

HIAA

Health Insurance Association of America



Charles N. Kahn III
President

March 30, 2000

Mr. Jonathan G. Katz, Secretary
Securities & Exchange Commission
450 Fifth Street, NW
Washington, D.C. 20549-0609

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Ave., NW

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
ATTN: Docket # 2000-13
1700 G Street, NW
Washington, D.C. 20552

Mr. Robert E. Feldman, Executive Secretary
ATTN: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429

Ms. Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th & C Streets, NW
Washington, D.C. 20551

Office of the Comptroller of the Currency (OCC)
Communications Division
ATTN: Docket # 00-05
250 E Street, SW
Washington, D.C. 20219

**RE: Comments to Proposed Privacy Rules, Published Pursuant to Section 504
of the Gramm-Leach-Bliley Act (RIN 1550-AB36)**

March 30, 2000

Health Insurance Association of America (HIAA)

RE: Comments to Proposed Privacy Rules, Published Pursuant to Section 504 of the Gramm-Leach-Bliley Act (RIN 1550-AB36)

To Whom It May Concern:

The Health Insurance Association of America (HIAA) is the nation's most prominent trade association representing the private health care system. Its 290 member companies provide a variety of health insurance products to more than 123 million Americans. HIAA's members represent a cross-section of companies that finance and deliver health care and provide other health insurance products and services. Among those members that provide group and individual coverage for medical expenses are commercial health insurers, HMOs (and other managed care plans), and Blue Cross/Blue Shield carriers. HIAA members also offer supplemental insurance, group and individual disability insurance, long-term care insurance, reinsurance, and other products and services.

In February and March, the Department of the Treasury (Officer of the Comptroller of the Currency and Office of Thrift Supervision), the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Federal Trade Commission (the Agencies) promulgated proposed privacy regulations pursuant to § 504 of the Gramm-Leach-Bliley (GLB) Act (15 U.S.C. § 6804). *See* 65 Fed. Reg. 8770 (Feb. 22, 2000); 65 Fed. Reg. 11174 (March 1, 2000). Although these proposed regulations (the GLB Regulations) do not apply directly to insurers, they raise important issues that could seriously affect insurers, in part because the States are likely to look to the GLB Regulations as their model in developing their own privacy regulations. HIAA is concerned, among other things, that the standards set forth in the proposed GLB Regulations vary from, and at times are inconsistent with, those standards set forth in the proposed privacy regulations promulgated by the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Assuming the States adopt the GLB model, as the Agencies hope, this could lead to consumer confusion and significant additional – and unnecessary – costs to the health insurance industry (and ultimately consumers).

Accordingly, HIAA submits these comments to alert the Agencies to the potential inconsistencies between the proposed GLB and HIPAA regulations and to encourage the Agencies to formulate regulations that are consistent with the HHS confidentiality initiative. HIAA also writes to encourage the Agencies to clarify certain issues that remain unclear under the proposed rules.

Although the GLB Act clearly applies to banking institutions, it appears that health insurers may be swept into the purview of the Act as well. *See* § __.3¹; 12 U.S.C. § 1843(k). Thus, the GLB Act applies to “financial institutions,” which include those entities engaging in the business of “insuring.” *See* 15 U.S.C. § 6809(3); 12 U.S.C. § 1843(k). A closer review of the Act, however, suggests that Congress intended for the States to retain sole regulatory authority with respect to health insurers. *See* 15 U.S.C. § 6701. Although Congress could not require the States to enforce a federal law, it provided incentives for States to adopt the requirements outlined in the GLB Act. *See* 15 U.S.C. § 6805. Thus, if States adopt regulations to carry out the GLB privacy provisions, they are eligible to override certain other federal insurance customer protection regulations. *See* 15 U.S.C. § 6805(c).

HIAA believes that it is important for the health insurance industry to provide comments on the proposed GLB Regulations for several reasons. First, the Agencies should make clear that the GLB Regulations do not apply directly to health insurers. Second, the States will likely look to the federal regulations when developing their own regulation (or legislation) in this area and thus the regulations will have an indirect effect on insurers. Third, although we do not interpret the law in this manner, it is possible that if States do not exercise their regulatory authority, the Federal Trade Commission (FTC) may be able to step in and regulate insurers. The GLB Act designates the FTC as the default regulatory agency. *See id.* at § 6805(a)(7). HIAA believes that exercise of jurisdiction by the FTC in this context would be contrary to Congress’ clearly expressed intent that the States, and not the federal government, regulate health insurers. Fourth, health insurers may work with other entities that must adhere to these regulations and, therefore, would be indirectly subject to some of the provisions. Lastly, if banking institutions sell insurance products at some future date, the Agencies may eventually regulate these insurers. With all this in mind, HIAA believes that it is important to comment about the impact these regulations would have on the operations of member companies.

