

1  
2  
3  
4  
5  
6  
7  
8  
9

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

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

11  
12       Dear Secretary Burwell:

13  
14       As chair of the National Committee on Vital and Health Statistics (NCVHS), your  
15       advisory committee on health data, statistics, and the Health Insurance Portability and  
16       Accountability Act (HIPAA), I write to transmit findings and recommendations of the  
17       Committee regarding § 1179 of HIPAA.<sup>1</sup>

18  
19       Section 1179 creates a limited exemption from the requirements of HIPAA for financial  
20       institutions engaged in certain transactions. HIPAA and its implementing rules do not  
21       apply to financial institutions in custody of protected health information (PHI) when they  
22       are “engaged in authorizing, processing, clearing, settling, billing, transferring, or  
23       collecting payments.”

24  
25       NCVHS’s Subcommittee on Privacy, Confidentiality and Security held hearings in  
26       Washington DC on May 6-7, 2015, to gather information about the interpretation and  
27       implementation of HIPAA § 1179. The hearing sought to understand the evolving  
28       practices of banks and financial service businesses in relation to health care billing and  
29       related activities, how § 1179 is being understood in the industry, and whether there are

---

<sup>1</sup> [Pub. L. 104–191](#), 110 [Stat. 1936](#) (1996).

30 problems with how the current HIPAA Privacy and Security Rules are functioning with  
31 respect to this industry.

32

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

37 Based on this hearing, a prior NCVHS letter on this same topic in 2004,<sup>2</sup> discussions with  
38 outside experts, and written submissions to the record, we offer four recommendations  
39 that are discussed in detail below.

40

41 **Recommendation 1. HHS should issue guidance clarifying which banking and**  
42 **financial service business activities are covered by the Section 1179 exemption. Such**  
43 **guidance should include an explication of**

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

50

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

56

---

<sup>2</sup> 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/>.

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

68 We concluded our 2004 letter by making two recommendations: first, that HHS clarify  
69 the scope of the § 1179 exemption; and second, that covered entities sharing PHI with  
70 financial institutions do so under BA agreements for any services beyond claims payment  
71 and electronic funds transfer clearly covered under § 1179 or when there is any question  
72 about the applicability of the exemption. Our 2015 hearing indicated that HHS has not  
73 made these clarifications, even as the complexity of the relationship between the health  
74 and financial sectors has increased.

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

- 82
- Collection and processing of accounts receivables

---

<sup>3</sup> 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.

- 83 • Cash management
- 84 • Health claims submission services
- 85 • Electronic remittance services
- 86 • Insurance eligibility services
- 87 • Patient payment plans
- 88 • Patient payment portals
- 89 • Patient billing services
- 90 • Credit card operations including virtual card payments to providers
- 91 • Revenue cycle management, and
- 92 • Administering medical savings accounts (MSAs), health savings accounts
- 93 (HSAs), health reimbursement arrangements (HRAs), and flexible spending
- 94 accounts (FSAs).

95

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

98

99 A number of banks and financial service businesses have leveraged their competencies by  
100 filling growing demands for data management and processing. The testimony at our May  
101 2015 hearing made it clear that the regulatory obligations of banks or financial service  
102 businesses for privacy and security depend on which services are offered, the nature of  
103 the relationship of the parties to the service, the information being handled, and the way  
104 that information is processed in the course of providing these services.

105

106 Our May hearing also revealed the importance of the introduction of the business  
107 associate structure in the HIPAA Security and Privacy Rules. The BA concept was not in  
108 the original HIPAA statute. HHS developed the concept as a way of including within the  
109 HIPAA regulations the activities of covered entities that involved sharing PHI with third  
110 parties. In 2010, the Health Information Technology for Economic and Clinical Health  
111 (HITECH) Act codified the concept of a BA, applied many of the Privacy and Security  
112 Rule obligations to BAs, and gave BAs their own breach notification responsibilities. The  
113 HITECH Act also applied these requirements to entities performing BA functions even if

114 they were not operating subject to BA agreements with a covered entity. Thus, today,  
115 banks and financial service businesses handling PHI outside the scope of the § 1179  
116 exemption may be held accountable as BAs even when they have not entered into a  
117 formal BA agreement. These statutory changes and their accompanying regulations  
118 further highlight the importance of clear understanding of the scope of the § 1179  
119 exemption.

120

121 In 2014, the ACH Network using healthcare EFT standard transactions handled  
122 nearly 150 billion health claims reimbursement payments. In these transactions, banks  
123 separate the “dollars” from the “data” as they process a payment. Funds transfers and  
124 “remittance advice” are transmitted under separate cover and re-associated by a provider  
125 to reconcile which payments are for which patients and for which procedures. While this  
126 process precludes inadvertent disclosure or inappropriate use of PHI, the Committee  
127 heard testimony that it leads to inefficiencies in transmitting payments from health plans  
128 to providers.

129

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

136

137 Testimony highlighted providers’ challenges of fully managing the expanded network of  
138 BAs. In large organizations it may be difficult to track when the relationship with banks  
139 and financial service businesses changes from exempt services to those requiring a BA  
140 agreement. Covered entities must assess whether a particular banks or financial service  
141 business is capable of carrying out the responsibilities of a BA, and, given the complexity

---

<sup>4</sup> 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.

142 of banks and other financial service businesses, this can be challenging. Covered entities  
143 are obligated under HIPAA to oversee and monitor business associates, a growing  
144 challenge given resource constraints and the complexity of these relationships.

