Comment #: 5

America's Health Insurance Plans

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.net

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,

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.

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.

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

[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.

Background on the Privacy Rule

The privacy rule was published by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The rule governs the use and disclosure of protected health information (PHI) by health plans, certain health care providers, and health care clearinghouses.

"Covered entities" are required by the privacy rule to take a number of actions to be in compliance, including the following:

- Develop policies and procedures for using and disclosing PHI.
- Train its workforce on the requirements of the rule and the entity's privacy practices.
- Have privacy agreements with any business associate that uses or discloses PHI on its behalf.
- Only use or disclose PHI with the individual's written authorization unless such use or disclosure is for treatment, payment or health care operations.
- Establish procedures to allow individuals to have access to their PHI and to ask that the information be amended if the individual believes there are any inaccuracies.
- Allow individuals to have the use and disclosure of the information restricted in certain cases (for example, if the individual believes a disclosure would place them in danger).
- Provide a notice of how it uses and discloses PHI to individuals.

Most covered entities must comply with the rule by April 14, 2003. "Small health plans" (those with $5 million or less in annual receipts) have an additional year -- until April 14, 2004 -- to come into compliance with the privacy rule.

A "health plan" for purposes of the privacy rule includes health maintenance organizations (HMOs), health insurance issuers, and ERISA employee welfare benefit plans that provide group health benefits. HMOs and health insurance issuers are required to provide privacy notices to any individuals whose PHI is used or disclosed by the HMO or health insurance issuer. Employee welfare benefit plans that are "self-insured" are also required to provide privacy notices.

Fully insured employee welfare benefit plans (i.e., those that provide health coverage through an insurance contract with an HMO or health insurance issuer) are required to maintain a privacy notice and provide it to any person upon request if the benefit plan creates or uses PHI. This requirement, however, does not apply if the benefit plan only creates or uses the following categories of PHI:

- summary health information;
- information regarding whether the individual is participating in the benefit plan; or
- information regarding the individual's enrollment or disenrollment in the benefit plan.

"Summary health information" is defined by the privacy rule as any PHI that summarizes claims history, claims expenses, or type of claims experience and does not include any individual identifiers (e.g., name, address, etc.) except for five digit zip codes (*see* 45 CFR § 164.504 (a)).

HMOs and health insurance issuers may be asked by their contracting employee welfare benefit plans to develop privacy notices for the benefit plan. In these situations, the HMO or health insurance issuer should carefully review the privacy rule provisions to determine if a notice of privacy practices is required, what information to include in the notice, and whether drafting the privacy notice on behalf of their clients is appropriate.

The sample HIPAA privacy notice attached to this *Regulatory Brief* is intended for use by HMOs or health insurance issuers only. The sample notice does not include any additional disclosures or notice requirements that may be required under

the regulation when employee welfare benefit plans maintain or provide privacy notices.

Joint Notices of Privacy Practices

The privacy rule allows covered entities that participate in an "organized health care arrangement" (OHCA) to comply with the regulation by producing a single notice that describes their combined privacy practices. (45 CFR 164.520(d)). One or more covered entities participating in an OHCA may provide a joint notice. An OHCA includes the following types of arrangements:

- Clinically integrated care settings in which individuals typically receive health care from multiple health care providers.
- An organized system of health care in which one or more covered entities participates, they hold themselves out to the public as participating in a joint arrangement, and they participate in joint activities such as utilization review, quality assessment or payment activities.
- Multiple group health benefit plans maintained by the same plan sponsor.
- An employee welfare benefit plan and one or more HMOs or health insurance issuers that provide insurance coverage to the plan's participants. (45 CFR § 164.501)

If covered entities are involved in an OHCA and send out a joint privacy notice, the entities must all agree to abide by the terms of the notice and must disclose all of the covered entities (or classes of entities) that are participating in the OHCA as part of the notice of privacy practices.

Who Gets the Notice and When

All covered entities required to produce a notice must provide the notice upon request by any person -- HHS intends the notice to be a public document that individuals can use when choosing between covered entities.

Health plans are required to distribute the notice to all individuals covered by the health plan. If a named insured and one or more dependents are covered by same policy, health plans may satisfy the distribution requirement by sending the privacy notice to the named insured on behalf of any dependents. Employee welfare benefit plans may distribute the privacy notice to each covered employee (*see* 65 Fed. Reg. 82723 (2000)).