General Comments

Health insurers have long recognized the importance of maintaining the confidentiality of individually identifiable health information. They have processed personal health and financial information for decades. As well-established businesses in the United States, health insurers have adopted comprehensive policies and procedures for maintaining patient confidentiality. Our customers, both employers and individuals who purchase health insurance, have long had confidence that identifiable health and financial information is confidential, protected, and secure. In a competitive marketplace, it simply would be foolhardy for an insurer not to run its business with appropriate safeguards.

Moreover, health insurers are already subject to various federal regulations, rules, and industry standards governing the confidentiality or security of personal information.

¹ For ease, we adopt the Agencies’ manner of referring to the proposed regulatory provisions (*i.e.*, according to their section number, leaving the part number undesignated).

HHS recently proposed two new sets of rules under the authority of HIPAA. HHS published the first set of proposed rules for “Security and Electronic Signature Standards” (HIPAA security regulations) in the Federal Register on August 12, 1998. *See* 63 Fed. Reg. 43242 (1998). On November 3, 1999, HHS proposed the second set of proposed rules for “Standards for Confidentiality of Individually Identifiable Health Information” (HIPAA confidentiality regulations) in the Federal Register. *See* 64 Fed. Reg. 59918 (1999). Neither set of proposed rules has been issued in final form.

The proposed HIPAA regulations are broader than, and overlap with, the GLB Regulations. This overlap will create confusion for health insurers by placing them in the difficult position of having potentially to comply with conflicting regulations. The HIPAA and GLB regulations should work in tandem to achieve the laudable goal of protecting the confidentiality of identifiable health and financial information. As drafted, they do not. For example, while the HIPAA regulations use an individual authorization model for consent, the GLB Regulations rely upon an opt-out model. Permitting significant differences to exist will only exacerbate the troubling crazy quilt of state and federal confidentiality laws in effect today.

Detailed Comments

1. Although health insurers may be “financial institutions,” the GLB Regulations should not apply to them.

Although health insurers may fall within the GLB Act’s broad definition of “financial institutions,” HIAA strongly believes Congress did not intend for the Agencies’ regulations to apply directly to insurers. Congress provided that State insurance authorities, rather than federal agencies, should enforce the GLB Act requirements. *See* 15 U.S.C. § 6805. While it is unknown the extent to which the States will adopt regulations similar to those promulgated by the federal agencies, Congress’ intent that State insurance authorities, and not federal agencies, regulate insurers is clear. Therefore, HIAA recommends that the Agencies revise regulations to provide explicitly that the GLB Regulations do not apply to health insurers.

2. The Agencies should adopt the Alternative B definitions related to “nonpublic personal information.”

The GLB Regulations protect “nonpublic personal information” (NPI). The regulations define NPI as:

personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by a financial institution. Such information does not include publicly available information . . . [but does include] any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but

shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

§ ____.3(n).

The GLB Regulations, except for those promulgated by the Board of the Federal Reserve System, provide two alternative versions of what constitutes NPI. The Agencies solicit comments as to which approach they should adopt. The distinction between Alternative A and Alternative B lies in what “publicly available” means. *See id.* § ____.3(p). Alternative A requires that an entity actually *obtain* the information from government records, widely distributed media, or disclosures to the general public pursuant to law to be considered “publicly available.” Alternative B provides that if information *is available* from one of the public sources, then it will be considered lawfully available to the general public and excluded from the scope of NPI even if it is obtained elsewhere.

HIAA recommends that the final rules adopt Alternative B, which is the alternative the Federal Reserve System has selected. *See* 65 Fed. Reg. at 8797-98. HIAA believes this latter alternative is the better one because it would permit insurers to use information they know is publicly available, even if they did not obtain it from one of the designated sources. To require entities to protect information that is already public merely because they received it from a non-designated source would be inefficient and nonsensical. After all, once something is public it is no longer confidential. Therefore, HIAA recommends that the Agencies follow the Federal Reserve System’s approach and adopt Alternative B.

3. The potential overlap between the personal information protected by the GLB and HIPAA regulations will confuse consumers and make it difficult for health insurers to comply with both standards.

