Trustmark Insurance Company
Trustmark Life Insurance Company

HIPAA Privacy Rule Information Packet Contents

1. Plan Sponsor Cover Letter (ASO)

2. Documents to be **reviewed, signed and returned to Trustmark within 7 days after receipt of these materials**:

   a. Plan Sponsor Certification to the Group Health Plan
   b. List of Authorized Representatives
   c. Business Associate Agreement

3. Documents you may want to consider copying and distributing to your Trustmark covered employees:

   a. Notice of Privacy Practices
   b. HIPAA Privacy Amendment

4. Frequently Asked Questions about HIPAA Privacy

5. Resources for additional HIPAA Information

Please return signed documents to Trustmark within 7 days after receipt of these materials.

Mail to: Trustmark Insurance Company
HIPAA G445
400 Field Drive
Lake Forest, IL 60045-2581

Trustmark

INSURANCE COMPANY

Dear ASO Plan Sponsor:

HIPAA Privacy Regulations went into effect April 14, 2003. Trustmark is providing you with the enclosed packet of information to help you understand the implications and requirements of this complex legislation.

What is HIPAA?
HIPAA stands for The Health Insurance Portability and Accountability Act of 1996. The Privacy Rule aspect of HIPAA creates national standards regarding Protected Health Information (PHI), which is defined as any information that could tie a specific health condition to a specific patient or healthcare consumer. This could include name, address and Social Security number in connection with any reference to a particular treatment or condition.

The Privacy Rules govern how entities covered under HIPAA, such as your health plan, use and share PHI. The rules also include provisions to help individuals understand and control how their health information is used.

What are my responsibilities under the HIPAA Privacy Rules?
Because HIPAA applies to you as a plan sponsor of a group health benefit plan, you have responsibilities under this law. Trustmark is providing you with this packet of information in order to assist your health plan in complying with the regulation. The nature of the administrative requirements associated with self-funding includes the receipt of PHI by your health plan. **Trustmark requires that you:**

1. Review, complete and sign the Plan Sponsor Certification and the List of Authorized Representatives
   Please return to Trustmark within 7 days after receipt of these materials and instructions.
2. Complete and sign the Business Associate Agreement
   Please return to Trustmark within 7 days after receipt of these materials and instructions. (You may use an identical version of this agreement, less Trustmark's name, with your other business associates.)

Trustmark asks that you:

1. Consider using the enclosed sample Notice of Privacy Practices and distribute to your employees.
2. Consider using the enclosed sample HIPAA Privacy Amendment and distribute to your employees.

Please note: The enclosed information constitutes our interpretation of HIPAA Privacy Rules and is not intended as legal advice. Trustmark encourages you to review the laws and to seek the advice of your own counsel.

Under the HIPAA Privacy Rules, Trustmark Insurance Company is not a covered entity with regards to our self-funded clients. We are a Business Associate of your health benefit plan and will be compliant with these rules by April 14, 2003. If you have specific questions regarding the information contained in this packet, please contact your Trustmark sales representative.

Sincerely,

Trustmark Insurance Company
and
Trustmark Life Insurance Company

Plan Sponsor Certification

- ❑ **Complete, sign and return the attached Plan Sponsor Certification to Trustmark within 7 days after receipt of these materials.**

List of Authorized Representatives

- ❑ **Complete, sign and return the attached List of Authorized Representatives to Trustmark within 7 days after receipt of these materials.**

TRUSTMARK INSURANCE COMPANY
TRUSTMARK LIFE INSURANCE COMPANY

PLAN SPONSOR CERTIFICATION TO THE GROUP HEALTH PLAN

During the term of this group health benefit plan you, the plan sponsor, may receive Protected Health Information. As set forth in the HIPAA Privacy Rule ("Rule"), Protected Health Information ("PHI") includes individually identifiable health information and relates to the past, present, or future:

- condition of an individual's physical or mental health;
- health care provided to an individual; or
- payment for health care provided to an individual.

As plan sponsor of a self-funded or minimum premium group health plan, you will receive PHI from us. The HIPAA Privacy Rule requires that you, the plan sponsor, must agree to safeguard and protect the confidentiality of any PHI you receive. This will be accomplished by the completion and return of this Certification and the attached List of Authorized Representatives. The plan sponsor also agrees to amend the plan document of the group health plan consistent with this Certification.