Health plans must send out their first privacy notice no later than the compliance date of the privacy rule (April 14, 2003 or, in the case of "small health plans," April 14, 2004). Thereafter, plans must provide the privacy notice to any new enrollees in the plan and to all individuals within 60 days after the plan makes a material revision to the contents of the privacy notice. In addition, health plans must notify all individuals covered by the plan at least once every three years of the availability of the privacy notice and how to obtain a copy.

Health care providers that have a direct treatment relationship with an individual must provide the privacy notice no later than the first time the provider "delivers service" to the individual after the April 14, 2003 compliance date of the privacy rule. If there is an emergency treatment situation, the provider must provide the privacy notice, "as soon as reasonably practicable" after such treatment (*see* 45 CFR § 164.520 (c)(2)).

Health care providers with a direct treatment relationship must make a good faith effort to obtain the individual's written acknowledgement that they received a copy of the privacy notice. If the individual refuses to sign the acknowledgement, the provider must document that they tried to obtain the acknowledgment but were unable to do so. The written acknowledgement is not required, however, in an emergency treatment situation.

In addition, all health care providers that are subject to the rule that maintain a physical delivery site must provide a copy of its privacy notice if requested and post it in a location where

it will likely be seen by individuals seeking services from the provider. Covered entities, including health plans, that maintain a web site must prominently post the privacy notice on the web site and make a copy electronically available through the site.

Use of "Plain English" and Notices for Non-English Speakers

The privacy notice must be written in "plain language." Although the rule does not include any specific directions regarding the format of the notice, HHS has provided the following guidance on the plain language requirement:

> A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice, using "you" and other pronouns; use common, everyday words in sentences; and divide material into short sections. (65 Fed. Reg. 82548 (2000)).

The privacy rule does not require that the privacy notice be printed in languages other than English. The preamble to the regulation, however, indicates that covered entities receiving any type of federal assistance must comply with Title VI of the 1964 Civil Rights Act which requires such programs to take reasonable steps to serve populations that have limited proficiency in the English language (*see* 65 Fed. Reg. 82549 (2000)). HHS has published detailed guidance for health care providers and health plans that provide services to groups of individuals with limited English proficiency (*see* HHS Office for Civil Rights, Policy Guidance on the Prohibition Against National Origin Discrimination as it Affects Persons With Limited English Proficiency, 67 Fed. Reg. 4968 (2002)).[3]

HHS also encourages covered entities to assist individuals who are unable to read the entity's privacy notice. For example, a covered entity could read the privacy notice to such individuals, or could prepare a video presentation that explains its privacy notice (*see* 65 Fed. Reg. 82549 (2000)).

What Should be Included in the Notice

In general, the privacy rule requires covered entities to inform individuals as to:

- how the covered entity uses or discloses PHI;
- what the individual's rights are with respect to his or her PHI; and
- what the covered entity's legal duties are with respect to using or disclosing the individual's PHI.

Uses and Disclosures of PHI

The privacy notice must include the following information about the covered entity's privacy practices:

- a description (including examples) of the entity's uses and disclosures of PHI for treatment, payment, and health care operations;
- a description of any other uses or disclosures of PHI that the entity is allowed to make without the individual's written authorization;
- a statement that all other uses or disclosures of PHI will only be made after the individual provides his or her written authorization (and instructions on how the individual can revoke the authorization);
- a description of any applicable restrictions on the use or disclosure of PHI that may be required by other state or federal laws;

[3] There are also a number of other state and federal laws that require efforts to assist individuals with limited English proficiency with understanding of printed materials. According to the HHS Office for Civil Rights, at least 26 states and the District of Columbia have enacted laws requiring assistance to individuals with limited English proficiency, including provision of interpreters and translation of forms and other written materials.

- if applicable, a statement that the entity intends to use or disclose PHI to provide the individual: (a) with appointment reminders; or (b) with information about other health-related benefits and services or treatment alternatives;
- if applicable, a statement that the entity may contact the individual to raise funds for the covered entity; and
- in the case of an HMO or health insurance issuer, that the entity may share PHI with the sponsor of an employee welfare benefit plan.

