evidentiary data, represented to the Congress that Communism and the Communists are, in the current world situation, potential threats to the security of this country. For that reason, and for that reason alone, we held that Congress had the power, and a duty, to inquire into Communism and the Communists.

The CCG inquisition, by contrast, implicated less weighty governmental interests that did not justify intrusion into the private First Amendment rights of the CCG.

Judge Prettyman took a decidedly narrow view of government's legitimate inquiry into "the public distribution of books and the formation of public opinion through the processes of information and persuasion," which he characterized as "the healthy essence of the democratic process."[21]

continued on page 9

continued from page 8

Congress had no power to investigate or regulate the right of people to share ideas among themselves under the power to regulate "lobbying."[22] And further, Judge Prettyman found that "anonymous donations of printed material to Congressmen appear to be a danger too insignificant to support abridgement of freedoms of speech, press and religion," for Congressmen could choose to read the materials or not.[23]

The similarities between the Prettyman decision in *Rumely* and the Edgerton Dissent in *Barsky* are noteworthy. Finally, Judge Prettyman had come around to the First Amendment paradigm articulated by Judge Edgerton.

The Supreme Court Weighs In – A Jurisprudential Opening

The government appealed to the Supreme Court, which took up the case in late 1952. The Court, in a decision by Justice Felix Frankfurter, a Roosevelt New Deal appointee, affirmed the Court of Appeals, though on narrower grounds. While recognizing the First Amendment right articulated by Judge Prettyman, the Court scrupulously invoked the doctrine of constitutional avoidance to parse the meaning of "lobbying activities" in the Congressional resolution authorizing the Buchanan Committee's investigation and concluded the phrase did not include "all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiations of influence which they may exert upon the ultimate legislative process."[24]

Justices Douglas and Black, who had dissented on the denial of certiorari in the Hollywood Ten case, issued a concurring opinion giving full-throated protection for the obvious First Amendment rights at stake. "Of necessity," Justice Douglas wrote, "I come then to the constitutional questions."[25]

> Like the publishers of newspapers, magazines, or books, this publisher bids for the minds of men in the market place of ideas…. A requirement that a publisher disclose the identity of those who buy his books, pamphlets, or papers is indeed the beginning of surveillance of the press. True, no legal sanction is involved here. Congress has imposed no tax, established no board of censors, instituted no licensing system. But the potential restraint is equally severe. The finger of government leveled against the press is ominous. Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears.[26]

The concurring justices observed that government cannot do by inquiry, investigation, or public harassment that which it cannot do by direct legislation.[27]

Aftermath

According to historian Beito, although Edward Rumely won in the courts, sustained "Buchananism"[28] and multiple investigations and legal proceedings had the effect of draining the CCG's resources, stigmatizing the organization, chasing off donors, and ultimately undermining the organization.[29]

Rumely was more successful jurisprudentially. Justices Douglas and Black had introduced the First Amendment right to anonymous financial support for a political speaker, in this case an ideological book publisher, into Supreme Court case law. And

continued on page 10

continued from page 9

although Justice Frankfurter had avoided an explicit First Amendment holding, his opinion (joined by four other justices) nodded to the First Amendment argument. Unfortunately for the communists in Hollywood, their efforts to influence public opinion through films, unlike CCG's publication and dissemination of books to shape public opinion against New Deal philosophy, did not receive the same First Amendment protection against government inquiry and public disclosure. But Justice Frankfurter would revisit the First Amendment right to anonymous political association four years later in the case of Marxian economist and political activist Paul Sweezy, in an opinion announced on June 17, 1957 – a day J. Edgar Hoover called "Red Monday," the subject of our next chapter in this series. ■

For more information on the First Amendment right of political privacy, please contact:

Lee E. Goodman
202.719.7378
lgoodman@wileyrein.com

[1]The organization originally was named the Committee to Uphold Constitutional Government in 1937. It changed its name to Committee for Constitutional Government in 1941.

[2]David Beito & Marcus Witcher, "New Deal Witch Hunt" – The Buchanan Committee Investigation of the Committee for Constitutional Government, The Independent Review Vol. 21 No. 1 (Summer 2016) at p. 47-48 (hereinafter cited as "Beito").

[3]Id. at 50-52, citing Joanne Dunnebecke, The Crusade for Individual Liberty: The Committee for Constitutional Government 1937-1958 (M.A. Thesis, University of Wyoming, 1987).

[4]*Id.* at 55.

[5]The books included The Road Ahead by John T. Flynn, Labor Monopolies and Freedom by John W. Scoville, Compulsory Medical Care and the Welfare State by Melchior Palyi, Why The Taft-Hartley Law by Irving McCann, and hundreds of thousands of copies of the U.S. Constitution and the Bill of Rights.

[6]Beito at 56.

