2004

HIPAA: Demystifying the Implications for Financial Institutions

Jessica M. Lewis

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi

Part of the Banking and Finance Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncbi/vol8/iss1/8

This Notes is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
Notes & Comments

HIPAA: Demystifying the Implications for Financial Institutions

Insurance companies spend between $0.25 and $0.75 processing an electronic claim.\(^1\) Processing that same claim via paper costs insurance companies between $2 and $12.\(^2\) By enacting the Health Information Portability and Accountability Act of 1996 (HIPAA), Congress aimed to decrease health care costs by promoting the more economically efficient electronic claim process, while simultaneously protecting the privacy of individually identifiable health information.\(^3\) Although designed to decrease costs and protect privacy, the rules promulgated by the Department of Health and Human Services (HHS)\(^4\) pursuant to HIPAA may actually cause an increase in health care costs as companies strive to meet stringent and costly standardization requirements for electronic transactions.\(^5\) Failure to meet HIPAA

---

2. Id.
4. United States Department of Health and Human Services: What We Do, at http://www.dhhs.gov/news/press/2002pres/profile.html (last visited Jan. 28, 2004). The Department of Health and Human Services [hereinafter HHS] is the “United States government’s principal agency for protecting the health of all Americans.” Id. Its services include programs in substance abuse, infectious disease control, food and drug safety, financial assistance for low-income families, and running Medicare, the nation’s largest health insurer. Id. The Office of the Secretary, currently headed by Secretary Tommy Thompson, runs the Department. Id. The Department includes the following operating divisions: the National Institute of Health, the Food and Drug Administration, the Centers for Disease Control and Prevention, the Indian Health Service, the Health Resources and Services Administration, Substance Abuse and Mental Health Services Administration, the Agency for Health care Research and Quality, the Centers for Medicare and Medicaid Services, the Administration for Children and Families, the Administration on Aging, the Office of Public Health and Science, the Office of the HHS Inspector General, and the HHS Office for Civil Rights. Id. The U.S. Public Health Service Commissioned Corps, headed by the Surgeon General, includes more than 6,000 health care professionals who serve in the various operating divisions within the HHS. Id.
5. See Marks, supra note 1, at 560 (noting that entities which cannot meet the
regulations may result in penalties as high as $25,000 per year per violation.\textsuperscript{6} 

Banks are among the institutions that must concern themselves with these new HIPAA regulations.\textsuperscript{7} Many banks have instituted increased privacy measures in order to comply with the Gramm-Leach-Bliley Act (GLBA).\textsuperscript{8} Yet a bank classified under HIPAA as a “health care clearinghouse” or as a “business associate” of a “covered entity”\textsuperscript{9} may find itself facing the need for additional safeguards.\textsuperscript{10} While HIPAA regulations mandate privacy, security, and administrative simplification, this Note focuses on the electronic transaction standards found within the administrative simplification rule.\textsuperscript{11} The HHS enacted these rules to promote administrative simplification and a subsequent reduction of health care costs.\textsuperscript{12}

It should be noted that it remains largely unclear as to the exact measures a “health care clearinghouse” qualified bank must take to satisfy HIPAA mandates.\textsuperscript{13} This uncertainty stems from the broad language of the HIPAA statute\textsuperscript{14} as well as from the fact that HHS will rely on complaints to enforce the HIPAA rules,\textsuperscript{15} which became effective for most institutions in October 2003 and

\begin{itemize}
\item \textsuperscript{7} See generally Laura K. Thompson, \textit{Bankers Sick Over ACH Health-Care Law}, AM. BANKER, Sept. 10, 2002, at 5.
\item \textsuperscript{8} See generally 15 U.S.C. §§ 6801-02 (1999).
\item \textsuperscript{9} Moynihan, \textit{supra} note 6, at 33-34.
\item \textsuperscript{10} See id. at 35-36.
\item \textsuperscript{11} 45 C.F.R. § 162 (2003).
\item \textsuperscript{12} Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,312 (Aug. 17, 2000) (codified at 45 C.F.R. § 162). Entities subject to such electronic transaction standards also must comply with the privacy and security rules. 42 U.S.C. § 1320d. However, this Note does not explore rules of compliance in these areas.
\item \textsuperscript{13} See generally 45 C.F.R. § 162.
\item \textsuperscript{14} See generally 42 U.S.C. § 1320d.
\end{itemize}
are not fully effective for small health plans until August 2005.\footnote{16} Some complaints have already been filed, but HHS has yet to take definitive action.\footnote{17} Consequently, this Note seeks not to set forth the exact measures necessary to comply with HIPAA rules but to present the issues that banks must now consider in the wake of HIPAA's passage.