Rights of Individuals

The privacy notice must inform the individual of his or her rights with respect to their protected health information:

- the right to inspect and copy PHI that is maintained by the entity and its business associates;
- the right to ask the covered entity to restrict how it uses or discloses PHI in certain circumstances;
- the right to receive a confidential communication of PHI in certain circumstances;
- the right to receive an accounting of how the covered entity has used or disclosed his or her PHI;
- the right to amend protected health information; and
- the right to obtain a paper copy of the notice from the covered entity upon request, including where the individual has agreed to receive the notice electronically.

Covered Entity's Responsibilities

The privacy notice must include information regarding the covered entity's legal responsibilities, including:

- a statement that the entity is required by law to maintain the privacy of PHI and to provide the privacy notice;
- a statement that the entity is required to abide by the terms of the privacy notice;
- a statement that the entity reserves the right to change its privacy practices and that it will give individuals notice of any material revisions;
- a statement that individuals who believe their privacy rights have been violated may file a complaint with the covered entity and HHS, and that the covered entity will not retaliate against the individual if they file a complaint;
- the name of a contact person or office within the covered entity where the individual may ask questions about the entity's privacy policies; and
- the effective date of the notice.

In addition, the privacy rule specifically requires every privacy notice to include the following statement, either as a header or otherwise prominently displayed:

> THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Gramm-Leach-Bliley Act

Compliance with regulatory requirements for privacy notices is further complicated for HMOs and health insurance issuers by a 1999 federal law, the Gramm-Leach-Bliley Act (GLB) (PL 106-102, 15 USC 6801 *et seq.*). Title V of GLB directed state insurance regulators to issue regulations to protect the privacy of financial information held by insurers. The GLB provisions also require that privacy notices be provided to consumers in certain situations.

On its face, GLB applies only to "nonpublic personal information" that is maintained by "financial institutions." GLB defines these terms broadly, however, and they may be interpreted to include PHI that is used or disclosed by HMOs and health insurance issuers.

GLB requires a financial institution to provide consumers with a clear statement of its policies regarding:

- the disclosure of nonpublic personal information to affiliates and "non-affiliated third parties;"
- the disclosure of nonpublic personal information of individuals who are no longer customers of the financial institution; and
- how the financial institution protects its customers' nonpublic personal information.

In addition, a financial institution is prohibited from disclosing nonpublic personal information to a non-affiliated third party unless the consumer is first provided the opportunity to "opt-out" of such disclosures. There are a number of exceptions to this requirement, including disclosures for the business operations of the financial institution such as for marketing. (*See* 15 USC 6802).

In the case of HMOs and health insurance issuers, GLB is enforced by the applicable state regulatory agency. States have taken a variety of approaches to GLB enforcement. Some states have taken the position that they have the authority to enforce the federal statute in the absence of specific regulations using state unfair trade practice statutes or similar laws.

Other states have enacted legislation that specifically allows the state regulatory agency to enforce the GLB provisions or have promulgated a version of the National Association of Insurance Commissioners' Model Regulation on the Privacy of Consumer Financial and Health Information (NAIC Model Privacy Rule). Finally, some states have approved laws or regulations that provide that HMOs and health insurance issuers are compliant with the GLB requirements if they are in compliance with the HIPAA privacy rule.

Given the overlap in substantive notice requirements of the HIPAA privacy rule and GLB, for many HMOs and health insurers, compliance with the HIPAA privacy rule may be sufficient to meet most of the privacy notice requirements of GLB. (The GLB requirement that consumers be provided with the opportunity to "opt-out" of certain disclosures of nonpublic personal information probably will not apply to most, if not all, uses or disclosures of PHI in the normal course of business.) It is important, however, for HMOs and health insurance issuers to familiarize themselves with the requirements of GLB and how their state regulatory authority intends to enforce the federal statute. Because of the different regulatory requirements of GLB and the privacy rule, HMOs and health insurers may decide to send out separate privacy notices in order to comply with both laws.

Sample Privacy Notice

An example of a privacy notice for use by HMOs and health insurance issuers is attached. The sample privacy notice is a draft. The sample privacy notice should serve as a starting point for the development of a privacy notice that meets the business needs of, and regulatory requirements applicable to, health plans. Legal counsel should be consulted when developing the privacy notice.

The notice is intended to reflect the privacy rule provisions that apply to health maintenance organizations and health insurers. The sample privacy notice does not include privacy rule requirements applicable to other types of covered entities such as health care providers or employee welfare benefit plans.

