NCVHS
National Committee on Vital and Health Statistics

September 16, 2015

The Honorable Sylvia M. Burwell
Secretary, Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: **Recommendations on the financial services industry and § 1179 of HIPAA**

Dear Madam Secretary,

As chair of the National Committee on Vital and Health Statistics (NCVHS), your advisory committee on health data, statistics, and the Health Insurance Portability and Accountability Act (HIPAA), I write to transmit findings and recommendations of the Committee regarding § 1179 of HIPAA.[1]

Section 1179 creates a limited exemption from the requirements of HIPAA for financial institutions engaged in certain transactions. Accordingly, HIPAA and its implementing rules do not apply to financial institutions in custody of protected health information (PHI) when they are "engaged in authorizing, processing, clearing, settling, billing, transferring, or collecting payments."

The NCVHS Subcommittee on Privacy, Confidentiality and Security held hearings in Washington DC on May 6-7, 2015, to gather information about the interpretation and implementation of HIPAA § 1179. The hearing sought to understand the evolving practices of banks and financial service businesses in relation to health care billing and related activities, how § 1179 is being understood in the industry, and whether there are problems with how the current HIPAA Privacy and Security Rules are functioning with respect to this industry.

The Committee approached this hearing as a listening session, and we benefitted greatly from those who provided testimony and participated in a collaborative discussion of the complex and rapidly changing ecosystem regarding the use of patient information and health data by banking and financial service businesses.

[1] Pub. L. 104–191, 110 Stat. 1936 (1996).

Based on this hearing, a prior NCVHS letter on this same topic in 2004,[2] discussions with outside experts, and written submissions to the record, we offer four recommendations that are discussed in detail below.

Recommendation 1. HHS should issue guidance addressing banking and financial service business activities that are exempt by Section 1179. Such guidance should include an explication of

- **banking and financial services that are subject to business associate (BA) agreements;**
- **other provisions of HIPAA, such as standards for "minimum necessary" disclosures, relevant to evolving health-related banking and finance; and**
- **compliance obligations of covered entities when contracting with banks and financial service businesses.**

Recommendation 2. HHS should develop education focusing on the business associate relationship between a bank or financial service business and a covered entity and disseminate education to both the finance and healthcare sectors. The goals of the education and outreach should be to foster cross-sector collaboration to advance the shared goals of advancing privacy and security of PHI.

NCVHS last reviewed the effect of HIPAA on banking in 2004 shortly after the compliance date of the HIPAA Privacy Rule.[3] HIPAA law and regulations have evolved in the intervening decade, as have the ways in which banks and the broader financial sector use personal health data in their products and services. Our 2004 letter observed that the "vast majority" of banking services performed by financial institutions involving health information came within the § 1179 exemption. The letter noted that a small number of banks offer health clearinghouse services and are thus covered entities. Other services may require the use of business associate agreements. Our letter observed that neither the Gramm-Leach-Bliley Act (GLBA) nor the Fair and Accurate Credit Transactions Act (FACTA) amendments to the Fair Credit Reporting Act, banking privacy statutes already in place at that time, provided safeguards meeting HIPAA standards.

We concluded our 2004 letter by making two recommendations: first, that HHS clarify the scope of the § 1179 exemption; and second, that covered entities

[2] Letter from John R. Lumpkin, Chairman, National Committee on Vital and Health Statistics, to Tommy G. Thompson, Secretary, U.S. Dept. of Health & Human Svcs., (June 17, 2004), *available at* http://www.ncvhs.hhs.gov/recommendations-reports-presentations/june-17-2004-letter-to-the-secretary-recommendations-on-the-effect-of-the-privacy-rule-in-banking/.

[3] All covered entities, except "small health plans," were required to come into compliance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Parts A and E), on April 14, 2003. Small health plans had until April 14, 2004, to comply.

sharing PHI with financial institutions do so under BA agreements for any services beyond claims payment and electronic funds transfer clearly covered under § 1179 or when there is any question about the applicability of the exemption. Our May 2015 hearing revealed that HHS has not made these clarifications, even as the complexity of the relationship between the health and financial sectors has increased.

Our 2004 letter also observed that financial institutions' activities with respect to processing PHI were evolving and diversifying rapidly. In the decade since 2004, the range and volume of activities of banks and financial service businesses involving PHI have continued to expand. In addition to the Automated Clearing House (ACH) Network and basic Electronic Data Interchange (EDI) payment functions that were clearly the focus of the § 1179 exemption, the financial services industry is performing an expanding range of services in support of covered entities including:

- Collection and processing of accounts receivables
- Cash management
- Health claims submission services
- Electronic remittance services
- Insurance eligibility services
- Patient payment plans
- Patient payment portals
- Patient billing services
- Credit card operations including virtual card payments to providers
- Revenue cycle management, and
- Administering medical savings accounts (MSAs), health savings accounts (HSAs), health reimbursement arrangements (HRAs), and flexible spending accounts (FSAs).

This significantly expanded range of services illustrates why it is so important that the scope of the § 1179 exemptions be more clearly described in today's context.