Part I of this Note briefly summarizes the history and policy behind HIPAA and defines critical terms used in the HHS rules enacted pursuant to HIPAA.\footnote{18} Part II reviews typical payment processing functions of banks, including the use of the Automated Clearinghouse (ACH) Network.\footnote{19} Part III discusses the possible ways in which a bank may be subject to HIPAA as a "health care clearinghouse" or as a "business associate" of a "covered entity."\footnote{20} Part IV examines whether HIPAA's policy goals are hindered by subjecting banks to costly compliance measures and enforcing penalties for non-compliance.\footnote{21}

I. HIPAA: THE POLICY BEHIND THE ACT AND ITS RULES

A. HIPAA and Its Rules

HIPAA was enacted in 1996.\footnote{22} Its purpose was threefold: to increase portability of health care coverage for employees moving from the health plan of one employer to that of another, to

\hspace{1cm}


\footnote{17. \textit{See, e.g.}, Centers for Medicare & Medicaid Services, HIPAA: Direct Enforcement, \textit{available at} http://www.cms.hhs.gov/hipaa/hipaa1/content/enforcement.asp (last visited Feb. 7, 2004).}

\footnote{18. \textit{See infra} notes 22-41 and accompanying text.}


\footnote{20. \textit{See infra} notes 101-40 and accompanying text.}

\footnote{21. \textit{See infra} notes 141-76 and accompanying text.}

\footnote{22. 42 U.S.C. § 1320d (2000).}
reduce the cost of health care by simplifying health care administrative processes, and to increase protection of personal health information. To achieve these ends, Congress gave HHS broad authority to implement rules. HHS responded with regulations covering the areas of privacy and security, as well as electronic transactions.

Electronic standard transactions encompass eight different transactions, two of which are financial in nature and thus of importance to banks. The two financial functions, health care claim payment and health care premium payment, must meet national standards prescribed by HHS. These HHS-developed standards include electronic codes used to identify patients, employers, providers, and health plans during payment processing. For HIPAA to achieve its intended standardization of electronic data interchange, the entire health care industry, including banks dealing in health care information, must adopt these government-prescribed standards. While many organizations applied to HHS for an extension from the initial compliance deadlines, no entities subject to HIPAA (except

23. Id.
24. Id.
28. BANKING INDUSTRY HIPAA TASK FORCE, WHITE PAPER ON HIPAA RELATED ISSUES AFFECTING THE BANKING INDUSTRY at 6 (May 29, 2002, Revised July, 2003) [hereinafter WHITE PAPER], available at http://www.hipaabanking.org/whitepaper_revised_July_2003.pdf (last visited Feb. 7, 2004); see also 45 C.F.R. § 160.103 (stating that "[t]ransaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information exchanges: (1) Health care claims or equivalent information, (2) Health care payment and remittance advice . . . ").
29. Moynihan, supra note 6, at 34.
30. Id.
31. See Marks, supra note 1, at 559. HHS set the following compliance deadlines: All covered entities, except for small health plans, must have complied with the privacy rule since April 14, 2003. Small health plans must comply by April 14, 2004. All covered entities, except for those that applied for an extension and small health plans, must have complied with the Electronic Standard Transaction rule since October 16, 2002. All covered entities must comply with the rule by October 16, 2003. Centers for Medicare & Medicaid Services, HIPAA Administrative Simplification Compliance Deadlines, supra note 16.
32. See Thompson, supra note 7, at 5-6.
small health plans) remain exempt from the final compliance date of October 16, 2003. However, some time may elapse before HHS learns whether institutions have fully complied with the use of mandated code sets because HHS agencies monitor HIPAA compliance via complaints rather than actively seeking violations.

B. Essential Definitions

A banking organization may become subject to HIPAA if it is considered a “health care clearinghouse” or a “business associate” of a “covered entity.” HIPAA defines each of these terms. It is therefore important for banks to understand these definitions in order to discern whether they must comply with HIPAA standards. A “health care clearinghouse” is defined as a public or private entity... that does either of the following functions: (1) Processes or facilitates the processing of health information... in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction... and processes or facilitates the processing of health information [in the standard transaction] into nonstandard format or nonstandard data content for the receiving entity.

Even if a bank fails to meet the above definition of a “health care clearinghouse,” it may still find itself subject to

---

33. Centers for Medicare & Medicaid Services, HIPAA Administrative Simplification Compliance Deadlines, supra note 16. The time lag between HIPAA’s enactment and promulgation of the rules pursuant thereto was intended to provide time for covered entities and business associates to identify themselves as such and institute mechanisms to comply with the rules. See Marks, supra note 1, at 561.


35. See generally Moynihan, supra note 6, at 33-35.

HIPAA if it is found to be a "business associate" of a "covered entity" which handles "individually identifiable health information." 

Health care providers, health plans, and health care clearinghouses are considered "covered entities." A "business associate," while not a covered entity itself, handles individually identifiable health information in performing services for a covered entity. HIPAA defines protected "health information" as "individually identifiable health information . . . that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium." This definition notably does not include individually identifiable health information contained in education or employment records held by an employer.

