AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Lisa J. Bleier
Senior Trust Counsel
Regulatory & Trust Affairs
Phone: 202-663-5479
Fax: 202-828-4548
lbleier@aba.com

April 26, 2002

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building, Room 425A
200 Independence Avenue, SW
Washington, DC 20201

Re: Department of Health and Human Services; Standards for Privacy of Individually Identifiable Health Information; proposed rule modification; 45 CFR Parts 160 and 164; 67 Federal Register 14776, March 27, 2002

To Whom It May Concern,

On March 27, 2002, the Department of Health and Human Services published for public comment the above notice of proposed rulemaking which modifies the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), 45 CFR Part 160[1] and provides model Business Associate contract language. These regulations may affect some financial institutions in their dealings with health care clients.

The American Bankers Association (ABA) brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional, and money center banks and bank holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.

The ABA supports the goals of the Privacy Rule of enhancing patient privacy in the health care industry and creating national standards to protect individual's medical records and other personal health information.[2]

---

[1] Title II Subtitle F Section 261-264 of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

[2] To this end, the ABA has been working with NACHA – The Electronic Payments Association - through a task force to assist in the education of the industry. NACHA represents more than 12,000 financial institutions through direct memberships and a network of regional payment associations and 650 organizations through its industry councils. NACHA develops the operating rules and business practices for the Automated Clearing House (ACH) Network and for electronic payments in the areas of Internet commerce, electronic bill and invoice presentment and payment (EBPP, EIPP), e-checks, financial electronic date interchange (EDI), international payments, and electronic benefits transfer (EBT).

The use of these standards is intended to improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information.

The banking industry believes that there are situations in which financial institutions in the normal course of processing payments or other routine banking transactions for health care providers may be considered to be in a "Business Associate" relationship with a covered entity. For those situations, the ABA felt it would be helpful to provide comments regarding the Business Associate model contract language.

The banking industry has a long history of having the strongest protections against unauthorized access to customer information. Financial institutions currently receive detailed guidance from federal and state banking regulators concerning information technology procedures and are regularly examined in this area by the regulators.[3] In addition, financial institutions already have in place security policies and procedures that are developed on a bank-by-bank basis, factoring in the size and structure of each institution. We believe that the proposal's goal of having effective policies in security and confidentiality of customer information is being met by the banking industry.

Further, in 1997, the financial services industry announced a set of privacy principles that emphasizes the need for financial institutions to "maintain appropriate security standards and procedures regarding unauthorized access to customer information."[4] As a result, it is clear that all institutions already have policies and procedures regarding the protection of customer information.

More importantly, the Gramm-Leach-Bliley Act[5] included a section that requires the banking agencies to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information. This was codified as Regulation P in 12 CFR 216 on June 1, 2000. The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Federal Deposit Insurance Corporation (the "banking agencies") have each adopted Interagency Guidelines for examining in this area. These agencies regularly examine financial institutions for compliance with all applicable rules and regulations. Interagency guidelines establishing standards for safeguarding customer information were issued on February 1, 2001.[6]

---

[3] See, for example, OCC release NR-98-13 (February 4, 1998) in which the Comptroller of the Currency emphasizes the importance of technology risk assessment.

[4] On July 21, 1997, an ABA Task Force put together Privacy Principles for U.S. Financial Institutions. In addition, in June 2000, the ABA created the Task Force on Responsible Use of Customer Information. The Task Force developed voluntary guidelines for the industry. Among other things, these guidelines reaffirmed the industry commitment to maintaining confidentiality and security of customer data.

[5] Pub. L. 106-102 signed into law on November 12, 1999.

[6] Federal Register Vol. 66, No. 22, February 1, 2001, pp. 8616-8641.

We understand that the business associate model language proposed by the Department of Health and Human Services is voluntary. However, the ABA believes it is important at this early stage in rulemaking to bring to the Department's attention certain conflicts between the proposed Business Associate model language and current banking laws and practices.

Directly Conflicts with the Bank Secrecy Act

In the business associate model contract provisions on Term and Termination, part (c), the proposed language calls for the destruction of all Personally Identifiable Health Information (PHI) should the agreement between the Business Associate and the Covered Entity end. It is foreseeable that PHI may be contained within certain records or transactions that banks are currently required to maintain under the Bank Secrecy Act. This would create a regulatory problem for financial institutions, because such destruction would conflict with the Bank Secrecy Act.[7]

The Bank Secrecy Act was enacted in 1970 and has evolved into a reporting and recordkeeping requirement that is used by the government to combat money laundering – the acts of disguising the source of monies that are derived from criminal activities. Under the Bank Secrecy Act, financial institutions are required to retain certain records for a period of 5 years. In several sections of the regulation, the law states, "Records required to be kept shall be retained by the financial institution for a period of five years and shall be made available to the Secretary upon request at any time." 31 CFR Sec. 103.27; 31 CFR Sec. 103.29; 31 CFR Sec. 103.33; 31 CFR Sec. 103.34; 31 CFR Sec. 103.38.

In addition to the record retention requirements of the Bank Secrecy Act, many states have enacted their own rules pertaining to record retention. Some states require the retention of documents for up to 10 years. As a result, many financial institutions which do business in multiple states have internal policies which require retention of documents for 10 years to ensure compliance with every state in which they may do business.

Although certain of these requirements might apply only to the payments that are associated with the PHI, it would be impractical, if not impossible, for banks to separate the payment information from the accompanying remittance information that might include PHI. Thus, the proposed model provision on destruction of records would place banks in the untenable position of having to choose between complying with a contractual obligation and potentially violating a regulatory requirement. Congress could not have intended this result.

[7] Title 31 CFR, Subtitle B, Chapter 1, Part 103.