[7]*Id.* at 57, citing Congressional Record, House, June 15, 1950, 8676.

[8]*Rumely v. United States,* 197 F.2d 166, 168 (D.C. Cir. 1952) (the Select Committee's subpoena demanded disclosure of "(1) the name and address of each person from whom a total of $1,000 or more has been received by the Committee during the period, January 1, 1947, to May 1, 1950, for any purpose, including but not limited to (a) receipts from the sale of books, pamphlets, and other literature, (b) contributions, (c) loans; (2) as to each such person the amount, date, and purpose of each payment which formed a part of the total of $1,000 or more.").

[9]*Id.* at 170.

[10]*Id.*

[11]*Id.* So intensive was the Buchanan Committee's investigation into CCG that it subpoenaed Edward Rumely twice, and he appeared for testimony on June 6, 27, 28 and 29, 1950. Id. at 170.

[12]*Id.*

[13]197 U.S. 166 (D.C. Cir. 1952).

[14]*Id.* at 173.

[15]*Id.* at 171.

[16]Judge Prettyman was joined by Judge James Proctor. Judge David L. Bazelon, who had been appointed to the bench two years earlier, dissented on the basis of Barsky and more pointedly on the rationale, heard often today, that

> The First Amendment is not violated merely because disclosure might conceivably deter some from implementing their political views with financial support…. The Buchanan Committee has restricted no one in the free exercise of his rights to say what he pleases, or to assemble and to petition for any purpose…. The CCG's right to promote, retard and otherwise influence legislation is inviolate. But that right does not extend to protection from disclosure of its financial support.

197 F.2d at 187 (Bazelon dissenting). All three judges had been appointed by President Truman.

[17]197 F.2d at 172.

[18]*Id.* at 174.

[19]*Id.* at 174.

[20]*Id.* at 173.

[21]*Id.* at 174.

[22]*Id.* at 175.

[23]*Id.* at 176.

[24]*United States v. Rumely,* 345 U.S. 41, 46 (1953).

[25]*Id.* at 56 (Douglas *concurring*).

[26]*Id.* at 56-57 (Douglas *concurring*).

[27]*Id.* at 58 ((Douglas *concurring*).

[28]Beito at p. 68, *citing* Frank Chodorov, Is Lobbying Honest?, Freeman 3, No 21 (July 13, 1953) at p. 742).

[29]*Id.*

misconstrued the state of feasible technology for tracking uses and disclosures of health care information, resulting in a proposal that was both not realistically feasible and exceedingly burdensome. HHS identified few specific patient interests that were furthered by the proposal, and the interests that were identified either were already addressed through privacy notices or were more appropriately and directly addressed by privacy investigations. In addition, HHS failed to assess the risks to health care company employees that would be created by providing information about them to patients, in addition to failing to analyze other unintended consequences of providing details about internal operations of health care facilities.

Overall, as I said at the time:

> My conclusion is that this NPRM is fundamentally misguided and should be withdrawn – it relies on an unreasonable interpretation of the HIPAA Security Rule, fails to reflect the technological reality of today's health care environment, and mistakenly presumes (even if its assumptions were correct) that creation of this access report will impose little burden, all to support (in a surprisingly untargeted way) an ill-defined and relatively unjustifiable patient interest in learning specific details about the internal activities of health care companies. See generally, Nahra, "The HIPAA Accounting NPRM and the Future of Health Care Privacy," *BNA Health IT Law & Industry Report* (July 4, 2011), available (https://www.wileyrein.com/media/publication/338_BNA--Nahra--07.04.11.pdf.)

Any future proposal on the accounting rule will stem from the broad "Request for Information" that HHS is planning to issue to cover these various topics. It will be critical for HIPAA-covered entities and business associates to carefully think through the issues presented by the accounting rule, so that they can help HHS get to a much more balanced approach on the HITECH requirements for the accounting rule.

General Regulatory Burden Provisions

In its notice, HHS indicated that it will be seeking public comment "on whether there are provisions of the HIPAA Rules ... [that] otherwise impose regulatory burdens that may impede the transformation to value-based health care without providing commensurate privacy or security protections for patients' protected health information and while maintaining patients' ability to control the use or disclosure of their PHI and to access PHI." This includes "patients' acknowledgment of receipt of a providers' notice of privacy practices," where the Administration is reviewing options to "change the requirement that health care providers make a good faith effort to obtain from individuals a written acknowledgment of receipt of the provider's notice of privacy practices, and if not obtained, to document its good faith efforts and the reason the acknowledgment was not obtained." While we have not yet seen a lot of discussion about the interests served by this proposal, HHS seems to be of the view that this obligation is burdensome for health care providers without much benefit for patients. In addition (without additional detail and as part of the HITECH requirements as well), HHS will be seeking comment on "the minimum necessary standard/requirement." While

continued on page 12

HHS is seeking comment on these specific points, the notice seems to indicate that it will also seek general comments from the public about ways to reduce overall regulatory burdens (even though this has not been a meaningful concern for the health care industry, in general).