The GLB Regulations protect NPI, which is personally identifiable financial information. *See* § ____.3(n). The proposed HIPAA regulations cover “protected health information” (PHI). *See* 64 Fed. Reg. 59918, 60052. PHI is defined as “individually identifiable health information” that is electronically transmitted or maintained. *See id.* at 60053. Individually identifiable health information is information that is created by or received from a health care provider, health insurer, employer, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of a patient or the past, present, or future provision of health care or payment for health care and identifies the individual or creates a reasonable basis to believe the information can be used to identify the individual. *See id.* at 60053. Information only becomes PHI once it is electronically transmitted (meaning exchanged) or electronically maintained (meaning stored). *See id.* Any non-electronic version of records that at any time have been electronically transmitted or maintained also comes within the definition. *See id.*

It is very likely that there will be overlap between personal information that is PHI and personal information that is NPI. For example, when health care providers submit claims to insurers, the documents often contain *both individually identifiable health and financial information*. In these cases, the potential exists for both sets of regulations to apply. Thus, if States adopted these regulations in their entirety, health insurers might be required to follow conflicting provisions, such as having to obtain from consumers both the authorization required by HIPAA and the opt out required by GLB for personal information that falls under both PHI and NPI. *See infra* comment 4.

Not only will this overlap cause a dilemma for health insurers concerning how to comply with both sets of regulations, but it will also confuse consumers who will need to understand how the two different sets of regulations affect their ability to limit uses and disclosures of their individually identifiable information and their rights to access, copy, amend, or correct such information. While we understand the financial and health care industries differ in many ways, the Agencies and HHS should strive to adopt a unified approach as to what information is protected so that insurers and consumers clearly understand the requirements and rights under both systems.

4. Individual authorizations and opt out opportunities under the GLB and HIPAA regulations are potentially confusing for consumers and health insurers.

The proposed GLB Regulations prohibit financial institutions from disclosing NPI directly or indirectly to nonaffiliated third parties unless: (1) they have provided the consumer with an initial notice; (2) they have provided the consumer with an opt out notice; (3) they have given the consumer reasonable opportunity to opt out of the disclosure; and (4) the consumer has chosen not to opt out. *See* § __.7. The Act requires that consumers be given the opportunity to opt out before information is initially disclosed and be provided with an explanation of how to exercise that option. *See* § __.8.

By contrast, the proposed HIPAA regulations require health insurers to obtain authorizations from individuals for the use or disclosure of personal information in certain circumstances. HIPAA does not require such authorizations for the use or disclosure of PHI if it is related to treatment, payment, or health care operations. *See* 64 Fed. Reg. at 60053. The regulations also provide several exceptions to the authorization requirement for activities such as public health agency matters, judicial and administrative procedures, coroners and medical examiner matters, and law enforcement. *See id.* at 60056. Any PHI that has been stripped of certain designated “identifiers” may be used or disclosed without first obtaining an authorization. *See id.* at 60054.

There are practical differences between the individual authorization requirement in the proposed HIPAA regulations and the opt out opportunity in the GLB Regulations that could impede the ability of health insurers to provide consumers with efficient services. Under the HIPAA regulations, the authorization requirement is an affirmative step that health insurers must take prior to use and/or disclosure. By contrast, under the GLB Regulations, the opt out requirement places the burden on the consumer to limit the disclosure of his/her information. As a result, it is unclear whether an insurer would be

required to obtain both an authorization from and provide an opt out opportunity to a consumer. HIAA recommends that the final regulations clarify that the Agencies would view an individual's authorization for a particular disclosure as sufficient to satisfy the opt out requirements of the GLB Regulations.

5. “Captive” insurance agents fall under the “[e]xceptions to notice and opt out requirements for processing and servicing transactions.”

Many health insurers have “captive” agents who are not employees. A captive insurance agent is one that sells exclusively for one insurance company. HIAA seeks clarification that the Agencies agree that health insurers and their captive agents should fall under the “[e]xceptions to notice and opt out requirements for processing and servicing transactions” of § __.9, and § __.10, thus permitting information to be exchanged between those entities as permitted according to the exception language.

6. The notice requirements of the proposed GLB and HIPAA regulations are inconsistent.

Both the proposed GLB and HIPAA regulations require entities to notify individuals of their policies and procedures regarding personal information.