II. PAYMENT PROCESSING: TRADITIONAL TRANSACTIONS, THE ACH NETWORK, AND HEALTH CARE CLEARINGHOUSE FUNCTIONS

A. Overview of Health Care Payment Processing – Traditional Processing and the Role of Banks

Health care payments typically originate from insurance carriers or patients. Payments may run through the ACH system in electronic form, the lockbox system in paper form, or through a consumer payments processing system in paper form. When the ACH system processes the payment, intermediary

37. Moynihan, supra note 6, at 35.
39. 45 C.F.R. § 160.103 (2003). Services that a business associate might provide, inter alia, include claims processing, utilization review, quality assurance, billing, repricing, data aggregation, and financial services. Id.
40. Id.
43. See NACHA, supra note 19; see also infra notes 54-78 and accompanying text.
44. See NAHCA, supra note 19. Banks typically engage in all of these types of payment processes. Id.
45. Id.
financial institutions handle the payments via computer and eventually transfer electronic funds to the health care provider to whom payment is owed. In contrast, a lockbox service processes paper check payments and aggregates the data. The health care provider then receives the compilation of payment data either electronically or via filing boxes. Through the traditional consumer payments processing system, a paper check system, the health care provider receives the processed payment via direct mail.

Banks may find themselves subject to HIPAA if involved in the ACH Network or a lock box system for a health care provider. A bank’s role in the ACH Network will determine whether the bank performs a health care clearinghouse function subject to HIPAA regulation. Alternatively, a bank that provides a lockbox service for a health care provider or health plan may meet HIPAA’s definition of a health care clearinghouse. HIPAA regulations, however, do not apply to a bank that merely sends a checking account statement to an account holder who has paid for a health service via credit or debit.

B. The ACH Network

The ACH Network, an electronic funds transfer system widely used by financial institutions, provides participating depository institutions with electronic payment clearing services. The ACH Network facilitates direct deposit and direct payments for consumers and businesses. It provides the benefits of efficiency in payment processing and, unlike paper checks, nearly

46. Id.
47. Id.
48. Id.
49. See NACHA, supra note 19.
50. THE MEDICAL BANKING PROJECT, supra note 42.
51. See generally id. See also infra notes 105-124 and accompanying text.
52. THE MEDICAL BANKING PROJECT, supra note 42.
53. THE MEDICAL BANKING PROJECT, supra note 42.
54. NACHA, supra note 19.
55. See id.
eliminates the possibility of delay or loss of the payment information.\textsuperscript{56}

Payment information flows between five key players within the ACH Network: an originating customer, an Originating Depository Financial Institution (ODFI), an ACH Operator, a Receiving Depository Financial Institution (RDFI), and a receiving customer.\textsuperscript{57} An originating customer\textsuperscript{58} starts the process by making an entry into the ACH Network directing an ODFI\textsuperscript{59} to credit accounts with certain amounts of money.\textsuperscript{60} The ODFI, operating under an agreement with its customers and the National Automated Clearinghouse Association (NACHA)\textsuperscript{61} Operating Rules and Guidelines, decrypts, edits,\textsuperscript{62} re-encrypts, and transmits the originating customer's request to the ACH Operator.\textsuperscript{63} If the file generates an error during the ODFI's editing process, the ODFI rejects the payment request and returns it to the originating customer.\textsuperscript{64} If no editing error occurs, the ODFI processes the payment information and transmits it to the ACH Operator, comprised of the Federal Reserve and the Electronic Payments Network.\textsuperscript{65} The ACH Operator bears the responsibility of


\textsuperscript{57} See generally NACHA, supra note 19.

\textsuperscript{58} Id. For health care payments, an originating customer would be either the recipient of health care services or the person covered under the health plan. Id.

\textsuperscript{59} Id. The Originating Depository Financial Institution would be the financial institution at which originating customer has a deposit account [hereinafter ODFI]. Id.

\textsuperscript{60} See id.

\textsuperscript{61} Id. NACHA develops operating rules and business practices for financial institutions using the ACH Network. NACHA also monitors quality control of electronic payment processes, responds to regulatory issues, and markets electronic payment services. Id.

\textsuperscript{62} Banking Industry HIPAA Task Force, A Primer on HIPAA and the ACH Network, 11 (PowerPoint presentation on file with the NCBI courtesy of Cristeena Naser, Senior Counsel, American Bankers Association) [hereinafter Banking Task Force]. Editing means “comparing the formatting of the transaction to the formatting rules for that particular type of standard.” Id. at 13.

\textsuperscript{63} NACHA, supra note 19.

\textsuperscript{64} Banking Task Force, supra note 62, at 16.