Broader Information Sharing

Perhaps the most interesting issue involves potential means to expand the ability of health care providers (and perhaps others) to share health care information for appropriate purposes. As part of the HHS notice, HHS stated that:

> With over 60,000 individuals dying of opioid overdoses in 2016 and others suffering from addiction to the opiates, HHS issued a declaration of emergency to recognize a nationwide opioid epidemic. HIPAA permits providers and other covered entities to disclose protected health information about an individual to families, caregivers and other relevant parties in circumstances related to opioid overdose and addiction. Despite this permission and HHS guidance clarifying HIPAA, HHS continues to receive anecdotal evidence that providers and other covered entities are reluctant to share an opioid patient's health information with family or other caregivers.

While concerns over the opioid crisis are driving a significant component of the health care privacy debate in Washington these days, it is not at all clear that changes to the HIPAA rules are in fact needed (as HHS notes). Nonetheless, HHS will be seeking comment on a proposal that "seeks to encourage covered entities to share protected health information with family members, caregivers, and others in a position to avert threats of harm to health and safety when necessary to promote the health and recovery of those struggling with opioid addiction." While HHS will consider whether it can address this issue through "additional guidance," it also has stated that:

> HIPAA continues to be cited as a barrier to sharing protected health information in crisis situations, despite extensive existing guidance and outreach efforts. Without regulatory changes, it is not clear that additional guidance would be effective in clarifying the ability to share protected health information in such situations. Revising the Privacy Rule would be a more effective and permanent vehicle for achieving the desired policy, and would provide additional Good Samaritan safe harbor protections to health care providers who share protected health information when trying to help patients.

While additional flexibility in the rule may provide health care providers with additional encouragement to disclose information in specific contexts, HHS notes the potential risk that "the impact of these amendments, taken together, could be expected to discourage individuals from seeking care based on concerns that their PHI may be disclosed against their wishes."

Accordingly, HHS will be seeking comment on "whether there are provisions of the HIPAA Rules which present barriers that limit or discourage coordinated care and case management among hospitals, physicians (and other providers), payors, and patients," including: (a) creation of a safe harbor for good faith disclosures of PHI for purposes of

continued on page 13

continued from page 12

care coordination or case management; and (b) disclosures of protected health information without a patient's authorization for treatment, payment, and health care operations. It will be interesting to see how HHS tries to motivate this additional sharing (beyond the flexibility built into the privacy rule today), without moving towards a mandatory disclosure regime that would be very different from HIPAA's overall approach today.

Conclusion

The health care industry can expect to see one or more requests for information on these topics. Most of these topics, at this point, are quite abstract, and seem still a long way away from an actual proposed rule or any meaningful implementation. Nonetheless, it will be important for the health care industry and other stakeholders to evaluate how these changes could be implemented, and what effects we could see from the potential changes being considered. ■

For additional information, please contact:

Kirk J. Nahra

202.719.7335
knahra@wileyrein.com

Events & Speeches

Critical Challenges in Privacy and Security Law

Institute for Health Plan Counsel

Kirk J. Nahra, Speaker

November 2, 2018 | Chicago, IL

Is Our Critical Infrastructure Cyber Resistant?

NIST Cybersecurity Risk Management Conference 2018

Megan L. Brown, Speaker,
Matthew J. Gardner, Speaker

November 7, 2018 | Baltimore, MD

"The HIPAA Privacy Rule 15 Years Later: What's Next?" Workshop

Future of Privacy Forum

Kirk J. Nahra, Panelist

December 4, 2018 | Washington, DC

Mastering the Evolving Law of Data Analytics

AHIMA Data Institute: Making Information Meaningful

Kirk J. Nahra, Speaker

December 6, 2018 | Las Vegas, NV

"The Exchange" Data Privacy and Cybersecurity Forum

Today's General Counsel Institute

Matthew J. Gardner, Co-Chair

December 13, 2018 | Los Angeles, CA

"The Path Towards a New and Complete Consumer Health Privacy and Security Regulatory Structure."

28th National HIPAA Summit

Kirk J. Nahra, Speaker

March 5, 2019 | Washington, DC

"Regulatory Challenges For Digital Health – The Emerging Law and Filling The Gaps,"

ABA Health Law Section Emerging Issues Conference

Kirk J. Nahra, Panelist

March 13-16, 2019 | Orlando, FL

Privacy Boot Camp

IAPP 2019 Global Privacy Summit

Kirk J. Nahra, Speaker

May 1, 2019 | Washington, DC

Contributing Authors

Stephen J. Claeys	202.719.7425	sclaeys@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com