A copy of the privacy rule and related materials are available on AAHP's web site at: www.aahp.org under "Our Issues > HIPAA & Privacy.

If you have questions, please contact Tom Wilder, Executive Director, Private Market Regulation (202-778-3255 or twilder@aahp.org) or Melissa Bartlett, Director, Private Market Regulation (202-861-1473 or mbartlett@aahp.org).

Attachment A

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

XYZ HEALTH PLAN PRIVACY NOTICE

Effective April 14, 2003

Drafting Note: The notice must include the date on which the notice is first in effect. Small health plans (those with $5 million or less in annual receipts), have until April 14, 2004 to comply with the privacy rule.

At XYZ Health Plan, we respect the confidentiality of your health information and will protect your information in a responsible and professional manner. We are required by law to maintain the privacy of your health information and to send you this notice.

This notice explains how we use information about you and when we can share that information with others. It also informs you of your rights with respect to your health information and how you can exercise those rights.

When we talk about "information" or "health information" in this notice we mean the following:

Drafting Note: Although "protected health information" is defined in the privacy rule at 45 CFR § 164.501, health plans may wish to develop their own definition.

How We Use or Share Information

The following are ways we may use or share information about you:

- We may use the information to help pay your medical bills that have been submitted to us by doctors and hospitals for payment.
- We may share your information with your doctors or hospitals to help them provide medical care to you. For example, if you are in the hospital, we may give them access to any medical records sent to us by your doctor.
- We may use or share your information with others to help manage your health care. For example, we might talk to your doctor to suggest a disease management or wellness program that could help improve your health.
- We may share your information with others who help us conduct our business operations. **We will not share your information with these outside groups unless they agree to keep it protected.**
- We may use or share your information for certain types of public health or disaster relief efforts.

- ❖ We may use or share your information to send you a reminder if you have an appointment with your doctor.
- ❖ We may use or share your information to give you information about alternative medical treatments and programs or about health related products and services that you may be interested in. For example, we might send you information about smoking cessation or weight loss programs.
- ❖ We may use or share your information to share information with an employee benefit plan through which you receive health benefits. **We will not share detailed health information with your benefit plan unless they promise to keep it protected.**

Drafting Note: If you intend to contact your members for fund raising efforts as permitted by the privacy rule you should include the following.

- ❖ We may contact you to raise funds for our charitable foundation [insert name of foundation].

There are also state and federal laws that may require us to release your health information to others. We may be required to provide information for the following reasons:

- ➢ We may report information to state and federal agencies that regulate us such as the US Department of Health and Human Services and the [insert name of state regulatory agency].
- ➢ We may share information for public health activities. For example, we may report information to the Food and Drug Administration for investigating or tracking of prescription drug and medical device problems.
- ➢ We may report information to public health agencies if we believe there is a serious health or safety threat.
- ➢ We may share information with a health oversight agency for certain oversight activities (for example, audits, inspections, licensure and disciplinary actions.)
- ➢ We may provide information to a court or administrative agency (for example, pursuant to a court order, search warrant or subpoena).
- ➢ We may report information for law enforcement purposes. For example, we may give information to a law enforcement official for purposes of identifying or locating a suspect, fugitive, material witness or missing person.
- ➢ We may report information to a government authority regarding child abuse, neglect or domestic violence.
- ➢ We may share information with a coroner or medical examiner to identify a deceased person, determine a cause of death, or as authorized by law. We may also share information to funeral director as necessary to carry out their duties.
- ➢ We may use or share information for procurement, banking or transplantation of organs, eyes, or tissue.
- ➢ We may share information relative to specialized government functions, such as military and veteran activities, national security and intelligence activities, and the protective services for the President and others.

- We may report information on job-related injuries because of requirements of your state worker compensation laws.

Drafting Note: The privacy notice must also include a description of how your uses and disclosures of information may be prohibited or materially limited by other applicable federal or state law.

If one of the above reasons does not apply, **we must get your written permission to use or disclose your health information.** If you give us written permission and change your mind **you may revoke your written permission at any time.**

WHAT ARE YOUR RIGHTS

The following are your rights with respect to your health information. If you would like to exercise the following rights, please contact us [insert contact information and procedures for making a request].