The proposed GLB Regulations require financial institutions to provide an initial notice to consumers at the time the relationship is established. *See* § __.4. In addition, an annual notice must be provided at least once during any twelve consecutive month period. *See* § __.5. The proposed GLB Regulations allow financial institutions to include in these notices a statement that they may disclose additional, but currently non-identified categories of NPI in the future. Similarly, the notices may also include statements that disclosures may be made to additional, yet-to-be-named categories of affiliates and nonaffiliated third parties in the future. *See* § __.6. Both the initial and annual notices must include descriptions of the:

- Categories of consumer NPI collected by the financial institution;
- Categories of consumer NPI that is disclosed by the financial institution;
- Categories of affiliates and nonaffiliated third parties to whom the financial institution discloses NPI (except for disclosures related to the processing or servicing exception or one of the general exceptions);
- Categories of former customer NPI that the financial institution discloses and the categories of affiliates and nonaffiliated third parties to whom these disclosures are made (except for disclosures related to the processing or servicing exception or one of the general exceptions);
- Categories of information disclosed and the nonaffiliated third parties to whom the information is disclosed pursuant to the service provider and joint marketing exception;

- Rights of consumers to opt out of disclosures of NPI to nonaffiliated third parties and the methods by which consumers may exercise these rights;
- Any disclosures under the Fair Credit Reporting Act; and
- Policies and procedures regarding the protection of the confidentiality, security, and integrity of NPI.

See id.

Under the HIPAA regulations, a health insurer must provide such notice when individuals enroll in a health plan and also when any material changes are made to these policies and procedures. The notice is to be provided at least once every three years. *See* 64 Fed. Reg. at 60059. The HIPAA proposed rules state that the notification must, in plain language:

- Describe a covered entity's policies and procedures regarding uses or disclosures of PHI so as to put each individual on notice of these uses or disclosures;
- Describe the types of uses and disclosures that will be made without an authorization;
- Distinguish between uses and disclosures required by law and those permitted by law;
- State that other uses and disclosures will be made only with an individual's authorization and that this authorization may be revoked;
- State that an individual may request that certain uses or disclosures of his/her PHI be restricted, but that the covered entity does not have to comply with such requests;
- State that an individual has the right to request to inspect, copy, amend, and correct his/her PHI and to obtain a description of the process for such requests;
- State that an individual has the right to request an accounting of the disclosures of his/her PHI by the covered entity;
- State that the covered entity is "required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect;"
- State that the entity may change its policies and procedures at any time and describe how individuals will be notified of such changes;
- State that individuals may complain to the covered entity and the Secretary of the Department of Health and Human Services if they believe their privacy rights have been violated;

- Provide the name and telephone number of a contact person or office to which questions and complaints may be directed; and
- Provide the date of the version of the notice.

See id.

In addition to the content differences, the notices required under the GLB Act and regulations differ from the HIPAA regulations with respect to timing. The GLB Regulations require more frequent notification. Thus, both an initial and *annual* notice must be given. *See* § __.4, .5. Under the HIPAA regulations, entities must provide an initial notice to consumers at the time the relationship is established and when any material changes are made to policies and procedures, but no less than once every three years. *See* 64 Fed. Reg. at 60059.

HIAA recommends that the Agencies and HHS align these requirements to achieve consistency among the final versions of these regulations. We believe a sensible approach is to adopt the HIPAA timing requirement so that notice would be provided to consumers when the relationship is initially established. After that, the entity would provide additional notices when any material changes to policies and procedures are made, but no less often than once every three years. Annual notices, as required in the GLB Regulations, would be unnecessary, often duplicative, administratively expensive, and could confuse consumers.

7. The proposed GLB Regulations require “financial institutions” to monitor the activities of nonaffiliated third parties and mandate the renegotiation of hundreds of thousands of contracts with nonaffiliated third parties.

The proposed GLB Regulations require “financial institutions” enter into contractual agreements with nonaffiliated third parties. The agreements must be designed to ensure that these third parties maintain the confidentiality of NPI. *See* § __.9. This requirement has an unintended consequence: it would require insurers to become “pseudo-regulators” or “monitors” of nonaffiliated third parties. Health insurers are ill equipped to take on such a role. HIAA recommends that the Agencies modify the proposed provisions to assure that no financial institution would be subject to penalty or liability for failure to regulate another person or entity.

The proposed GLB Regulations, if applied to insurers or if states adopted similar requirements for insurers, would be extremely disruptive for an additional reason: they would disturb hundreds of thousands of existing contractual or other arrangements between financial institutions and nonaffiliated third parties. Health insurers would face the difficulties associated with renegotiating a high volume of contracts with their many nonaffiliated third parties. The costs of these negotiations would increase administrative costs that could lead to higher premiums.

HIAA, however, understands the need to provide protection to NPI when it is disclosed to nonaffiliated third parties. There are many ways to achieve the goal of having financial institutions require that nonaffiliated third parties comply with the proposed regulations. One approach is through contract provisions as proposed. Another approach would be to permit parties to adopt their own policies and procedures tailored to their specific organizations. With these policies and procedures in place, these entities could certify or attest to compliance with the federal regulations. HIAA recommends that the final regulations include the option to use contracts, certifications, or other methods to require nonaffiliated third parties compliance with the regulations.