\textsuperscript{65} See NACHA, supra note 19. The Electronic Payments Network (EPN) is a private ACH Operator that provides payment processing services to many financial institutions. See Electronic Payments Network, About Us, at http://www.epaynetwork.com/index.php (last visited Feb. 7, 2004).
decrypting the information transmitted by the OFDI. It then edits the payment information and sorts it by bank to receive payment. Finally, it re-encrypts the information and distributes the encrypted payment files to the originating customer’s designated RDFI. The RDFI is the institution where the receiving customer (who authorizes the originator to initiate a transaction) maintains a deposit account. The RDFI, acting under agreement to receive ACH entries and abiding by the NACHA Operating Rules and Guidelines, decrypts, edits, processes, and re-encrypts the payment file to make funds and statements available for the receiving customer.

Standard payment processing by the ODFI and the RDFI requires compliance with NACHA and ANSI X12 guidelines. The NACHA, which makes rules for the ACH Network and other electronic payment systems, takes the position that no bank performs a health care clearinghouse function simply by originating or receiving an ACH transaction for health care premium or claim payments. Rather, the bank provides health care clearinghouse functions, and is subject to HIPAA, when its services go beyond receiving or originating the payment information. Thus, access to protected health information does not occur in any process prior to the RDFI’s receipt of the payment file and may not even occur upon the RDFI’s receipt of such information. For instance, the RDFI — in decrypting the payment file, editing that file by validating the money amount, further processing the payment, and posting the payment amount as a credit to the receiving customer’s account — is not subject to

66. See NACHA, supra note 19.
67. See id.
68. Id. The Receiving Depository Financial Institution (RDFI) would be the financial institution at which the receiving customer has a deposit account. Id. In a health care payment transaction, the receiving customer would be the health plan or health care provider. Id.
70. See NACHA, supra note 19.
71. Id. ANSI X12 simply indicates a transaction in compliance with HIPAA standards. HIPAA Banking Task Force, supra note 62, at 26.
72. WHITE PAPER, supra note 28, at 8.
73. Id.
74. Id. at 6.
However, an RDFI steps beyond standard payment processing and into health care clearinghouse functions when a receiving customer, which is also a covered entity, requests remittance data in a human readable form (as opposed to computer) from the RDFI. Such a request requires the RDFI to access HIPAA-protected health information, therefore, the RDFI must add two protective steps between decryption and editing in order to comply with HIPAA. The RDFI must (1) sort the files it receives for health care claims and (2) edit those health care claim files against HIPAA standards before continuing to edit and process the files.

C. Health Care Clearinghouse: Intermediary Between Health Plans and Health Care Providers

Health care clearinghouses process claims using a structure similar to that used by the credit card industry. The typical credit card payment originates with a merchant who accepts the card for payment and sends a request for payment to a clearinghouse. The clearinghouse then processes and transmits the payment request to the appropriate bank. A health care clearinghouse likewise “accept[s], sort[s], process[es], edit[s], and then forward[s] the claims to the appropriate payors, either electronically or on paper.” An electronic deposit of a payment with a provider is an electronic funds transfer (EFT); performing the transfer function may be characterized as an electronic data interchange (EDI). Each transaction receives a standard number based on its payment

---

75. Banking Task Force, supra note 62, at 26. 835 indicates the type of payment - remittance. Id.
76. See id. at 27, 29.
77. Id. at 32-33.
78. Id. at 33.
80. Id.
81. Id.
82. Id.
For instance, "837" identifies a health care claim, and "835" identifies a remittance.

Unlike generic payment processing, a health care claim must be processed in compliance with HIPAA. HIPAA rules require standardized code sets for administrative and financial transactions in order to reduce payment information to the minimum amount necessary to complete the payment transaction. Health care clearinghouses frequently provide HIPAA compliance services to insurance companies (the health plan) and health care providers who lack the resources to make their own systems HIPAA compliant. Thus, in its role as the intermediary between the health care provider and the insurance company, health care clearinghouses may convert non-standardized payment codes into HIPAA-compliant payment data, which is then transmitted between the parties.

In formatting payment transaction codes to meet HIPAA standards, a health care clearinghouse looks to three authorities for compliance measures (the HIPAA statute, HHS rules implementing the statute, and transaction implementation guides published as part of the transaction rules) as well as to the transaction agreement between the insurance company and health care provider. First, the HIPAA statute contains a list of electronic transactions that must be standardized. Second, the HHS rules lay out the format for each of these enumerated standard transactions. HHS requires the X12N format. This format was developed by the American National Standards Institute (ANSI), a body which controls electronic data interchange industry standards to insure the integrity of

---

84. See Banking Task Force, supra note 62, at 10.
85. Id.
86. Id.
87. 45 C.F.R. § 162.600(a) (2003).
88. Marks, supra note 1, at 561.
89. Id.
90. Id at 563.
91. Id.
92. Id.
93. See supra note 71.
94. See supra note 83 and accompanying text.
HHS selected the ANSI X12N format because only that standard transaction format met HIPAA's goal of increasing the efficiency of payment claim processing. Third, implementation guides for each particular transaction further specify which version of the general format to use. Finally, the parties involved in these standard transactions typically engage in "trading partner agreements," defining the specifics of the transaction. However, these agreements cannot alter the standards set forth by the HHS rules.