PLAN SPONSOR CERTIFICATION

I, the plan sponsor, or the designated representative of the plan sponsor, certify that the plan sponsor will:

- not use or disclose PHI for employment-related actions and decisions, or in connection with any other benefit or employee benefit plan of the plan sponsor.

- Not use or disclose to anyone the PHI of any individual covered under this group health benefit plan other than as described in this Certification, and permitted or required by the HIPAA Privacy Rule and other applicable law.

- Ensure that any agents, including subcontractor, to whom I provide PHI, agree to the same restrictions and conditions that apply to the plan sponsor in connection with the HIPAA Privacy Rule.

- Report to the group health benefit plan any use or disclosure of the information that is inconsistent with the uses or disclosures permitted or required by the HIPAA Privacy Rule and other applicable law.

- Make available PHI as required in the Rule for Access of Individuals to their own PHI.

- Make available PHI as required in the Rule in order to amend PHI and incorporate any amendment to PHI in accordance with the Rule.

- Make available the information required to provide an accounting of disclosures of PHI as required by the Rule.

- Make its internal practices, books and records relating to the use and disclosure of PHI received from the group health benefit plan available to the Secretary of the Department of Health and Human Services.

- Return or destroy, if feasible, all PHI received from the group health benefit plan that the plan sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made. If destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

- Provide a List of Authorized Representatives which includes the identity or job title and affiliation of persons required or permitted to receive information in order to perform services on behalf of the group health benefit plan (e.g. claim administrator, case management vendor, pharmacy benefit manager, claim subrogation vendor, claim auditor, provider network manager, utilization and review management vendor, stop loss insurance carrier, insurance broker/consultant), and any other entity subcontracted to assist in administrating the health plan.

- Provide PHI only to those individuals or entities identified on the List of Authorized Representatives.

- Provide an effective mechanism for resolving any issues of noncompliance with the provision of this Certification.

Name of Group Health Benefit Plan (Employer):_____

Group Number:_____

Signed by (Plan Sponsor):_____

Print Name and Title:_____

Date:_____

TRUSTMARK INSURANCE COMPANY
TRUSTMARK LIFE INSURANCE COMPANY

LIST OF AUTHORIZED REPRESENTATIVES

The following individuals perform administrative functions for my group health plan and may have access to Protected Health Information (PHI) or summary health information. These individuals are authorized to discuss PHI that is the minimum necessary to administer the group health plan. ******The primary function must be described in detail and all duties specifically outlined. If more space is needed, please use another sheet of paper.***

Group Name: _____ Group Number: _____

Name and Title of Person: _____

Company Name: _____

***KEY – for Primary Function(s) usage of information:**
LMTD: Limited access - an individual who works with enrollment, termination, COBRA, etc. – needs no additional health information)
CLMS 1: Individual who needs to check status of claims – minimal PHI to include eligibility information
CLMS 2: Assists participants in filing claims or appeals on claims denials – should have access to all claims data, including eligibility, upon request)
FINANCE: Individual to whom we are to deliver reports related to financial maintenance of the coverage (e.g. check register, etc.)

Primary Function(s)* with regard to the group health benefit plan:

___ LMTD ___ CLMS 1 ___ CLMS 2 ____FINANCE ___ OTHER

If other, how does the Authorized Person use or disclose PHI in the performance of their job duties?

_____

_____

Name and Title of Person: _____

Company Name: _____

Primary Function(s)* with regard to the group health benefit plan:

___ LMTD ___ CLMS 1 ___ CLMS 2 ____FINANCE ___ OTHER

If other, how does the Authorized Person use or disclose PHI in the performance of their job duties?

_____

_____

Name and Title of Person: _____

Company Name: _____

Primary Function(s)* with regard to the group health benefit plan**:

___ LMTD ___ CLMS 1 ___ CLMS 2 ____FINANCE ___ OTHER

If other, how does the Authorized Person use or disclose PHI in the performance of their job duties?

_____

_____

(If more space is needed, please use another sheet of paper.)

If there are any changes to be made to this list, additions or deletions, the plan sponsor is required to notify us within 30 days of the change.

