TUFTS Health Plan

HIPAA Privacy Summary for Self-insured Employer Groups

I. Overview

The Privacy Regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulate the uses and disclosures of protected health information (PHI).

PHI is any information that:

- Is created or received by a health care provider, health plan, employer or health care clearinghouse
- Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual
- Identifies the individual; or, with respect to which there is a reasonable basis to believe the information, can be used to identify the individual

The following categories of covered entities must comply with the Privacy Regulations by April 14, 2003:

- Group health plans that are employee welfare benefit plans, as defined by the Employee Retirement Income Security Act (ERISA)
- Health insurance issuers (e.g., HMOs)
- Health care providers
- Health care clearinghouses

It is important to note, references to "group health plan" throughout this document represent your employer-sponsored plan.

Please note, in our relationship with self-insured group health plans, Tufts Health Plan is functioning as a third party administrator (TPA) and is not a covered entity under the Privacy Regulations. Your ERISA group health plan is a covered entity. In addition, the Privacy Regulations compel the sponsor of a group health plan to comply with additional requirements if it will access PHI.
This document is a summary of the applicable HIPAA Privacy Regulations and requirements. For a comprehensive overview of compliance requirements, we suggest you read the regulations and/or obtain advice from your legal counsel.

This document covers the following HIPAA-related topics:

- Overview
- General Information
- Plan Document Amendment
- Authorization
- Business Associate Contracts
- Additional Compliance Information

II. General Information

A. Uses and Disclosures of PHI

A covered entity may use or disclose PHI only as permitted or required by the Privacy Regulations. The following are some examples of permitted disclosures:

- To the member who is the subject of the PHI
- For treatment, payment and health care operations. Examples of health care operations include quality assessment/improvement, credentialing, evaluating plan and provider performance and accreditation
- For other public purposes (e.g. research and health care oversight activities)
- Upon receipt of a HIPAA compliant authorization from the member
- As required by law

B. Plan Sponsor Access to PHI for Plan Administration Purposes

Because the administration of a self-insured plan involves accessing PHI, the plan sponsor (i.e., self-insured employer group) will need to meet all of the HIPAA Privacy requirements.

The self-insured employer group must meet multiple requirements in order to access PHI for plan administration purposes. Plan administration includes the functions related to payment and health care operations. The following are some examples of plan administration:

- Claims management and collection activities
- First and second level appeals decisions
- Conducting or arranging for medical review, legal services and auditing functions.

III. Plan Document Amendment

In order to access PHI for plan administration purposes, you will need to:

- Amend your plan document to reflect the requirements of the regulations. The plan document is the instrument that establishes the employee benefit plan under ERISA and establishes the group health plan as a legal entity. Please note, the plan document is not your description of benefits.

As plan sponsor, provide a certification to your group health plan that your plan documents have been amended and you agree to certain conditions specified in the regulations. Please note, Tufts Health Plan will not require a copy of the certification.

IV. Authorization

The Privacy Regulations require plan sponsors to obtain member authorization or permission for the uses and disclosures of PHI beyond plan administration. We understand that you may, at times, act to resolve issues on behalf of your members. In order to act in this capacity, the regulations require you to obtain either written authorization or verbal permission from the member. Tufts Health Plan will not require proof of member authorization or permission from you or your broker to resolve member issues requiring PHI.

Tufts Health Plan is currently developing a standard authorization form that, once finalized, will be posted to our Web site, www.tuftshealthplan.com, and may be downloaded. If you wish, you may use this form to obtain authorization from the member.

V. Business Associate Contracts

The Privacy Regulations allow a covered entity to disclose PHI to a business associate if the two parties enter into a business associate contract (BAC) that governs the permitted uses and disclosures of PHI.

The following are some examples of a group health plan's business associates:

- Third party administrator (e.g., Tufts Health Plan)
- Brokers and consultants
- Attorneys
- Accountants

You will need to execute BACs with each of your business associates. A sample BAC is available as an attachment to the regulations. We recommend you contact your legal counsel or advisor to develop a BAC for use with your business associates.

Tufts Health Plan has provided two copies of its standard Tufts Health Plan employer BAC for you to complete and return to us. This contract requires Tufts Health Plan to use and disclose PHI only as you have permitted, requires Tufts Health Plan to comply with many other parts of the Privacy Regulations and imposes certain requirements on your group health plan.

Enrollment/Disenrollment and Premium Bidding, Modifying, Amending or Terminating the Plan:
You do not need to provide written confirmation that you have entered into a BAC with entities acting on your behalf in order for Tufts Health Plan to disclose the following information to them: (1) PHI for the purposes of enrollment/disenrollment; or (2) summary health information (as defined in our Definitions of HIPAA-related Terms document) for the purposes of obtaining premium bids or modifying, amending or terminating the group health plan. Tufts Health Plan may disclose this information to entities acting on your behalf provided we have written confirmation that the person or entity is acting as your legal agent.

For brokers and other types of agents, please use the enclosed Agent Documentation form to notify Tufts Health Plan of your agents. If the activities your agents perform on your behalf of your clients are limited to those listed above, an Agent Documentation form is sufficient documentation.

Plan Administration:
If the activities performed on your behalf require access to PHI for plan administration purposes, other than those described above (i.e., the functions related to payment and health care operations as defined in our Definitions of HIPAA-related Terms document), Tufts Health Plan will require written confirmation that you have entered into a valid BAC with each of your business associates, permitting us to disclose PHI to them for plan administration. Please note, if you do not provide a copy of your certification to Tufts Health Plan of your own compliance, the terms of your BAC with that business associate must include language prohibiting the business associate from disclosing PHI received from Tufts Health Plan back to you, as the plan sponsor.

