



Health Insurance Association of America

44

DISSEMINATION BRANCH  
2000 DEC -5 A 9:09

Charles N. Kahn III  
President

December 4, 2000

Communications Division  
Office of Comptroller of the Currency  
250 E Street, SW  
Washington, DC 20219  
**Attn: Docket No. 00-20**

Ms. Jennifer Johnson, Secretary  
Board of Governors of the Federal Reserve System  
20<sup>th</sup> and C Streets, NW  
Washington, DC 20551  
**Attn: Docket No. R-1082**

Mr. Robert E. Feldman, Executive Secretary  
Attn: Comments/OES  
Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street, NW  
Washington, DC 20429  
**(RIN 3064-AC35)**

Manager, Dissemination Branch  
Information Management and Services Division  
Office of Thrift Supervision  
1700 G Street, NW  
Washington, DC 20552  
**Attn: Docket No. 2000-81**

**RE: Comments to Proposed Fair Credit Reporting Regulations**

December 4, 2000

**Health Insurance Association of America (HIAA)**

**RE: Comments to Proposed Fair Credit Reporting Regulations**

To Whom It May Concern:

The Health Insurance Association of America (HIAA) appreciates the opportunity to submit comments to the proposed regulations—"Fair Credit Reporting Regulations"—published in the Federal Register on October 20, 2000. *See* 65 Fed. Reg. 63120.

The Health Insurance Association of America (HIAA) is the nation's most prominent trade association representing the private health care system. Its nearly 300 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 provide a wide array of 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.

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 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.

We have one specific comment about the proposed rules. We believe that the definition of "opt-out information" should be revised as follows (new text is in bold italics):

**§\_\_\_.3 Definitions**

(k) *Opt out information* means information that ***would constitute a consumer report if the condition specified by §\_\_\_.3(g)(2)(iii) were not satisfied and:***

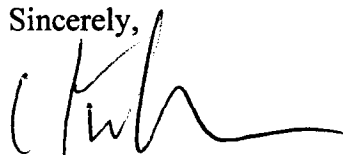
- (1) Bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living;
- (2) Is used or is expected to be used or collected in whole or in part to serve as a factor in establishing the consumer's eligibility for credit or another purpose listed in section 604 of the Act (15 U.S.C. 1681b); and
- (3) Is not a report containing information solely as to transactions or experiences between the consumer and the person reporting or communicating the information.

We believe that this additional language is necessary to clarify that, at the outset, "opt out information" must necessarily be information that would constitute a "consumer report" within the meaning of section 603(d) of the Fair Credit Reporting Act, if the condition specified in section 603(d)(2)(A)(iii) (i.e., the opt out notice requirement) were not satisfied. The proposed clarification ensures that the regulatory definition of "opt out information" tracks the statute precisely.

We appreciate the preamble's acknowledgement that it appears likely that there will be areas of overlap between the Health Insurance Portability and Accountability Act (HIPAA) and the FCRA affiliate information-sharing rules. With that in mind, we enclose for your information a background piece about some of the concerns that HIAA has about the federal statutes that may have a bearing on health insurers' handling of personal information.

HIAA appreciates the opportunity to submit comments to the proposed fair credit reporting regulations. 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](mailto:Kfyffe@hiaa.org).

Sincerely,



Enclosure

December 4, 2000

**Federal Statutes  
And  
Health Insurers' Handling of Personal Information**

There are several federal statutes that could affect health insurers' handling of personal information such as: the Health Insurance Portability and Accountability Act (HIPAA); and, the Gramm-Leach-Bliley Act (GLBA.) It will be problematic for health insurers to comply with both statutes because their privacy provisions are potentially overlapping.

Although we interpret GLBA not to apply to health information, we are aware that the federal banking agencies may take a different view. We believe that HIPAA should be the exclusive federal regulatory authority over the issue of confidentiality of health information. Without this exclusivity, health insurers are potentially subject to overlapping federal statutes.

Although the GLBA regulations appear to not apply directly to insurers, they raise important issues that could seriously affect insurers, because financial institutions with which insurers may do business are subject to the regulation and the States may look to the regulations as their model in developing their own privacy regulations for insurers.<sup>1</sup> HIAA is concerned, among other things, that the standards set forth in the GLBA final 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 HIPAA. These inconsistencies could lead to consumer confusion and significant additional – and unnecessary – costs to the health insurance industry (and ultimately consumers).

Health insurers are already subject to various federal regulations, rules, and industry standards governing the confidentiality or security of personal information. 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” in the Federal Register on August 12, 1998. On November 3, 1999, HHS proposed the second set of proposed rules for “Standards for Confidentiality of Individually Identifiable Health Information” in the Federal Register. Neither set of proposed rules has been issued in final form.

The proposed HIPAA regulations are broader than, and overlap with, the GLBA 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 GLBA regulations should work together 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 GLBA and FCRA regulations rely upon an opt-out model.

**1. The potential overlap among the personal information protected by the GLBA and HIPAA regulations will confuse consumers and make it difficult for health insurers to comply with two standards.**

Each of the regulations has differing definitions for sensitive personal information. The GLBA 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.”

The proposed HIPAA regulations cover “protected health information” (PHI). PHI is defined as “individually identifiable health information” that is electronically transmitted or maintained. 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. Further, information only becomes PHI once it is electronically transmitted or electronically maintained. Any non-electronic version of records that at any time have been electronically transmitted or maintained also comes within the definition.

Not only will this overlap cause a dilemma for regulated entities concerning how to comply with two 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.

**2. The notice requirements between the two regulations are inconsistent.**

There are differences between the GLBA regulations and the proposed HIPAA regulations for the content of notices provided to individuals who are the subject of the information being disclosed.<sup>ii</sup>

**3. 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 FCRA, 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 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.

## End Notes

<sup>i</sup> Although the GLBA final regulations clarified that the Federal Financial Agencies do not maintain jurisdiction over insurance entities, health insurers may still be required to comply with the spirit of the GLBA and regulations. In the preamble to the final rules for the privacy provisions of GLBA, the Federal Trade Commission (FTC) noted that in addition to the designated agencies, "state insurance authorities" might enforce the requirements of the GLBA pursuant to their jurisdictional authority.

<sup>ii</sup> Under HIPAA, a health plan must provide notice to individuals at the time of enrollment and when any material changes are made to the policies and procedures. The regulations state that this notification must, in plain language:

- ◆ Describe a covered entity's policies and procedures regarding uses or disclosures of protected health information ("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 (those for which an authorization is not required) 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 protected health information 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.

According to GLB, each notice must include the 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 the 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 FCRA; and
- ◆ Policies and procedures regarding the protection of the confidentiality, security, and integrity of NPI.