The ABA recommends that HHS provide particular relief for financial institutions in the proposed model language for Business Associates. Such relief should make it clear that financial institutions would be expected to comply with the current federal and state banking regulations in instances where there is a conflict with the Privacy Rule.

Lending relationships which are asset based

Loans to health care providers are often secured by accounts receivables of the provider. Because there is no permissive disclosure provision, it is unclear how common lending and lockbox relationships would be handled in these situations. Typically in such cases, a lender is allowed access to the borrower's receivables, whether related proceeds are received through electronic payments, lockbox[8] or any other method, especially after an event of default. In fact, Revised Article 9 of the UCC provides that in order to perfect a security interest in a deposit account (into which the proceeds of the receivables would be deposited), a lender must have "control" over the account. Many of the "control" account agreements among the lender, the borrower and the borrower's bank provide that in an event of default, the lender steps into the place of the borrower with respect to those receivables, and the lender would have a right to take possession of them.

It would also be a common practice for the banker to monitor the credit quality of the loan by reviewing the accounts receivable of the practice. The amount of credit available to the provider might fluctuate based upon the age of the receivable (i.e. how long it has remained unpaid by the insurance company) and the credit of the underlying patient for the self-pay portion of the receivable.

Similarly, the receivables of a health care provider might be the subject of an asset securitization. In such a case, a bank or a bank affiliate might be the lender or other conduit financing or facilitating the purchase of the receivables, which are pooled and sold as investments, or a bank might be the depository in which the receivable are deposited, with instructions to provide information about the receivables to other parties in the transaction.

In both cases, we believe that banks should be able to act to carry out the terms of their loan agreements and other contractual commitments without violating either the Privacy Rule or the terms of a Business Associate contract. We are concerned that such situations are neither addressed nor particularly protected by the model language.

---

[8] A "lockbox" is a banking service provided for the rapid collection of a customer's receivable and rapid credit to the customer's account. The service includes collecting the mail from the company's post office box; sorting, totaling, and recording the payments; processing the items; and making the necessary bank deposit. Definition from ABA Banking Terminology Resource.

Requires Business Associates to understand the intricacies of the law for a "Covered Entity"

In the Business Associate model contract provisions on Obligations and Activities of Business Associate, part (i), the proposed language requires the Business Associate to agree to document disclosure of PHI "as would be required" for the Covered Entity to respond to a request by an individual. To make that determination, the Business Associate would be contracting to analyze the law as if it were a Covered Entity. This burden should be on the Covered Entity alone, and not on the Business Associate. This would be unfair and unnecessary to place the Business Associate in the position of needing to know the intricacies of the law for the Covered Entity.

Similarly, in the section on Permitted Uses and Disclosures by Business Associate, first section, the language refers to the use or disclosure of PHI "if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity." This section also requires an analysis of the law by the Business Associate as if it were a covered entity. This also creates an additional and unnecessary burden on the Business Associate. To address this situation, HHS should clarify that the burden is on the Covered Entity to make it clear to the Business Associate what use of the information is permissible, and is not permissible.

No protection against unreasonable requests

Several sections of the Business Associate model agreement reference "in time and manner designated by Covered Entity," without including any protection for the business associate against unreasonable requests. In the section on Obligations and Activities of Business Associate, part (j), the Business Associate must be prepared to provide any information requested of the Covered Entity in the manner and time requested by the Covered Entity.

Considering the Business Associate may be required to go through thousands of documents to answer the request, there needs to be some limitation on the Covered Entity from being able to request that this information be provided in 24 hours, for example. This would be an unreasonable request, and a heavy burden on the business associate. HHS should revise the model agreement to make it clear that the Covered Entity may only make "reasonable requests" of the Business Associate in complying with its duties under the Privacy Rule.

Request for an exception for premium billing and payment

In section 164.504(f)(1)(iii), the Privacy Rule is modified to allow group health plans to share enrollment and dis-enrollment information with plan sponsors without amending plan documents. The ABA believes that premium billing and payment

should also be expressly permitted for sharing between group health plans and plan sponsors without amendment of plan documents.

Enrollment and dis-enrollment in a health plan and premium payments are both HIPAA standard transactions. Some of the same concerns regarding information misinterpretation cited in the notice of proposed rulemaking about the exchange of enrollment and dis-enrollment data between plan sponsor and health plan is common to the exchange of data related to premium bills and premium payments. This may be due to the status of the premium payment as a HIPAA standard transaction. While the premium payment is a HIPAA standard transaction, its limited dataset for remittance information – (usually the member name and identification number, along with a related dollar amount associated with a payment period) - does not constitute Protected Health Information.

Using the same analysis and rationale, the ABA recommends that the Department add an explicit exception at Sec. 164.504(f)(1)(iii) to clarify that group health plans (or health insurance issuers or HMOs, as appropriate) be permitted to disclose premium billing and payment information to a plan sponsor without meeting the plan document amendment and other related requirements.

Conclusion

In conclusion, the ABA supports the goals of the Privacy Rule, but has concerns regarding certain provisions of the proposed Business Associate model agreement. We believe that the existing rules covering financial institutions that govern the privacy of customer information meet the goals of the Privacy Rule. Financial institutions are currently regularly examined by the banking regulators for compliance with the rules and regulations currently in place.

We look forward to working with the Department of Health and Human Services. We believe that the unintended consequences of this Privacy Rule would make it virtually impossible for financial institutions to comply with both the Privacy Rule and other banking laws. We are seeking to discuss with you some relief for financial institutions in this area, and would welcome the opportunity to meet with appropriate staff to discuss further our concerns.

Sincerely,

Lisa J. Bleier
Senior Counsel
American Bankers Association