A number of banks and financial service businesses have leveraged their competencies by filling growing demands for data management and processing. The testimony at our May 2015 hearing made it clear that the regulatory obligations of banks or financial service businesses for privacy and security depend on which services are offered, the nature of the relationship of the parties to the service, the information being handled, and the way that information is processed in the course of providing these services.

Our May hearing also revealed the importance of the introduction of the business associate structure in the HIPAA Security and Privacy Rules. The BA concept was not in the original HIPAA statute. HHS developed the concept as a way of including within the HIPAA regulations the activities of covered entities

that involved sharing PHI with third parties. In 2010, the Health Information Technology for Economic and Clinical Health (HITECH) Act codified the concept of a BA, applied many of the Privacy and Security Rule obligations to BAs, and gave BAs their own breach notification responsibilities. The HITECH Act also applied these requirements to entities performing BA functions even if they were not operating subject to BA agreements with a covered entity. Thus, today, banks and financial service businesses handling PHI outside the scope of the § 1179 exemption may be held accountable as BAs even when they have not entered into a formal BA agreement. These statutory changes and their accompanying regulations further highlight the importance of clear understanding of the § 1179 exemption.

In 2014, the ACH Network using healthcare EFT standard transactions handled nearly150 billion health claims reimbursement payments. In these transactions, banks separate the "dollars" from the "data" as they process a payment. Funds transfers and "remittance advice" are transmitted under separate cover and re-associated by a provider to reconcile which payments are for which patients and for which procedures. While this process precludes inadvertent disclosure or inappropriate use of PHI, the Committee heard testimony that it leads to inefficiencies in transmitting payments from health plans to providers.

Credit and debit card payments for insurance and health care services are becoming more commonplace and seem to be exempt under § 1179. Health care payment card transactions are also considered exempt under § 1179 because the cards generally do not include PHI other than as necessary to effectuate the transaction.[4] Virtual card payment is a more common business-to-business transaction in which payers transfer funds to providers.

Testimony highlighted providers' challenges of fully managing the expanded network of BAs. In large organizations it may be difficult to track when the relationship with banks and financial service businesses changes from exempt services to those requiring a BA agreement. Covered entities must assess whether a particular bank or financial service business is capable of carrying out the responsibilities of a BA, and, given the complexity of banks and other financial service businesses, this can be challenging. Covered entities are obligated under HIPAA to oversee and monitor business associates, a growing challenge given resource constraints and the complexity of these relationships.

HIPAA covered entities have had an uneven record of providing thorough and consistent assessments of the BA practices of banks and financial service businesses. On the opposite side, the Committee identified confusion among

[4] Card transactions are covered by the Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338 (1999), which requires a notice to consumers about the practices of the card issuer; and the Payment Card Industry security standards, a private self-regulatory regime to which most card issuers adhere.

those who provided testimony about certain provisions of HIPAA regarding banking obligations. For example, the HIPAA Privacy Rule requires that when a HIPAA-covered entity or BA uses or discloses PHI, or when it requests PHI from another covered entity or BA, the covered entity or BA must make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[5] The meaning and application of the minimum necessary standards was not entirely clear to all of the hearing participants, and that is not surprising as HHS has extended the minimum necessary obligations to BAs and subcontractors, but has yet to issue guidance on what constitutes a "minimum necessary" disclosure.

Thus our May 2015 hearing reinforced the importance of issuing guidance for the industry about the § 1179 exemption. It also revealed the need for educational materials addressing when BA relationships are created and at what point BA agreements should be executed.

Recommendation 3. NCVHS recommends that HHS work with the appropriate federal financial regulatory agencies to develop an analysis comparing federal privacy and security regulations of HIPAA with those of the banking and financial services sector. The analysis would be useful in preparing the guidance and educational materials described in Recommendations 1 and 2, and would support the conversation between the health information sector and the financial services sector described in Recommendation 4.

The May 2015 hearing revealed that historically the top 50 originators generate at least 80% of the ACH volume, but for 2014, the top 50 originators generated about 90% of the ACH Network volume and have taken steps to organize for compliance with HIPAA.[6] Often they provide services through a subsidiary, separating HIPAA-covered business lines from traditional banking. These "firewalls" ensure that access to PHI is strictly controlled and handled in accordance with applicable regulations while not burdening the banking functions with HIPAA compliance. Panelists reported that these sophisticated institutions are well aware of their obligations under HIPAA, and have the policies and practices in place to comply. There are many thousands of smaller and local banks for which a full § 1179 picture was not available to the Committee. It would be helpful for these banks and the health care providers in their communities to have more information with regard to any possible obligations.

[5] HHS HIPAA Privacy Rule, 45 C.F.R. § 164.502(b).

[6] NACHA, the Electronic Payments Association, 2015 Quarterly Network Statistics and List of Top 50 ACH-Originating and Receiving Financial Institutions available at https://www.nacha.org/ach-network/timeline.