- ***You have the right to ask us to restrict*** how we use or disclose your information for treatment, payment, or health care operations. You also have the right to ask us to restrict information that we have been asked to give to family members or to others who are involved in your health care or payment for your health care. *Please note that while we will try to honor your request, we are not required to agree to these restrictions.*

- ***You have the right to ask to receive confidential communications*** of information. For example, if you believe that you would be harmed if we send your information to your current mailing address (for example, in situations involving domestic disputes or violence), you can ask us to send the information by alternative means (for example, by fax) or to an alternative address. We will accommodate your reasonable requests as explained above.

Drafting Note: You may want to determine how you will describe "alternative means" and explain in further detail.

- ***You have the right to inspect and obtain a copy*** of information that we maintain about you in your designated record set. A "designated record set" is [insert definition].

Drafting Note: Although the privacy rule includes a definition of "designated record set" (45 CFR 164.501), health plans may want to develop their own definition.

However, you do not have the right to access certain types of information and we may decide not to provide you with copies of the following information:

- contained in psychotherapy notes;
- compiled in reasonable anticipation of, or for use in a civil criminal or administrative action or proceeding; and
- subject to certain federal laws governing biological products and clinical laboratories.

In certain other situations, we may deny your request to inspect or obtain a copy of your information. If we deny your request, we will notify you in writing and may provide you with a right to have the denial reviewed.

❖ ***You have the right to ask us to make changes*** to information we maintain about you in your designated record set. These changes are known as amendments. We may require that your request be in writing and that you provide a reason for your request. We will respond to your request no later than 60 days after we receive it. If we are unable to act within 60 days, we may extend that time by no more than an additional 30 days. If we need to extend this time, we will notify you of the delay and the date by which we will complete action on your request.

If we make the amendment, we will notify you that it was made. In addition, we will provide the amendment to any person that we know has received your health information. We will also provide the amendment to other persons identified by you.

If we deny your request to amend, we will notify you in writing of the reason for the denial. The denial will explain your right to file a written statement of disagreement. We have a right to respond to your statement. However, you have the right to request that your written request, our written denial and your statement of disagreement be included with your information for any future disclosures.

❖ ***You have the right to receive an accounting*** of certain disclosures of your information made by us during the six years prior to your request. Please note that we are not required to provide you with an accounting of the following information:

- Any information collected prior to April 14, 2003

Drafting Note: April 14, 2004 for small health plans.

- Information disclosed or used for treatment, payment, and health care operations purposes.
- Information disclosed to you or pursuant to your authorization;
- Information that is incident to a use or disclosure otherwise permitted.
- Information disclosed for a facility's directory or to persons involved in your care or other notification purposes;
- Information disclosed for national security or intelligence purposes;
- Information disclosed to correctional institutions, law enforcement officials or health oversight agencies;

- Information that was disclosed or used as part of a limited data set for research, public health, or health care operations purposes.

We may require that your request be in writing. We will act on your request for an accounting within 60 days. We may need additional time to act on your request. If so, we may take up to an additional 30 days. Your first accounting will be free. We will continue to provide you with one free accounting upon request every 12 months. If you request an additional accounting within 12 months of receiving your free accounting, we may charge you a fee. We will inform you in advance of the fee and provide you with an opportunity to withdraw or modify your request.

EXERCISING YOUR RIGHTS

- **You have a right to receive a copy of this notice upon request at any time.** You can also view a copy of the notice on our web site at [insert web site URL]. Should any of our privacy practices change, we reserve the right to change the terms of this notice and to make the new notice effective for all protected health information we maintain. Once revised, we will provide the new notice to you by direct mail and post it on our website.

- If you have any questions about this notice or about how we use or share information, please contact [insert contact person or office] at (800) [insert contact telephone number]. That office is open Monday through Friday from 9:00 a.m. to 5:00 p.m. You can also send us questions by e-mail at [insert contact email address].

If you believe your privacy rights have been violated, you may file a complaint with us by [insert contact information and address and/or telephone number.] You may also notify the Secretary of the U.S. Department of Health and Human Services of your compliant. **WE WILL NOT TAKE ANY ACTION AGAINST YOU FOR FILING A COMPLAINT.**

Drafting Note: You may want to provide the address and telephone number of the Office for Civil Rights at HHS which is responsible for enforcement of the privacy rule although providing the address and telephone number are not required by the rule.