Some examples of PHI your business associates may receive for plan administration purposes include:

- Identified information for obtaining premium bids, modifying, amending or terminating the group health plan
- Any identifiable claims information

Once you have executed a BAC with your business associates, please use our Business Associate Documentation form, available at www.tuftshealthplan.com, to provide written confirmation to Tufts Health Plan of your business associates. Once this confirmation is received, Tufts Health Plan will be permitted to disclose PHI to the specified business associates for plan administration purposes. Please note, a Business Associate Documentation form entitles your business associates to receive PHI for plan administration, in addition to PHI for enrollment/disenrollment and summary health information for obtaining premium bids, modifying, amending or terminating the group health plan. If Tufts Health Plan has received a Business Associate Documentation form for a particular business associate, we do not require an Agent Documentation form as well.

VI. Additional Compliance Information

A. Individual Rights

Employer-sponsored group health plans that access PHI for plan administration purposes must provide their members with certain individual rights, including the following:

1. ***Notice of Privacy Practices*** – The group health plan must send a Notice of Privacy Practices that describes the uses and disclosures of PHI by the health plan to the subscriber. A sample Notice of Privacy Practices is enclosed for your reference. Once finalized, a copy of the Tufts Health Plan Notice of Privacy Practices will be available upon request.
2. ***Right to Request Restrictions on Uses and Disclosures of PHI*** – Individuals have the right to request a group health plan restrict its uses and disclosures of PHI.
3. ***Right to Access PHI*** – Individuals have the right to obtain and inspect most of their PHI held by the group health plan.
4. ***Right to Amend PHI*** – Individuals have the right to ask the group health plan to amend their PHI.
5. ***Right to an Accounting of Disclosures of PHI*** – Individuals have the right to request an accounting of disclosures of PHI made by the group health plan for purposes other than treatment, payment or health care operations.

As covered entities, self-insured plans are required to provide a method for members to invoke these individual rights. As a service to you, Tufts Health Plan will administer these rights for your members with respect to the PHI that Tufts Health Plan maintains. You will need to provide your members with a process and contact person for invoking their rights with respect to the PHI you maintain. Please note, the Tufts Health Plan Notice of Privacy Practices may be referenced or incorporated into your notice. Our Notice of Privacy Practices only addresses our obligations with the respect to the PHI we maintain. To obtain a copy of Tufts Health Plan's Notice of Privacy Practices, visit www.tuftshealthplan.com or contact your account manager.

You have an independent legal obligation to send a notice of privacy practices to your subscribers (current subscribers as of April 14, 2003 and new ones thereafter) describing how you use and disclose PHI. We suggest you include Tufts Health Plan's contact telephone numbers in your notice so members can use them to invoke their rights with respect to the PHI we maintain. In addition, you must provide similar contact numbers and information for members to contact you with respect to the PHI you maintain.

B. Administrative Requirements

Employer-sponsored group health plans that access PHI for plan administration purposes must comply with all of the following administrative requirements:

1. ***Privacy Official*** – The group health plan must designate a privacy official who is responsible for developing and implementing policies and procedures regarding PHI. In addition, the group health plan must designate a person or office responsible for receiving complaints related to the Privacy Regulations.
2. ***Workforce Training*** – The group health plan must train all members of their workforce on the policies and procedures regarding PHI. All trainings must be documented.
3. ***Safeguards*** – The group health plan must have appropriate administrative, technical and physical safeguards to protect PHI.
4. ***Internal Complaint Process*** – The group health plan must implement an internal complaint process regarding the protection of PHI and document any complaints.
5. ***Sanctions*** – The group health plan must adopt and apply appropriate sanctions for failure to comply with privacy policies and procedures.

6. ***Mitigation of Harmful Effects*** – The group health plan must implement a process to mitigate the harmful effects of unauthorized uses and disclosures of PHI.
7. ***Refrain from Retaliatory Acts*** – The group health plan may not intimidate, discriminate or retaliate against individuals for exercising their privacy rights.
8. ***Waiver of Rights*** – The health plan may not require individuals to waive their privacy rights.
9. ***Policies and Procedures*** – The group health plan must implement privacy policies and procedures that are reasonable and appropriate for their size.
10. ***Documentation*** – The group health plan must maintain required documentation for six years. Some examples of required documentation include policies and procedures, Notice of Privacy Practices and plan document amendments.

C. Consent

The Privacy Regulations do not require health plans to obtain written consent from members to perform treatment, payment or health care operations. Tufts Health Plan has removed the consent language from our membership applications and we suggest employer groups with customized membership applications remove consent language, if applicable.

D. Minimum Necessary

Covered entities must make reasonable efforts to use, disclose and request only the minimum amount of PHI necessary.

E. Preemption

In general, the HIPAA Privacy Regulations do not preempt applicable state laws. When a standard requirement or implementation specification of the HIPAA Privacy Regulations is in direct conflict or contrary to a provision of a state law, then the HIPAA Privacy Regulations will preempt that provision of the state law. When a provision of state law is more restrictive than a standard requirement or implementation specification of the HIPAA Privacy Regulations, then the state law is not preempted by the HIPAA Privacy Regulations.

F. Penalties for Non-Compliance

1. Civil Penalties

- $100 per violation
- Capped at $25,000 per calendar year for each requirement or prohibition that is violated

2. Criminal Penalties

- $50,000 and 1 year in jail for knowingly disclosing PHI
- $100,000 and 5 years in jail, if disclosure is made under false pretenses
- $250,000 and 10 years in jail, if intent to sell or for commercial advantage, personal gain or malicious harm

G. Enforcement

The Health and Human Services Office for Civil Rights has been designated to enforce the Privacy Regulations. The Department of Justice will prosecute criminal violations.