III. BANK CLASSIFICATION: HEALTH CARE CLEARINGHOUSE AND/OR BUSINESS ASSOCIATE

A bank may find itself subject to HIPAA if classified as a "health care clearinghouse" (a "covered entity") or as a "business associate" of a "covered entity." Being deemed a health care clearinghouse under HIPAA imposes two dimensions of compliance on a bank – that of a business associate and that of a covered entity. If a bank does not perform health care clearinghouse services, it does not meet the covered entity definition. However, a bank that provides other services for a covered entity may meet the business associate definition. Meeting either the covered entity or business associate definition subjects the bank to some degree of HIPAA compliance.

95. a la mode, inc. at www.alamode.com/EDI/x12.asp (last visited Feb. 7, 2004). Recall that X12 simply indicates that the EDI process complies with ANSI standards, but X12 does not indicate any particular category of data, such as health care claims. Id.

96. Id.


98. See Marks, supra note 1, at 564. For example, ASC X12N 820 must be used for health plan premium payments, and ASC X12N 835 must be used for health care payment and remittance advice. 45 C.F.R. §162.1802 (2003).

99. See Marks, supra note 1, at 567.

100. Id.

101. Moynihan, supra note 6, at 35.

102. WHITE PAPER, supra note 28, at 4.

103. Id. at 7-8.

104. Id.
NEW REGULATIONS 153

A. The Bank as a Health Care Clearinghouse

The HIPAA “covered entity” definition includes health care clearinghouses.\(^{105}\) An entity that provides health care clearinghouse services among its secondary, not primary, functions, as would be the case with most banks that provide such services, would likely be considered a “hybrid entity.”\(^{106}\) As a “hybrid entity,” HIPAA requirements apply only to the health care components of the bank.\(^{107}\) However, the bank must ensure that it does not share protected health information used in its health care components with the parts of the bank not subject to HIPAA compliance.\(^{108}\) As a “hybrid entity,” a bank has two ways to prevent this unauthorized sharing of protected health information.\(^{109}\) It may implement firewalls to prevent sharing of protected health information\(^{110}\) or the bank may choose to be considered a covered entity in its entirety.\(^{111}\) The latter choice permits the bank to avoid the challenges of identifying its covered components and implementing firewall protection.\(^{112}\)

Encryption of protected health information poses another issue for a bank classified as a health care clearinghouse. HIPAA does not require encryption of protected health information transmitted across open networks, such as the telephone and the

---


108. Id.


110. Id.


112. Id.
HIPAA rules therefore allow insurance companies (health plans) and health care providers to determine, in conjunction with their payment processing institution, whether to encrypt protected health data transmitted via open networks. However, HHS holds covered entity health care providers and insurance companies (health plans) directly responsible for their business associate's use of protected health information. Thus, in order to avoid inadvertent liability for improper protected health information disclosure, health care providers and insurance companies (health plans) will likely require their payment processing institutions (the health care clearinghouse) to encrypt protected health information.

Banks classified as health care clearinghouses must also confront the issue of "data mining." The Health Privacy Project (the Project), a coalition of several interest groups, has proposed that HIPAA rules should require encryption to protect an individual's health information from being improperly used by a bank. This group urges that HIPAA rules should require encryption of protected health information before it enters the ACH Network and then allow access to the information in decrypted form only to receiving health care providers or health plans. The Project argues that the encryption requirements will prevent financial institutions from being able to "mine" their customers' protected health information for risk assessment.

---

114. Id.
119. Id.
120. Id.
purposes.\textsuperscript{121} The concern about "data-mining" is that banks may gain access to information about non-customers and use that information in determining whether to extend loans or other credit.\textsuperscript{122} Banks may also share non-customer information with affiliates, such as insurance companies, which may also use the non-customer data to the non-customers' disadvantage when they apply for services.\textsuperscript{123} This issue arises where a bank chooses to be considered a covered entity in whole, but the issue may be addressed by erecting firewalls to prevent sharing of protected health information with the non-covered functions of the bank.\textsuperscript{124}

B. The Bank as a Business Associate

A bank may also be deemed a "business associate" of "covered entities" for which it provides services.\textsuperscript{125} Business associate banks fall into two categories: those conducting services for a "covered entity," which is the bank itself, and those conducting services for a "covered entity," which is not the bank but another party such as an insurance company (health care plan) or health care provider.\textsuperscript{126} A business associate must enter into a written contract with the covered entities it services to ensure that the business associate's use of protected health information complies with HIPAA security rules.\textsuperscript{127} Under that contract, the covered entity may disclose protected health information to the