Signed by: _____

Title: _____ Date: _____

Business Associate Agreement

- ❑ **<u>Complete, sign and return</u> the attached Business Associate Agreement to Trustmark within 7 days after receipt of these materials.**

TRUSTMARK INSURANCE COMPANY
TRUSTMARK LIFE INSURANCE COMPANY
Lake Forest, Illinois

BUSINESS ASSOCIATE AGREEMENT

I. PREAMBLE

Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, and its implementing regulation, the Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 *et seq*. (Dec. 28, 2000), the Final Rule, (Aug. 14, 2002), and future amendments to the implementing Regulation, (hereinafter the "HIPAA Privacy Rule"), as well as other applicable federal and state privacy and confidentiality rules, _____{"Covered Entity" **(Name of Group Health Benefit Plan)}** and **Trustmark Insurance Company and Trustmark Life Insurance Company** ("Business Associate") (jointly "the Parties") wish to enter into an Agreement that addresses the requirements of the HIPAA Privacy Rule with respect to "business associates," as that term is defined in the HIPAA Privacy Rule.

Specifically, this Agreement is intended to ensure that the Business Associate will establish and implement appropriate safeguards (including certain administrative requirements) for "Protected Health Information" the Business Associate may create, receive, use, or disclose in connection with certain functions, activities, or services (collectively "services") to be provided by Business Associate to or on behalf of Covered Entity. The services to be provided by Business Associate are identified in a separate agreement ("Services Agreement") between the Parties.

The Parties acknowledge and agree that in connection with the services to be provided, Business Associate may create, receive, use or disclose Protected Health Information. Protected Health Information ("PHI"), which is defined in the Rule, includes individually identifiable health information that is created or received by a covered entity (provider, health plan, clearinghouse or insurer), a health authority, employer, school or university, maintained or transmitted in any form or medium, which relates to the past, present, or future (i) physical or mental health or condition of an individual; (ii) provision of health care to an individual; *or* (iii) payment for the provision of health care to an individual. PHI does not include summary health information or information that has been de-identified in accordance with the standards for de-identification provided for in the HIPAA Privacy Rule.

In connection with Business Associate's creation, receipt, use or disclosure of PHI as a Business Associate of the Covered Entity, Business Associate and Covered Entity agree as follows:

II. GENERAL TERMS AND CONDITIONS

a. **Definitions:** All terms used in this Agreement shall have the meanings set forth in the HIPAA Privacy Rule, unless otherwise defined herein.

b. **Existing Services Agreements:** All existing Services Agreements between the Covered Entity and Business Associate are subject to this Agreement and are hereby amended by this Agreement. In the event of conflict between the terms of any Services Agreement and this Agreement, the terms and conditions of this Agreement shall govern.

c. **Services Agreements:** include any agreement and amendments thereto, written or oral, between Covered Entity and Business Associate that describe services to be provided in connection with Covered Entities' Covered Functions. Such Services Agreements include but are not limited to; vendor agreements with Preferred Provider Organizations, claim repricing organizations, or retainer agreements with law firms.

d. Where provisions of this Agreement are different from those mandated by the HIPAA Privacy Rule, but are nonetheless permitted by the Rule, the provisions of the Agreement shall control.

e. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Business Associates and the respective successors or assigns of the Business Associates, any rights, remedies, obligations, or liabilities whatsoever.

III. USE AND DISCLOSURE OF PHI

a. **Treatment, Payment and Operations:** Business Associate agrees to create, receive, use, or disclose PHI only in a manner that is consistent with this Agreement or the HIPAA Privacy Rule and only in connection with providing the services to or on behalf of Covered Entity identified in any existing Services Agreement and amendments thereto.

Accordingly, in providing services to or on behalf of for the Covered Entity, the Business Associate, for example, will be permitted to use and disclose PHI for Treatment, Payment and Healthcare Operations consistent with the HIPAA Privacy Rule, without obtaining authorization.

b. **Other Permissible Uses and Disclosures:** As permitted by 42CFR §164.504(e)(4) Business Associate also may use or disclose PHI it receives in its capacity as a Business Associate to the Covered Entity if:

(i) the *use* relates to: (1) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (2) data aggregation services relating to the health care operations of the Covered Entity; or

(ii) the *disclosure* of PHI received in such capacity may be made in connection with a function, responsibility, or service identified in (i)(1), *and* such disclosure is required by law *or* the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality.

