HIPAA Privacy Summary for Fully-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.

Both Tufts Health Plan and your group health plan are covered entities under the HIPAA Regulations and will need to take steps to be HIPAA compliant. 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 some of the applicable HIPAA Privacy 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

The Privacy Regulations outline specific conditions that must be met for most uses and disclosures.

B. Plan Sponsor Access to PHI

As a plan sponsor (i.e., fully-insured employer group), the type of PHI you choose to access and why you choose to access it affects your compliance requirements. There are three categories with varying requirements.

1. *Summary Health Information*

The plan sponsor may have access to summary health information for the following purposes:

- Soliciting premium bids
- Modifying, amending or terminating the plan

2. *Enrollment and Disenrollment*

The plan sponsor may have access to PHI to perform enrollment and disenrollment activities. The following are some examples of enrollment and disenrollment activities:

- Determination of eligibility or coverage
- Exchange of subscriber and dependent demographic and eligibility information with Tufts Health Plan
- Changes to existing subscriber/dependent information

If plan sponsors only access this level of PHI, the compliance requirements are limited. It has been our experience that this level of PHI is sufficient for the majority of fully-insured employer groups. However, if you wish to receive PHI for plan administration purposes, other than those described above, then you must meet all of the regulatory requirements.

3. *Plan Administration*

The plan sponsor must meet multiple requirements (see Section III – Plan Document Amendment for additional information) 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
- 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 welfare 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 and the insurer/HMO that your plan documents have been amended and you agree to certain conditions specified in the regulations.

- Once you have met the regulatory requirements, you must provide a copy of the certification that you have amended your plan documents, as required by the Privacy Regulations, to Tufts Health Plan. Our

Certification Documentation form, available at www.tuftshealthplan.com, is intended to serve as a cover sheet for your certification, which must be attached to the form prior to faxing it to Tufts Health Plan.

The certification is a legal document required by the regulations. We recommend you consult your legal counsel or advisor for assistance with certification. If you choose not to access PHI for plan administration purposes, then you do not need to amend your plan documents or provide 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 you may, at times, act to resolve issues on behalf of your members. In order to disclose PHI to you when acting in this capacity, Tufts Health Plan will require either written authorization or verbal permission from the member.

Please note, written member authorization or verbal permission will also be required in order to disclose PHI to any of your business associates (e.g., brokers) who help you resolve member issues.

Tufts Health Plan developed a standard authorization form to be used for this purpose. It is posted on our Web site, www.tuftshealhplan.com, and may be downloaded.

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:

- Brokers and consultants
- Attorneys
- Accountants

Please note, Tufts Health Plan is not a business associate of a fully-insured employer group.

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.

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 our Agent Documentation form, available at www.tuftshealthplan.com, 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 previously described (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, our 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 must provide their members with the following individual rights:

1. ***Notice of Privacy Practices*** – Fully-insured group health plans that access PHI for plan administration purposes, must maintain and provide, upon request by any person, a Notice of Privacy Practices that describes its uses and disclosures of PHI. A copy of the Tufts Health Plan Notice of Privacy Practices is available at www.tuftshealthplan.com for your reference.

   Fully-insured group health plans that only access PHI for enrollment/disenrollment activities or in the form of summary health information for premium bidding purposes, are not required to maintain such a notice.

2. ***Right to Request Restrictions on Uses and Disclosures of PHI*** – Individuals have the right to request the 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.

B. Administrative Requirements

Employer-sponsored group health plans that access PHI for plan administration purposes must comply with all of the regulatory requirements, including 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 training 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 group 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 comply with all sections of the regulations and 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.

Please note, if you do not access PHI for plan administration purposes (i.e., you only access summary health information for premium billing purposes or enrollment/disenrollment information), you need only comply with #7 (refrain from retaliatory acts) and #8 (waiver of rights) of the administrative requirements.

C. Consent

The Privacy Regulations do not require group 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

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