New financial services businesses such as PayPal, Apple Pay, and Google Checkout, which were not represented at the hearing, nevertheless appear, so far, to be limited to carrying out straightforward consumer-driven payment transactions and, therefore, exempt under § 1179.[7]

In testimony, financial sector representatives advised that their sector is governed by laws and regulations that are at least as rigorous as HIPAA. If so, compliance with the HIPAA Privacy and Security Rules might be redundant and unnecessary. However, the Committee's judgment is that it would be helpful to have an authoritative side-by-side analysis.

When compared to the HIPAA Privacy and Security Rules,[8] the privacy provisions of banking laws such as GLBA, FACTA and others have different purposes and perspectives. For example, GLBA requires covered financial institutions to provide a notice of practices and an opportunity to opt out. FACTA prohibits a financial institution from using health information for underwriting loans.

The HIPAA Privacy Rule, in contrast, sets minimum standards and provides rights beyond opting out. Under the HIPAA Privacy Rule, individuals have the right to access and correct their records or to view a list of disclosures. GLBA does not. The financial sector participants at the May hearing asserted that these greater rights would be impossible for banks to administer given the volume of electronic transactions. It may also be important to explore the impact of this gap on consumers and their interest, if any, in augmenting their rights in this way. However, bank-owned health care clearinghouses should not operate under a different set of rules than health care clearinghouses owned by other entities. Unless clearly a § 1179 exemption applies, NCVHS holds that personal health information be consistently protected regardless of what industry is processing or managing it.[9]

Moreover, HIPAA-covered entities lack a thorough understanding of the privacy and security obligations imposed on financial institutions by non-HIPAA banking regulations. Thus, the important differences in the privacy and security requirements of the healthcare and financial industries are not well known or

[7] Other non-financial services provided by these companies, such as cloud storage with Amazon, or Gmail with Google, are likely to give rise to a requirement for a Business Associate agreement.

[8] 45 CFR Part 160 and Part 164, Subparts A and E (HIPAA Privacy Rule) or 45 CFR

[9] For example, in a 2006 letter to then Secretary Michael O. Leavitt, NCVHS recommended that, "HHS should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools."

understood by either industry. In light of the growing dependence of the health sector on banks and financial services businesses to support the management of health administrative systems, improved cross-industry awareness of privacy and security practices would be highly beneficial. In the current climate, the value of a more detailed analysis of comparative privacy regulations by experts in both fields cannot be overstated.

Recommendation 4. HHS, working with industry groups such as Workgroup for Electronic Data Interchange (WEDI), should convene a public-private cross-industry panel of experts representing the health and financial services sectors that meets on a regular basis to identify opportunities for collaboration and cross-learning between these sectors.

The range of healthcare administrative services provided by the financial sector will continue to expand and evolve. The May hearings identified a number of issues that would benefit from more consistent cross-industry communication and collaboration.

For example, consumer-centered health is rapidly changing the relationship from a two-way provider-to-payer relationship to a three-way consumer-to-provider-to-payer structure. For example, consumers may authorize and own a health savings account into which they set aside monies for health expenses at a tax-advantaged rate. The presumption is that the bank is not subject to HIPAA or the HITECH Act. However, if the bank or financial service business uses the PHI on behalf of the group health plan to administer the HSA, it may be functioning as a BA without benefit of a formal business associate agreement. As consumers take on greater responsibility for curating and controlling their own health and medical information and paying for a greater share of their healthcare services, historical business-to-business relationships are being reshaped.

Cybersecurity is an example of an issue facing both industries with healthcare experiencing a marked increase in breaches due to an increase in cybersecurity incidents. The Committee heard testimony that the cybersecurity practices of banks are generally more sophisticated than they are for healthcare under the current Security Rule. Banking may have cybersecurity practices from which the health sector could benefit and protocols that could help prevent and accelerate the effective response of healthcare organizations to security incidents.

The use of aggregate data or “big data” analytics poses another issue only partially addressed by HIPAA. The current Privacy Rule permits BAs to aggregate data from different covered entities, including data about the same patients in both sets. The range of policy questions, however, are growing and cross industry debate would be helpful in addressing questions such as: the limits on how these data might be used or monetized; whether aggregate data

may be used to derive predictive algorithms that guide future health coverage or payment decisions; the rights of consumers in this regard; the impact of available methodologies for linking records and de-identifying the data, and the possibilities for integrating data from HIPAA covered entities with data derived from other sources.

Our hearing revealed there would be value in formalizing regular cross-industry dialogue of evolving privacy and security policy issues and best practices. For this reason, the Committee recommends that HHS convene a cross-industry panel to study policy issues and work collaboratively to advance privacy and security of PHI.

The complexity of data flows within healthcare and between industries is increasing. Information governance and management challenges often outpace regulations or are outside the scope of current regulations. The Committee was reminded at the May hearing about the importance of principle-based information practices: all stewards of personal health information must imbed strong privacy and security standards into their products and services. It is in this spirit of learning that the Committee offers these recommendations.

We look forward to discussing these proposed actions with you and HHS staff members, and to working with the Department to help carry them out.

Sincerely,

Walter G. Suarez, M.D., M.P.H., Chairperson,
National Committee on Vital and Health Statistics

Cc: HHS Data Council Co-Chairs