\textsuperscript{121} Id.
\textsuperscript{122} Id.
\textsuperscript{123} Id.; see also Sean Marciniak, Medical Data Can Show Up in Credit Reports, \textit{WALL ST. J.}, Aug. 6, 2003, at D2. While most financial institutions make credit extension decisions via a brief review of a customer's credit score, some fear that financial institutions may use customers' health information against the customer by calling loans due early, for example, where the customer has cancer. \textit{Id.} The Fair and Accurate Credit Transactions Act of 2003 (FACTA) intends to prohibit affiliates from sharing health information about customers without customers' consent. \textit{Id.} FACTA has not set dates for rulemaking yet. \textit{See} Federal Trade Commission, For Your Information, Announced Actions for December 16, 2003, \textit{at} http://www.ftc.gov/opa/2003/12/fyi0372.htm (last visited Feb. 7, 2004).
\textsuperscript{124} See Kopp, \textit{supra} note 118.
\textsuperscript{125} \textit{WHITE PAPER, supra} note 28, at 7.
\textsuperscript{126} See generally \textit{id}.
business associate, and the business associate may receive protected health information from the covered entity.\textsuperscript{128}

As stated previously, a bank may be both a business associate and a covered entity.\textsuperscript{129} The key difference between compliance requirements of a business associate that is not a covered entity and those of a business associate that is also a covered entity is that the former's responsibilities arise solely under the contract while the latter's responsibilities extend beyond the contract and directly to HHS.\textsuperscript{130} The HHS holds the covered entity directly responsible for compliance with privacy, security, and electronic standard transaction rules, as well as for ensuring a business associate's compliance with HHS rules in the services it provides under the business associate contract.\textsuperscript{131}

\textbf{C. Bank One: An Example of a Health Care Clearinghouse}

Banks not currently providing health care clearinghouse functions may find themselves doing so in the future as more health care transactions occur via the electronic standard formats, as HIPAA intends.\textsuperscript{132} Bank One Healthcare Link, a concrete example of a bank knowingly functioning as a health care clearinghouse, promotes its business as the first bank to obtain Claredi certification\textsuperscript{133} for HIPAA compliance.\textsuperscript{134} Bank One

\begin{enumerate}
\item[128.] \textit{Id.} (stating that a business associate contract must provide boundaries for use and disclosure of protected health information, disallow the business associate to disclose protected health information in any way that the covered entity is disallowed, direct the business associate to prevent unauthorized use or disclosure and report violations, and provide that the covered entity may terminate the contract if the business associate materially breaches).
\item[129.] \textit{Id.}
\item[130.] \textit{Id.} at 1055, 1058. Once an entity determines that it is covered by the HIPAA rules, the next step is determining what information is covered by the rules, but that is beyond the scope of this Note. \textit{Id.} at 1058.
\item[131.] \textit{Id.} at 1057-58. An attorney for a covered entity also meets the definition of a "business associate" of that entity and, therefore, must abide by the business associate contract. Merideth C. Nagel, \textit{Litigation After HIPAA's Patient Privacy Regulations}, \textit{15 The Health Lawyer}, Aug. 2003, at 14; see also 45 C.F.R. § 162.923(c) (2003).
\item[132.] Woody, \textit{supra} note 127, at 1055.
\item[133.] Claredi: \textit{Answers to frequently asked questions, Why Certify?}, \textit{at} http://www.claredi.com/faq.php?PHPSESSID=3cd781df0c0a062fd7d82a3d5111be#f aq65 (last visited Jan. 30, 2004). Claredi claims to provide objective HIPAA
intends to serve health plans and health care providers by processing electronic payment transactions in compliance with HIPAA. Certification by Clareti provides Bank One with a competitive edge over other currently uncertified banks providing the same services. Because of the covered entities' concerns about liability for their business associates and themselves, engaging in transactions with a HIPAA certified business associate provides some sense of security to the covered entity.

Overall, banks are in a good position to promote efficiency in health care payments because of their well-developed ability to keep "dollars and data together" through the ACH network, where payment information flows with the payment entry. But NACHA notes that only the small number of banks that provide services beyond their traditional payment processing services, such as Bank One, will be considered health care clearinghouses.


A. Decreased Health Care Cost May Not Be Initially Achieved

Because HHS's electronic standard transactions rules fall under the premise of administrative simplification, the rules ultimately aim to decrease health care costs, without compromising the privacy and security of transactions. Increasing the efficiency of payment and claims transactions may decrease health care costs. However, compliance will likely cost

135. See id.
136. See id.
137. Id.
139. Id.
140. Id. at 4.
142. Id.
banks significant time and resources. The stringent HIPAA requirements in electronic standard transactions might also dramatically increase costs to the health insurance industry. This could occur if health care providers resort to sending paper claims because they are unable to comply with the HIPAA transaction rules for electronic claims. An increase in paper claim submissions would, in turn, require increased manpower and time, and could even result in violations of state prompt-payment laws.