IV. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. **SubContractors:** Business Associate represents to Covered Entity that [i] any disclosure it makes will be permitted or required under applicable laws, and [ii] that Business Associate will obtain reasonable assurances from any person or entity to whom Business Associate discloses the PHI that the PHI will be held confidentially and used or further disclosed only as required and permitted under the HIPAA Privacy Rule and other applicable laws, and [iii] any such person or entity agrees to be governed by the same restrictions and conditions contained in this Agreement, and that such person will notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

b. **Permissible Disclosures:** Except as otherwise limited in this Agreement, Business Associate may disclose PHI to other Business Associates of the Covered Entity (i) as directed by the plan sponsor, or (ii) to perform its duties under the Service Agreement.

c. **Safeguards:** Business Associate shall maintain safeguards as necessary to ensure that PHI is not used or disclosed except as provided for by this Agreement.

d. **Impermissible Use and Disclosure:** [I] Business Associate shall report to Covered Entity within 5 days of knowledge of any use or disclosure of PHI that is in violation of this agreement and not permitted under the HIPAA Privacy Rule. [ii] Business Associate agrees to mitigate any harmful effect that is known to Business Associate of such impermissible use or disclosure of Protected Health Information.

e. **Accounting of Disclosures:** Business Associate shall provide Covered Entity within 5 days of receipt of Covered Entity's request, the information necessary to provide an accounting of disclosures of PHI as provided for in C.F.R. § 164.528 of the HIPAA Privacy Rule.

f. **Access to PHI:** Business Associate shall report to Covered Entity within 5 days of receipt of a request from an individual for access to PHI provided for in C.F.R. § 164.524 of the HIPAA Privacy Rule. Business Associate shall not respond to individual requesting Access to PHI without specific authorization of Covered Entity.

g. **Amendment of PHI:** Business Associate shall report to Covered Entity within 5 days of receipt of a request from an individual for amendment to PHI. Business Associate shall not alter or amend PHI it receives from an individual or from Covered Entity without specific authorization by Covered Entity as provided for in C.F.R. § 164.526 of the HIPAA Privacy Rule.

h. **Disclosures Required by Law:** Business Associate may disclose PHI to Covered Entity for the purpose of reporting violations of law to appropriate Federal or State authorities, consistent with C.F.R § 164.502.

i. **Access to HHS:** Business Associate shall make available to the Covered Entity, HHS or its agents the Business Associate's internal practices, books and records relating to the use and disclosure of PHI as required in C.F.R. § 164.504 of the HIPAA Privacy Rule.

j. Business Associate shall cooperate with Covered Entity to comply with the HIPAA Privacy Rule as well as other applicable federal and state privacy and confidentiality rules.

V. OBLIGATIONS OF COVERED ENTITY

a. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

b. Covered Entity shall provide Business Associate with any changes in, or revocation of, or authorization by individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522.

VI. TERMINATION

a. **Termination for Cause:** Covered Entity will provide Business Associate 10 days to cure any material breach of this Agreement. If Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, the Parties agree that Covered Entity shall have the right to terminate the Services Agreement for cause and without any penalty.

b. **Termination not feasible:** If termination would cause irreparable business interruption or harm to customers of Covered Entity, or is otherwise not feasible, parties shall make all efforts reasonable to cure breach or mitigate harm to individuals caused by such breach. If this occurs, Covered Entity may report the situation to the Secretary of Health and Human Services.

c. **Return or Destruction of PHI:** Upon the termination or expiration of this Agreement or the Services Agreement, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or further protect the PHI if return or destruction is not feasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Covered Entity	**Business Associate**
Signed*:* _____	**Signed***:* _____
Print Name*:* _____	**Print Name***:* _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

Notice of Privacy Practices

- ❑ **<u>Consider using</u> the attached Notice of Privacy Practices for distribution to all your covered employees.**

(We, Us, Our)

NOTICE OF PRIVACY PRACTICES
Effective: April 14, 2003

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.

Introduction
In order to provide insurance coverage and/or health plan administrative services, we must obtain and maintain Protected Health Information (PHI). This privacy notice describes the types of information that is collected and your rights regarding how that information can be used.

PHI is individually identifiable health information that is created or received by your provider, your health plan or insurer, a data clearinghouse, a health authority, employer, school or university. PHI can be maintained or transmitted in any form or medium. It relates to the past, present or future:

- condition of your physical or mental health;
- health care provided to you; or
- payment for the health care provided to you.

PHI does not include summary health information or information that has been de-identified according to the standards for de-identification provided for in the HIPAA Privacy Rule.

Permitted/Required Uses and Disclosures of PHI
Your PHI will be used and disclosed for the purpose of routine treatment, payment and health care operations.

Use and Disclosure for Treatment
Your PHI may be used by, and disclosed to, health care providers including, but not limited to, doctors, nurses, laboratory technicians, medical students and other health care personnel involved in your treatment.