145

146 HIPAA covered entities have had an uneven record of providing thorough and consistent  
147 assessments of the BA practices of banks and financial service businesses. On the  
148 opposite side, the Committee identified confusion among those who provided testimony  
149 about certain provisions of HIPAA regarding banking obligations. For example, the  
150 HIPAA Privacy Rule requires that when a HIPAA-covered entity or BA uses or discloses  
151 PHI, or when it requests PHI from another covered entity or BA, the covered entity or  
152 BA must make “reasonable efforts to limit protected health information to the minimum  
153 necessary to accomplish the intended purpose of the use, disclosure, or request.”<sup>5</sup> HHS  
154 has extended the minimum necessary obligations to BAs and subcontractors, but has yet  
155 to issue guidance on what constitutes minimum necessary.

156

157 Thus our hearing re-enforced the importance of issuing guidance for the industry about  
158 the scope of the § 1179 exemption. It also revealed the need for educational materials  
159 addressing when BA relationships are created and at what point BA agreements should  
160 be executed.

161

162 **Recommendation 3. NCVHS recommends that HHS work with the appropriate**  
163 **federal financial regulatory agencies to develop an analysis comparing federal**  
164 **privacy and security regulations of HIPAA with those of the banking and financial**  
165 **services sector. The purpose of this analysis is to support a conversation between the**  
166 **health information sector and the financial services sector.**

167

168 The May 2015 hearing revealed that large, more sophisticated financial institutions, small  
169 in number but comprising about 80% of U.S. banking transactions,<sup>6</sup> have taken steps to  
170 organize for compliance with HIPAA. Often they provide services through a subsidiary,

---

<sup>5</sup> HHS HIPAA Privacy Rule, 45 C.F.R. § 164.502(b).

<sup>6</sup> We will find a citation for this assertion

171 separating HIPAA-covered business lines from traditional banking. These “firewalls”  
172 ensure that access to PHI is strictly controlled and handled in accordance with applicable  
173 regulations while not burdening the banking functions with HIPAA compliance. These  
174 more sophisticated institutions are well aware of their obligations under HIPAA and we  
175 were told that they have the policies and practices in place to comply. There are also  
176 many thousands of smaller and local banks; a HIPAA compliance picture for this sector  
177 of the financial industry is not publicly available. It would be helpful for these banks and  
178 the health care providers in their communities to have clarity with regard to their  
179 obligations.

180

181 New financial services businesses such as PayPal, Applepay, and Google Checkout,  
182 which were not represented at the hearing, nevertheless appear, so far, to be limited to  
183 carrying out straightforward consumer-driven payment transactions and, therefore,  
184 exempt under § 1179.<sup>7</sup>

185

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

191

192 When compared to the HIPAA Privacy and Security Rules,<sup>8</sup> the privacy provisions of  
193 banking laws such as GLBA, FACTA and others have different purposes and  
194 perspectives. For example, GLBA requires covered financial institutions to provide a  
195 notice of practices and an opportunity to opt out, but it does not require that a financial  
196 institution’s practices meet any minimal standards. FACTA prohibits a financial  
197 institution from using health information for underwriting loans.

198

---

<sup>7</sup> 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.

<sup>8</sup> 45 CFR [Part 160](#) and [Part 164](#), Subparts A and E (HIPAA Privacy Rule) or 45 CFR

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

210  
211 Moreover, HIPAA-covered entities lack a thorough understanding of the privacy and  
212 security obligations imposed on financial institutions by non-HIPAA banking regulations.  
213 Thus, the important differences in the privacy and security requirements of the healthcare  
214 and financial industries are not well known or understood by either industry. In light of  
215 the growing dependence of the health sector on banks and financial services businesses to  
216 support the management of health administrative systems, improved cross-industry  
217 awareness of privacy and security practices would be highly beneficial. In the current  
218 climate, the value of a more detailed analysis of comparative privacy regulations by  
219 experts in both fields cannot be overstated.

220  
221 **Recommendation 4. HHS, working with industry groups such as Workgroup for**  
222 **Electronic Data Interchange (WEDI), should convene a public-private cross-**  
223 **industry panel of experts representing the health and financial services sectors that**  
224 **meets on a regular basis to identify opportunities for collaboration and cross-**  
225 **learning between these sectors.**

---

<sup>9</sup> 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.”

226

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

230

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

241

242 Cybersecurity is an example of an issue facing both industries with healthcare  
243 experiencing a share increase in breaches due to cyber theft. The Committee heard  
244 testimony that the cybersecurity practices of banks are generally more sophisticated than  
245 they are for healthcare under the current Security Rule. Banking may have protocols that  
246 could help prevent and accelerate the effective response of healthcare organizations.

247

248 The use of aggregate data or “big data” analytics poses another issue only partially  
249 addressed by HIPAA. The current Privacy Rule permits BAs to aggregate data from  
250 different covered entities, including data about the same patients in both sets. The range  
251 of policy questions, however, are growing and cross industry debate would be helpful in  
252 addressing questions such as: the limits on how these data might be used or monetized;  
253 whether aggregate data may be used to derive predictive algorithms that guide future  
254 health coverage or payment decisions; the rights of consumers in this regard; the impact  
255 of available methodologies for linking records and de-identifying the data, and the

256 possibilities for integrating data from HIPAA covered entities with data derived from  
257 other sources?

258

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

263

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

271

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

274

275 Sincerely,

276

277

278 Walter G. Suarez, M.D., M.P.H.,

279 Chair

280 National Committee on Vital and Health Statistics

281

282 Cc: HHS Data Council Co-Chairs