



March 26, 2004

Federal Trade Commission
Office of the Secretary
Room 159-H
600 Pennsylvania Ave., NW
Washington, DC 20580

Re: Alternative Forms of Privacy Notices
Project No. PO34815

Dear Sir/Madam:

I am writing on behalf of America's Health Insurance Plans (AHIP) to offer comments regarding the "Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act (GLBA)" that was published in the *Federal Register* on December 30, 2003. The Gramm-Leach-Bliley Act requires certain "financial institutions" (defined to include insurance companies) to provide their customers with an annual notice of privacy practices.

America's Health Insurance Plans is the national trade association representing the private sector in health care. AHIP's nearly 1,300 member companies provide health, long-term care, dental, vision, disability, and supplemental coverage to more than 200 million Americans. Many of our members are considered "financial institutions" as defined in Title V of GLBA.

In general, health plans and insurers are regulated by state insurance regulatory authorities with respect to their obligations under GLBA rather than the federal agencies responsible for the Interagency Proposal. We believe it is likely, however, that state regulators will look to the Interagency Proposal for guidance in drafting state privacy notice requirements for health plans and insurers. As a result, AHIP is offering these comments to clarify how individuals can best be informed of their privacy rights in an efficient and cost-effective manner.

State and Federal Privacy Requirements

AHIP's members are subject to extensive state and federal privacy requirements in addition to GLBA. The Department of Health and Human Services has promulgated comprehensive rules on the use and disclosure of health information (45 CFR Parts 160 and 164, the "privacy rule"). These rules were issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HIPAA privacy rule includes provisions requiring health plans and insurers to provide plan members and insureds with a notice of privacy practices that is more comprehensive than the GLBA notice requirements (*see*: 45 CFR 164.520). We have attached a sample HIPAA privacy notice form that we



published as a guide for our members to use as they prepared privacy notices to send to their plan members and insureds. This model form demonstrates the breadth of the privacy notice requirements imposed by the HIPAA privacy rule.

Many states also passed their own versions of the GLBA and HIPAA privacy requirements and a number of states established protections for specific types of information such as laws governing the disclosure of mental health or substance abuse treatment records. Health plans and insurers must comply with these overlapping (and at times contradictory) requirements for the use and disclosure of nonpublic personal information. For example, GLBA requires privacy notices to be sent annually to consumers whereas HIPAA requires health plans and insurers to provide the privacy notice when a member or insured is enrolled and within sixty days after a material revision is made to the notice. Health plans and insurers must also notify individuals every three years of how to obtain a copy of the privacy notice.

AHIP strongly believes there should be a single, uniform set of privacy requirements for health plans and insurers. **We recommend that the agencies responsible for the Interagency Proposal work with industry groups and Congress to clarify and streamline the federal laws and regulations applicable to the use and disclosure of health information by health plans and insurers.**

Fair and Accurate Credit Transactions Act

In addition to the federal GLBA and HIPAA privacy requirements mentioned above, some health plans and insurers are subject to information sharing provisions contained in the Fair and Accurate Credit Transactions Act that was passed last fall by Congress. The legislation amended provisions of the Fair Credit Reporting Act and includes requirements to provide individuals with notice of certain types of information disclosures involving credit reports and credit reporting agencies.

It is anticipated that the Federal Trade Commission (FTC) will publish rules later this year to carry out the provisions of that Act. Many financial institutions including some of our member companies will be impacted by these regulations and may need to modify their Notices of Privacy Practices to appropriately inform their customers about their rights as consumers. **AHIP recommends that the agencies involved with the Interagency Proposal consider including as appropriate any of the Fair and Accurate Credit Transactions Act requirements that may be established by the FTC through rulemaking.**

Model GLBA Notices

As noted, many health plans and insurers currently provide privacy notices to consumers under GLBA and the HIPAA privacy rule and may have other federal and state requirements with regards to informing plan members and insureds of their privacy rights. Some health plans and insurers developed a single privacy notice to comply with all federal and state requirements. It is important that the Interagency Proposal provide only a "model" for a GLBA privacy notice and not mandate additional requirements or formats for such notices.