Use and Disclosure for Payment
Your PHI may be used by, and disclosed to, individuals involved in the collection of your premium and the payment of your benefits and other claims administration, including claim payment and adjudication or subrogation of health benefit claims. The use and disclosure also includes verification of participation or enrollment in the plan, eligibility for coverage and plan benefits. Your PHI may be shared with persons involved in utilization review, including pre-certification, pre-authorization, and concurrent and retrospective review, to assist in reimbursement of health care claims or other claims payment.

Use and Disclosure for Health Care Operations
Your PHI may be used and disclosed for plan operation purposes including, but not limited to: underwriting; premium rating; billing and premium adjustments; submitting claims; placing a contract for reinsurance of risk relating to claims for health care, including stop-loss and excess loss insurance; quality review assessments; audits, including fraud and abuse detection and compliance programs; business management and planning; the sale, transfer, merger or consolidation of a covered entity; legal or administrative services; actuarial pricing, studies and review; complaint review; and regulatory review and other legal compliance. In addition, your PHI may be used and disclosed for case management, and care coordination, contacting of health care providers and patients with information about treatment, drug and disease management alternatives and other related functions that do not include treatment.

We may share this information with our business associates for purposes of utilization reviews, appropriateness of care reviews, peer review for resolution of grievances, consultation with outside health care providers, consultants and attorneys, and other health related benefits and services that may be of interest to you. We require our business associates to sign an agreement specifying their compliance with our privacy policies.

We have developed privacy policies and procedures in order to ensure the privacy of your PHI. These policies and procedures are based on appropriate administrative, technical and physical safeguards necessary to maintain confidentiality. Access to your PHI is limited to those individuals that have a legitimate business need for that information. This protection extends to the use of your PHI by our business associates.

Other Permitted/Required Uses and Disclosures of PHI
We, or our approved business associates, may use and disclose your protected health information for reasons permitted by the Rule, including but not limited to the following:

- those required by law;
- in response to a court order or other legal proceeding;
- judicial and administrative proceedings;
- law enforcement purposes;
- to comply with worker's compensation or other similar laws;
- public health activities;
- health oversight activities;
- reporting abuse, neglect or domestic violence;
- the military if you are a member of the armed services;
- correctional institutions if you are an inmate;
- disclosures of decedent's information to coroners, medical examiners and funeral directors;
- organ, eye or tissue donation purposes;
- national security and intelligence agencies as authorized by law.

We will only use or disclose the minimum amount necessary to perform these functions. We may disclose PHI to the sponsor of your health plan for any purpose described in this section. If you are a member of a group health plan, contact your employer for the name of your plan sponsor.

Other Uses and Disclosures of PHI
Uses and disclosures of PHI for purposes other than those described in Permitted/Required Uses and Disclosures of PHI, will be made only with your written authorization. If you provide us authorization to use or disclose your PHI, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose information following the specific purpose contained in the authorization. You understand that we are unable to take back any disclosures already made with your authorization, and that we are required to retain any records we may have containing your PHI. If you revoke your authorization for payment or health care operations, you may jeopardize the administration of the benefits under your health plan.

Your Individual Rights With Respect to PHI
Upon written request, you have the right to:

- request restrictions on certain uses and disclosures of your PHI. We are not required to agree to a requested restriction.
- receive confidential communication of PHI;
- access our records containing descriptions of your PHI;
- request an amendment to your PHI; We are not required to agree to a requested amendment.
- receive an accounting of impermissible PHI disclosures or disclosures made in compliance with the Rule for which an accounting is required.

Unless specifically requested otherwise, we will communicate PHI in connection with treatment, payment or health care operations, with any family member covered under your plan. Should any family member want a restriction on such disclosure of PHI, they must request such restriction in writing. Although we are not required to agree to a requested restriction, we will consider all factors explained in the request.

Except for uses and disclosures associated with treatment, payment, or health care operations, we do not use or disclose PHI when specifically protected by more stringent state law. Examples of more stringent state laws include those protecting HIV status, results of genetic testing, and indications of domestic abuse. We will follow state privacy laws that are more stringent than this federal law.

If you have chosen to receive this privacy notice electronically, you may also receive a paper copy from us upon your request.

Our Duties Regarding the Use and Disclosure of PHI
We are committed to maintaining your privacy and are required:

- by law to maintain the privacy of PHI and to provide you with notice of our legal duties and privacy practices with respect to PHI;
- to abide by the terms of the Notice of Privacy Practices currently in effect.