To alleviate many of the problems associated with the nonaffiliated third party provisions, HIAA recommends the proposed regulations be changed to allow the option for nonaffiliated third parties to certify or attest to compliance with the regulations. Thus, no financial institution would be subject to penalty or liability for failure of a non-affiliated third party to comply with the regulations as long as the nonaffiliated third party has certified or attested to compliance with the federal regulations. With that in mind, we have attached a draft form, "Certificate of Compliance with Federal Privacy Regulations."

CERTIFICATE OF COMPLIANCE WITH FEDERAL PRIVACY REGULATIONS

The undersigned, having been duly sworn under oath, certifies that the person, corporation, partnership, or business entity named below ("Nonaffiliated Third Party")

- 1. intends to comply with Department of Treasury Privacy Regulations, 12 CFR _____ ("Regulations"); and*
- 2. has the means and ability to comply with the Regulations; and*
- 3. will in fact comply with the Regulations.*

The undersigned further agrees that Nonaffiliated Third Party will indemnify and hold harmless any person or entity from any cost or expense incurred by the person or entity as a result of any failure by Nonaffiliated Third Party to comply fully and completely with these Regulations.

Nonaffiliated Third Party

Attest _____

By _____

Title _____

Title _____

Date _____

Date _____

Sworn to and subscribed to before me this ___ day of ___, 20__.

Notary Public

*My commission expires:
sealed*

8. The lack of a definition of “marketing” could limit the ability of health insurers to perform beneficial disease or health management activities.

Both the proposed GLB and HIPAA regulations limit the ability of insurers to use identifiable information for marketing purposes. Under the GLB Regulations, financial institutions may not disclose account numbers (or such similar access information) to nonaffiliated third parties for telemarketing, direct mail marketing, or electronic mail marketing to the consumer. *See* § ____.13. Under the HIPAA regulations, health plans must obtain authorizations from individuals whose PHI is used for marketing purposes. *See* 64 Fed. Reg. at 60056.

It appears that both the GLB and HIPAA regulations could prohibit health insurers from performing important activities related to disease/health management that are accomplished via direct or electronic mail if the definition of “marketing” is not clarified. Therefore, HIAA recommends that the Agencies clarify the term “marketing” to ensure that disease/health management programs, which are accepted and utilized in both the private and public (*i.e.*, Medicare and Medicaid) programs, are not mistakenly classified as marketing.

9. Federal preemption of state laws is needed to avoid confusing and burdensome processes for patients and insurers.

While HIAA recognizes that the Agencies do not have the statutory authority to promulgate regulations that preempt all state confidentiality laws under the GLB Act, *see* 15 U.S.C. § 6807; § ____.15, we wish to express our serious concerns about the relationship between the proposed regulations and state laws. This lack of federal preemption is very problematic for insurers.

By establishing a “federal floor,” the proposed regulations perpetuate the current inconsistent and non-uniform environment. Current confidentiality protections, which vary by geographic location, are confusing and troubling to patients. In today’s mobile society, people frequently relocate, employees work and reside in different states, family members live in different states, and patients may receive health care anywhere in the country. Consumers simply cannot stay abreast of the various laws and regulations; therefore, they often do not know what, if any, protections they may receive.

Health insurers also have difficulty complying with varying and conflicting confidentiality laws. Many insurers engage in multi-state operations and must cope with the complexities of varying state laws for confidentiality of health information. Health insurers will have tremendous difficulty determining which state laws are not preempted and will be burdened by contrary and potentially harmful state laws. This multilevel compliance effort creates an expensive administrative burden for insurers that is, by necessity, absorbed into the overall cost of health care. The increased costs will be passed on to consumers in the form of higher premiums.

The proposed regulations exacerbate an already difficult environment for health insurers. By further confounding the existing patchwork of confidentiality laws, the proposed regulations would make the legal environment unworkable for these entities.

Conclusion

HIAA appreciates the opportunity to submit comments to the proposed regulations for confidentiality of personal information. If we may be of further assistance, or if you have questions about these comments, please contact Kathleen H. Fyffe, Federal Regulatory Director, HIAA, at (202) 824-1834 or e-mail Kfyffe@hiaa.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Kathleen H. Fyffe". The signature is written in a cursive, flowing style.

CC: Secretary of Health and Human Services
National Association of Insurance Commissioners