B. State Laws May Preempt HIPAA Rules

HIPAA creates only a "federal 'floor' of protections." Therefore, states may enact more stringent laws than the federal HIPAA rules on protected health information privacy, security, and health care claims processing. Thus, a state law that "relates to the privacy of individually identifiable health information" and is "contrary to and more stringent than the federal requirements" will control. Further, state laws that the Secretary of the HHS deems necessary, that provide for necessary reporting, or that require necessary reporting by health plans will also prevail over any contrary HIPAA requirements.

Entities can expect litigation over what it means for a state law to "relate to the privacy of individually identifiable health information" and when a state law is "contrary to and more significant time and resources. Separating health care payments from other ACH transactions will likely increase processing time and, in turn, raise processing costs to banks.

The stringent HIPAA requirements in electronic standard transactions might also dramatically increase costs to the health insurance industry. This could occur if health care providers resort to sending paper claims because they are unable to comply with the HIPAA transaction rules for electronic claims. An increase in paper claim submissions would, in turn, require increased manpower and time, and could even result in violations of state prompt-payment laws.

B. State Laws May Preempt HIPAA Rules

HIPAA creates only a "federal 'floor' of protections." Therefore, states may enact more stringent laws than the federal HIPAA rules on protected health information privacy, security, and health care claims processing. Thus, a state law that "relates to the privacy of individually identifiable health information" and is "contrary to and more stringent than the federal requirements" will control. Further, state laws that the Secretary of the HHS deems necessary, that provide for necessary reporting, or that require necessary reporting by health plans will also prevail over any contrary HIPAA requirements.

Entities can expect litigation over what it means for a state law to "relate to the privacy of individually identifiable health information" and when a state law is "contrary to and more

143. Thompson, supra note 7, at 5.
144. See id.
145. Marks, supra note 1, at 565.
146. Id.
147. Id. at 560.
149. Id.
150. See Woody, supra note 127, at 1070-71. A state law that is merely "contrary" to but not "more stringent" than the federal law will not control. Id.
151. AHIMA, supra note 148.
stringent than federal requirements."\footnote{152}{Woody, \textit{supra} note 127, at 1071.} The rules provide minimal specific guidance on determining which state laws are contrary to or more stringent than the federal rules.\footnote{153}{Nagel, \textit{supra} note 131, at 16. This anti-preemption scheme is similar to the scheme implemented by the Gramm-Leach-Bliley Act regarding privacy of financial information in financial institutions. \textit{See} 15 U.S.C. § 6807 (1999).} HHS defines a contrary state law provision as one that "a covered entity would find . . . impossible to comply with" in addition to the federal rules or one that "stands as an obstacle" to the objectives of the rules.\footnote{154}{45 C.F.R. § 160.202 (2003).} While the HIPAA rules preempt "contrary" state laws, the federal rules do not preempt state laws that are contrary to but also more stringent than the federal rules.\footnote{155}{Nagel, \textit{supra} note 131, at 18.} A state law is "more stringent" than the rules if it provides "greater privacy protection for the individual who is the subject of the individually identifiable health information."\footnote{156}{45 C.F.R. § 160.202 (2003).} These conflicts will likely be resolved in favor of applying both the state and federal law whenever possible.\footnote{157}{Woody, \textit{supra} note 127, at 1071.}

\section*{C. Reasonableness of the Burden Placed on Banks}

HIPAA places additional restrictions on how banks may use protected health information that they receive.\footnote{158}{\textit{See} id. at 1059.} While banks have already been subject to compliance with the Gramm-Leach-Bliley Act’s restrictions on disclosure of protected health information, HIPAA restricts not only the disclosure but also the internal use of protected health information.\footnote{159}{\textit{Id.} The Gramm-Leach-Bliley Act permits a financial institution to share customer information among its affiliates but not with its non-affiliates, unless the customer has been given an opportunity to opt out of the information sharing and has not opted out. \textit{See} 15 U.S.C. §§ 6801-27 (1999); \textit{see also} LISSA L. BROOME \& JERRY W. MARKHAM, \textit{REGULATION OF BANK FINANCIAL SERVICE ACTIVITIES: CASES AND MATERIALS} 263 (2001).} Absent consent or authorization to use the protected health information, or an exception to consent or authorization requirement, a bank that is considered to be a “health care clearinghouse” (a “covered
entity") cannot disclose or use the information. Authorization or consent may only be granted for treatment, payment, health care operations, and a few other exceptions such as some limited marketing purposes.