We reserve the right to change the terms of this privacy notice, and have such change be effective for all PHI that is maintained. Notification of a revised privacy notice will be provided through one of the following:

- U.S. Postal Service;
- revised Plan Document;
- Internet E-mail.

Up to date privacy notices are maintained on our Website.

How to File a Complaint Regarding the Use and Disclosure of PHI
If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of Health and Human Services. All complaints must be in writing. Please be assured that you may not be retaliated against for filing a complaint.

How to Contact Us
You may contact our representative at the following:

HIPAA Privacy Amendment

- ❑ **<u>Consider using</u> the attached Privacy Amendment for distribution to all your covered employees.**

HIPAA PRIVACY AMENDMENT

Effective as of: April 14, 2003

This amendment is attached to and made a part of the health benefit plan. Except as stated in this amendment, it shall not change any of the terms or provisions of the health benefit plan.

Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, the following language is attached to and becomes part of your health benefit plan.

DEFINITIONS

Plan Sponsor:

- the employer in the case of an employee benefit plan established or maintained by a single employer;
- the employee organization in the case of a plan established or maintained by an employee organization; or
- the association, committees, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations.

Protected Health Information (PHI): Protected Health Information (PHI) includes individually identifiable health information that is created or received by your provider, your health benefit plan or insurer, a data clearinghouse, a health authority, employer, school or university. PHI can be maintained or transmitted in any form or medium. It relates to the past, present, or future:

- condition of your physical or mental health,
- health care provided to you; or
- payment for the health care provided to you.

PERMITTED/REQUIRED USE AND DISCLOSURE OF YOUR PHI

- Your PHI will be used and disclosed for the purpose of routine treatment, payment of your benefits and health care operations, including plan and benefit administration. Your PHI may also be used or disclosed between your health plan, plan sponsor and any approved business associates as required or permitted by law, including the HIPAA Privacy Rule.

AMENDMENT PROVISION

The plan sponsor may receive information as to whether individuals are participating in the group health plan, or are enrolled or disenrolled in the plan.

The plan sponsor may also request summary health information for:

- obtaining premium bids from health plans for providing health insurance coverage, or
- modifying, amending or terminating the plan.

Summary health information summarizes claim history, claims expenses or types of claims experienced by individuals under the plan and also contains information which has been de-identified. De-identification deletes PHI and leaves only geographic information.

Your plan sponsor is required by law to:

- not use or disclose to anyone the PHI of any individual covered under this health benefit plan other than as permitted or required by the health benefit plan or by law;

- ensure that any agents, including subcontractor(s), to whom your plan sponsor provides PHI received from the health benefit plan, agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

- not to use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

- report to the health benefit plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for or which your plan sponsor becomes aware;

- allow you, upon written request, to:
  - access and amend your PHI;
  - receive an accounting of disclosures of PHI for other than treatment, payment and healthcare operations.

- make its internal practices, books and records relating to the use and disclosure of PHI received from the health benefit plan available to the Secretary of the Office of Civil Rights of HHS for the purposes of determining compliance by the group health plan;

- return or destroy, if feasible, all PHI received from the health benefit plan that your plan sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made; if destruction is not feasible, limit further uses and disclosures to those purposes that made the return or destruction of the information infeasible;

- provide PHI only to those individuals, under the control of the plan sponsor who perform plan administrative functions for the health benefit; (i.e. eligibility, enrollment, payroll deduction, benefit determination; claim reconciliation assistance), and to make clear to such individuals that they are not to use PHI for any reason other than for plan administrative functions nor to release PHI to an unauthorized individual;

- provide PHI only to those entities required to receive the information in order to maintain the health benefit plan (i.e. claim administrator, case management vendor, pharmacy benefit manager, claim subrogation, vendor, claim auditor, network manager, stop loss insurance carrier, insurance broker/consultant, and any other entity subcontracted to assist in administrating the health plan; and

- provide an effective mechanism for resolving any issues of noncompliance with regard to the items mentioned in this Amendment.

HOW TO FILE A COMPLAINT REGARDING THE USE AND DISCLOSURE OF YOUR PHI

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of Health and Human Services. All complaints must be in writing. Please be assured that you may not be retaliated against for filing a complaint.

How To Contact Us

You may contact our representative at:

Frequently Asked Questions about Privacy

What is HIPAA?