This approach allows financial institutions to either adopt the model notice, in whole or in part, or to use an alternate form that better meets their individual company's compliance needs. This option is also likely to benefit consumers because it can eliminate confusion that can result from receiving multiple forms addressing the same privacy requirements. **America's Health Insurance Plans recommend that any privacy notices that are promulgated in the Interim Proposal be issued as model notices rather than as required forms.**

Electronic Disclosure Formats

America's Health Insurance Plans support the use of advanced technology to deliver privacy notices and to make them accessible in electronic formats. A number of health plans and insurers currently use websites and electronic mail to maintain relationships with their members and insureds. We believe this trend will continue to increase. **America's Health Insurance Plans encourages the use of electronic methods, such as the intranet and electronic mail, to distribute privacy notices to consumers.**

AHIP's members support protections for the confidentiality of personal financial and health information. AHIP believes that the Interagency Proposal can further this process by outlining voluntary guidelines for consumer privacy notices.

We appreciate the opportunity to comment on these important proposals. Please feel free to contact me at (202) 778-778-3259 or ddennett@ahip.net should you have any questions.

Sincerely,

A handwritten signature in cursive script, appearing to read "Diana C. Dennett".

Diana C. Dennett
Executive Vice President

Attachment



American Association of
HEALTH PLANS

The HIPAA Privacy Rule: Notice of Privacy Practices

Under the Standards for the Privacy of Individually Identifiable Health Information (the “privacy rule”), entities subject to the rule must provide an “adequate notice” of privacy practices to individuals whose protected health information (PHI) they use or disclose.

This *Regulatory Brief* discusses the rule’s requirements for providing notice of privacy practices. The *Regulatory Brief* also reviews provisions of the federal Gramm-Leach-Bliley Act (“GLB”) pertaining to privacy notices. GLB applies to financial institutions, including most health maintenance organizations and health insurers.

Attached to this *Regulatory Brief* is a sample HIPAA privacy notice that may be used by health maintenance organizations and health insurers as a guide to design their own notices.¹ The Department of Health and Human Services (HHS) has not provided a model notice, intending instead to issue general guidance to assist covered entities in implementing the notice provisions.

Who is Responsible for the Privacy Notice

In general, the privacy rule requires health plans, health care providers, and health care clearinghouses to maintain and make available privacy notices. It is important to consider, however, the privacy rule’s specific definitions of health care provider and health plan when determining whether a privacy notice is required.

¹ The sample HIPAA privacy notice was developed in consultation with privacy rule experts at several AAHP member health plans.

Not all health care providers are subject to the privacy rule. The rule defines a health care provider as any person or entity that provides medical or health services; or furnishes, bills, or is paid for health care in the normal course of business (*see* 45 CFR § 160.103). In addition, the privacy rule only applies to health care providers that transmit PHI in electronic form in connection with one or more of the HIPAA “administrative simplification” transactions.²

Privacy Notice Requirements

The privacy rule requires most health plans and health care providers to provide individuals with a notice explaining how they use or share the person’s health information. The notice must also include a description of the individual’s rights with respect to his or her PHI and what legal responsibilities are placed on the covered entity by the privacy rule.

Health plans must provide the notice before the compliance date of the privacy rule (April 14, 2003 for most health plans and April 14, 2004 for small health plans). Thereafter, plans must give the notice to any new members. In addition, health plans must provide a new notice to all members within 60 days after any material change to the contents of the notice.

² The HIPAA transactions are: health claims or equivalent encounter information; health claims attachments; enrollment and disenrollment in a health plan; eligibility for a health plan; health care payment and remittance advice; health plan premium payments; first report of injury; health claim status; and referral certification and authorization.