HIPAA also makes a bank that qualifies as a health care clearinghouse directly responsible to yet another regulatory body, the HHS, and requires a bank designated as a health care clearinghouse to enter into "business associate" contracts with covered entities for which the bank provides clearinghouse services. However, standard contracts between health care clearinghouses and other covered entities already generally cover protected health information disclosure and require the health care clearinghouse to comply with federal and state rules on disclosure. HIPAA also subjects all covered entities to the same privacy requirements, regardless of the extent to which the entity uses protected health information. Thus, requiring health care clearinghouse banks to enter into business associate contracts may entail revising standard contracts that already address protected health information disclosure thereby increasing costs without realizing any privacy gains, contrary to the goals of administrative simplification.

Additionally, the rules provide for penalty assessments only against covered entities, such as banks qualified as health care clearinghouses, and not their business associates. HHS rules provide for penalty assessments only against covered entities because of the covered entity's direct responsibility to comply with

160. See Woody, supra note 127, at 1060-61.
161. Id. at 1061.
164. Id.
165. See id.
166. Id.
HIPAA and its regulations.\textsuperscript{168} HHS has not promulgated the enforcement regulation in full but has issued an interim final regulation that clearly gives the Secretary of HHS the authority to determine which penalty to assess against a covered entity.\textsuperscript{169} The interim final regulation lacks substantive guidance on what constitutes a violation, but the regulation does establish that the process will be complaint-driven.\textsuperscript{170} HHS delegates authority for monitoring compliance with the rules to offices within HHS.\textsuperscript{171} For example, the Center for Medicare and Medicaid Services monitors compliance with the electronic standard transaction rule, and the Office of Civil Rights monitors compliance with privacy standards.\textsuperscript{172}

Current civil money penalties for HIPAA violations promulgated by the Secretary of HHS include a maximum of $100 per violation with a $25,000 per year cap for all identical violations by one covered entity.\textsuperscript{173} The statute of limitations for these violations stands at six years.\textsuperscript{174} If a covered entity fails to request a hearing within sixty days after receiving notice that a penalty has been assessed against it, the Secretary of HHS must impose some form of penalty – either the proposed penalty or a lesser one.\textsuperscript{175} The Secretary of HHS may also settle a case or reject any penalty

\textsuperscript{168} Id. Recall that a business associate’s HIPAA compliance obligation arises only under its contract with the covered entity, and business associates have until April 23, 2004 to comply with the contract requirements. \textit{See generally} Woody, \textit{supra} note 127, at 1055.


\textsuperscript{170} Id. at 18,897. Complaint-driven means that HHS relies on voluntary covered entity compliance rather than actively seeking out violations. \textit{Id}.

\textsuperscript{171} Moynihan, \textit{supra} note 6, at 36.

\textsuperscript{172} \textit{Id}.


\textsuperscript{175} Id. at 18,899.
during the hearing process without consent of the administrative law judge.\textsuperscript{176}

V. CONCLUSION

The regulations promulgated pursuant to HIPAA hold some obvious and some less apparent implications for financial institutions. By processing health care payments, financial institutions play a role in meeting HIPAA's decreased health care cost goal. At the same time, HIPAA aims to maintain privacy of the information used in these payment transactions by subjecting institutions and individuals that use the information to HIPAA standards. Particularly, a financial institution will meet the definition of a health care clearinghouse when it utilizes the ACH Network and provides remittance advice to its health care provider customer.\textsuperscript{177} HHS holds the financial institution that qualifies as a health care clearinghouse directly responsible for compliance with HIPAA.\textsuperscript{178} On the other hand, a financial institution might fail to meet the health care clearinghouse definition and thereby escape covered entity classification. However, the financial institution will still likely meet the business associate definition and, thus, must expend resources and time to comply with the business associate contract requirements.\textsuperscript{179}

When banks explicitly contract with covered entities to provide health care clearinghouse services for a fee, it seems fair to impose the same burdens on banks that provide these services as are imposed on traditional health care clearinghouses under HIPAA. Banks choosing to provide health care clearinghouse functions will benefit from a new fee-generating device, if the costs of compliance do not exceed the demand for service on which the fee may be based. However, where banks inadvertently begin to deal with protected health information as more and more health care payments become processed electronically, banks may validly argue against having to increase their privacy and security

\textsuperscript{176} Id. at 18,898.
\textsuperscript{177} See supra notes 105-124 and accompanying text.
\textsuperscript{178} See supra notes 173-174 and accompanying text.
\textsuperscript{179} See supra notes 175-176 and accompanying text.
standards for those transactions.\textsuperscript{180} Therefore, banks may or may not look forward to extending their payment processing mechanisms to provide electronic standard transactions in compliance with HIPAA on behalf of covered entities that lack the capabilities to perform this function.

JESSICA M. LEWIS

\textsuperscript{180} See supra notes 158-176 and accompanying text.