The guide constitutes and interpretation of HIPAA Privacy Rules and is not intended as legal advise

Q-1: What is HIPAA?
A: *HIPAA is the Health Insurance Portability and Accountability Act (passed by Congress in 1996). The Privacy Rule was issued by the U. S. Department of Health and Human Services. The Privacy Rule (45 CFR Part 160 and Subparts A and E of 164) of HIPAA provides the first comprehensive Federal protection for the privacy of health information.*

Q-2: What does the HIPAA Privacy Rule do?
A: *The HIPAA Privacy rule creates national standards to protect individuals' medical records and other protected health information. It gives individuals more control over their health information; it sets boundaries on use and disclosure of health records; and it establishes safeguards that covered entities must set up to protect information.*

Q-3: What is protected health information (PHI)?
A: *PHI is individually identifiable health information that is created or received by a provider, a health plan or insurer, a data clearinghouse, a health authority, employer, school or university. PHI can be maintained or transmitted in any form or medium. It relates to the past, present or future:*

- *condition of physical or mental health,*
- *health care provided; or*
- *payment for health care provided.*

PHI does not include summary health information or information that has been de-identified according to the standards for de-identification provided for in the HIPAA Privacy Rule.

Q-4: Who must comply with the new HIPAA privacy standards?
A: *Health Plans, health care clearinghouses and health care providers (who conduct certain financial and administrative transactions electronically).*

Q-5: By what date must covered entities meet the HIPAA privacy standards?
A: *April 14, 2003. Small group health plans have until April 14, 2004. Small group health plans are defined as plans with annual receipts of $5 million or less.*

Q-6: Are long/short term disability, workers compensation, and automobile liability that included coverage for medical payments covered under HIPAA?
A: *No, the listed types of policies are not health plans.*

Q-7: Are there penalties for not complying?
A: Civil Monetary Penalties *Section 1176 provides that HHS will impose on any person who violates a provision of the Privacy Rule a penalty of up to $100 for each violation. This is capped at $25,000 per year, per violation of an identical requirement or prohibition.*

Knowing Violation *Congress, in Section 262 of HIPAA, created the crime of "Wrongful Disclosure of Identifiable Health Information." If a person obtains or releases protected health information under false pretenses, the penalty increases to a fine up to $100,000 and imprisonment of not more than five years.*

If the offense is committed with the intent to sell, transfer or use Individually Identifiable Health Information for commercial advantage, personal gain, or malicious harm, the perpetrator may be imprisoned for up to 10 years and fined not more than $250,000.

Q-8: Will the Department of Health and Human Services make future changes to the HIPAA Privacy Rule?
A: *Under HIPAA, HHS has the authority to modify the privacy standards, as the Secretary may deem appropriate. However, a standard can be modified only once in a 12-month period.*

What does the HIPAA Privacy Rule ***mean*** to ***me?***

Q-9 What can I do now with PHI and how will that change after April 14, 2003
A: *Now, aside from any ERISA restrictions, you can use and disclose PHI of your plan participants freely. After the effective date of this rule, only designated persons who need access to protected health information to carry out health plan administrative functions can use and disclose protected health information of plan participants.*

Q-10: What information will I be able to get concerning my plan participants after 14, 2003?
A: *You will be able to use and disclose to business associates protected health information that is minimally necessary to perform treatment, payment and healthcare operations (TPO.)*

Q-11: What is a business associate?
A: *A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a health plan.*

Examples of business associates are as follows:
- *A third party administrator that assists a health plan with claims processing.*
- *A consultant whose services to a health plan involve access to protected health information.*
- *A utilization review or case management company*
- *A pharmacy benefits manager that manages a health plan's prescription benefits.*
- *A preferred provider organization that manages a health plan's network of providers.*

Q-12: Is a reinsurer/stop loss provider a business associate of the plan?
A: *Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.*

Q-13: What are Treatment, Payment and health care Operations (TPO)?
A: *"Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.*

"Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provisions of health care.

Examples of common payment activities include, but are not limited to:

- *Determining eligibility or coverage under a plan and adjudicating claims;*
- *Billing and collection activities;*
- *Reviewing health care services for medical necessity, coverage, and justification of charges and the like;*
- *Utilization Review activities.*

"Health care operations" are certain administrative, financial, legal and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. Common activities include, but are not limited to:

- *Underwriting and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits and securing or placing a contract for reinsurance of risk relating to health care claims, -*
- *Conducting or arranging for medical review legal and auditing services, including fraud and abuse detection and compliance programs;*
- *Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and*
- *Business management and general administrative activities*

Q-14 Can the health plan use or disclose PHI for reasons other than TPO?
A: *No, not unless the use and disclosure is made in connection with a HIPAA Authorization or is required or permitted by the HIPAA Privacy Rule.*

Q:-15 Can persons designated by the health plan use and disclose any information they want?
A: *No, those individuals who are authorized to have access to PHI must use and disclose the minimum amount of information necessary to perform the required job function for the plan.*

Q-16: How are group health plans expected to determine what is the minimum necessary information that can be used, disclosed or requested for a particular purpose?
A: *The HIPAA Privacy Rule requires a health plan to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose.*

The minimum necessary standard requires health plans to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgement and standards. Therefore, it is expected that health plans will utilize input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

Q-17: Must the HIPAA Privacy Rule's minimum necessary standard be applied to uses or disclosures that are authorized by an individual?
A: *No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements.*

Q-18: In limiting access, are health plans required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's <u>mini</u>mum necessary requirements?
A: *No. The basic standard for minimum necessary uses requires that health plans make reasonable efforts to limit access to protected health information to those* in *the workforce who need access, based on their roles with the health plan.*

The Department generally does not consider facility redesigns as necessary to meet the reasonable standard for minimum necessary uses. However, health plans may need to make certain adjustments to their facilities to minimize access, such as isolating and locking filing cabinets or records rooms or providing additional security such as passwords on computers maintaining personal information.

Q-19: Are business associates required to restrict their uses and disclosures to the minimum necessary?
A: *A business associate contract must limit the business associate's uses and disclosures* of, *as well as requests for, protected health information to be consistent with the health plan's minimum necessary policies and procedures.*

What do I have to do to be in compliance with this Federal Rule?

Q-20: Generally, what does the HIPAA Privacy Rule require the average health plan to do?
A: *The Privacy Rule requires activities such as:*

- *Providing a notice to participants about their privacy rights and how their information can be used.*
- *Adopting and implementing privacy procedures for the plan.*
- *Training employees so that they understand the privacy procedures.*
- *Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.*
- *Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.*

Q-21 What information must be provided in the notice?
A: *Covered entities are required to provide a notice in plain language that describes:*

- *How the covered entity may use and disclose protected health information about an individual.*
- *The individual's rights with respect to the information, including a statement that the covered entity is required by law to maintain privacy of protected health information.*
- *Whom individuals can contact for further information about the covered entity's privacy policy.*

The notice must include an effective date.

A covered entity is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices.

Q-22: How should the notice be delivered?
A: *A covered entity must make its notice available to any person who asks for it.*

A covered entity must prominently post and make available its notice on any Web sites it maintains that provides information about its customer services or benefits.

A health plan must also:

- *Provide the notice to individuals then covered by the plan no later than April 14, 2003 (April 14, 2004, for small health plans) and to new enrollees at the time of enrollment.*
- *Provide a revised notice to individuals then covered by the plan within 60 days of a material revision.*
- *Notify individuals then covered by the plan of the availability of and how to obtain the notice at least once every three years.*

Q-23: Can covered entities distribute their notices as part of other mailings or distributions?
A: *Yes*

Q-24: Does a health plan have to provide a copy of its notice to each dependent receiving coverage under a policy?
A: *No. A health plan satisfies the HIPAA Privacy Rule's requirements for providing the notice by distributing its notice to the named insured or employee of a policy under which coverage is provided both the named insured or employee and his or her dependents.*

Q-25: Where can a group health plan obtain assistance or more information on the HIPAA Privacy Rule?
A: *The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) maintains a Web site with helpful information. The address is: http://www.hhs.gov/ocr/hipaa/*

Resources for Additional HIPAA Information

1. HIPAA web site links
http://pweb.netcom.com/~ottx4/HIPAA.htm

- Federal Government Sites.
- Professional Association and Organizations.
- Listservs.
- Implementation Guides.
- State Government and State-Specific HIPAA Sites.

2. HIPAAcomply
http://www.hipaacomply.com/

Up-to-date information regarding HIPAA security and privacy compliance.

3. Centers for Medicare & Medicaid Services
http://www.cms.hhs.gov/hipaa/hipaa1/content/links.asp

http://www.cms.hhs.gov/hipaa/hipaa1/content/more.asp
General HIPAA insurance reform and related information.

- What is HIPAA?
- Overview.
- Q&A.