
HIPAA PRIVACY REQUIREMENTS

by: Marcia S. Wagner, Esq.
Marcia S. Wagner, Esq. & Associates, P.C.
One Union Street, Fourth Floor
Boston, Massachusetts 02108
Tel: (617) 725-8811
Fax: (617) 725-1830
Website: www.erisa-lawyers.com
Email: marcia@mwagner.net

March 2003

TABLE OF CONTENTS

	<u>Page</u>
I. Overview and Compliance Dates..... 1	
II. Covered Entities.....	1
III. Business Associates.....	2
IV. Protected Health Information.....	3
V. Disclosure of PHI.....	4
VI. Plan Document Requirements.....	8
VII. Privacy Notice.....	9
VIII. Individual’s Rights to PHI.....	9
IX. Administrative Requirements for Covered Entities to Ensure Privacy.....	11
X. Enforcement and Penalties.....	12
XI. How Does the Plan Sponsor Comply – A Practical Roadmap.....	13

HIPAA Privacy Regulations

I. Overview and Compliance Dates

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) includes privacy requirements since Congress believed that HIPAA’s electronic data interchange (“EDI”) standards and the increased ease of transmitting and sharing individually identifiable health information posed an increasing threat to confidentiality. As a result, the United States Department of Health and Human Services (“DHHS”) issued final privacy regulations on December 28, 2000 entitled “Standards for Privacy of Individually Identifiable Health Information” (the “Privacy Rule”). On August 14, 2002, DHHS issued new final privacy regulations which modified and clarified some of the provisions of the Privacy Rule. The Privacy Rule creates national standards to protect individuals’ personal health information and gives patients increased access to their medical records.

The general rule established under the final regulation can be summarized as follows: “Covered Entities” may not use or disclose “Protected Health Information” (“PHI”) except as authorized by the individual who is the subject to the information, or as explicitly required or permitted by the regulation. Even when the use or disclosure of PHI is permitted, only the “minimum necessary” amount of information to accomplish the intended purpose of the use, disclosure or request may be provided.

As “Covered Entities” (see definition below under Section II), large group health plans must be in compliance no later than April 14, 2003, while small group health plans have until April 14, 2004. For self-funded plans, the regulations define “large” plans as those with annual paid claims in excess of \$5 million for the most recent fiscal year, while “small” plans are those with annual paid claims of \$5 million or less for the most recent fiscal year.

II. Covered Entities

Covered Entities include: (i) health plans, (ii) health care clearinghouses, and (iii) health care providers who transmit PHI in electronic form. While the Privacy Rule directly regulates group health plans and not employers, given that a group health plan is usually nothing more than a plan document, it is the sponsor of the plan, the employer or the trustees who must comply. In addition, the companies and individuals who provide services to the health plan as “Business Associates” (see definition below under Section III) must comply.

Medical, dental, vision and flexible spending account plans are covered as “health” plans under the Privacy Rule. The Privacy Rule does not cover worker’s compensation, reinsurance (stop loss), accident insurance, disability insurance or liability insurance.

The final modifications to the Privacy Rule emphasized that employers are not Covered Entities under the Privacy Rule and, as such, employment records are specifically excluded from the definition of PHI. Records created, received or maintained by the employer in its capacity as the employer are not covered by the Privacy Rule, e.g., records such as fitness-for-duty evaluations, drug screening results, sickness and disability leave requests and documents needed to comply with the Americans with Disabilities Act, worker's compensation laws, and the Family Medical Leave Act. Any PHI created, received or maintained by the employer in its health care capacity acting on behalf of the health plan, however, remains subject to the Privacy Rule.

III. Business Associates

A Business Associate is a person or entity who:

- (a) on behalf of a Covered Entity, performs or assists in the performance of a function or activity involving the use or disclosure of PHI including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing; or
- (b) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity.

Covered Entities may disclose PHI to a Business Associate only after receiving satisfactory assurance that the Business Associate will safeguard the information. As such, Covered Entities must enter into contracts with its Business Associates which will protect the confidentiality of PHI when it is created, received, used by or disclosed by the Business Associates. These requirements help to ensure that Covered Entities do not avoid their HIPAA privacy responsibilities through "outsourcing."

The contract between the Covered Entity and the Business Associate, otherwise known as a "Business Associate Agreement," must among other requirements, establish the permitted and required uses and disclosures of PHI by the Business Associate and ensure that any agents and subcontractors to whom the Business Associate provides PHI on behalf of the Covered Entity also agree to the same restrictions and conditions that apply to the Business Associate with respect to the information.

When a broker receives PHI directly from a plan and the broker then shares the PHI with a third party administrator ("TPA"), the broker is a Business Associate of the plan. As such, the plan must have a Business Associate Agreement with the broker. Plan sponsors will need to ensure such Agreements are in place. In the alternative, when a TPA provides PHI to a broker on behalf of the plan, the broker is an agent for the TPA. As such, the broker must agree to be bound by the restrictions on PHI as contained in the Business Associate Agreement between the TPA and the plan.

IV. Protected Health Information

Protected Health Information (“PHI”) is all “individually identifiable health information” in any form, electronic or non-electronic, that is held or transmitted by a Covered Entity, including oral communication.

“Individually identifiable health information” is information that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care to an individual. Individually identifiable health information also includes demographic information collected from an individual that identifies an individual (or could reasonably be used to identify an individual).

If information is “de-identified,” then it is not covered by HIPAA Privacy Rule. De-identified information is that which does not identify any individual and for which there is no reasonable basis to believe that the information can be used to identify an individual. In order to de-identify information, a Covered Entity must remove 18 factors concerning the individual, including names, birthdays, social security numbers, all geographic subdivisions smaller than a state, telephone numbers, fax numbers, e-mail addresses and more. The specific list of identifiers, is generally as follows:

1. Names of individuals.
2. Geographic units – all geographic subdivisions smaller than a state, including street address, city, county precinct, zip code.
3. Dates – any month or day directly related to an individual, including birthdate, admission date, discharge date and date of death. However, listing an individual’s age is broad enough to be allowed in de-identified information (subject to the exception for individuals age 90 or older described below).
4. Ages – all those over 89 and any combination of month, date or year that reveals an individual’s age to be over 89, because nonagenarians are relatively rare. However, ages and identifying dates (month, day and year) or several individuals may be aggregated into a single category of age 90 or older.
5. Telephone numbers.
6. Fax numbers.
7. E-mail addresses.
8. Social Security numbers.

9. Medical record numbers.
10. Health plan beneficiary numbers.
11. Account numbers.
12. Certificate/license numbers.
13. Vehicle identifiers and serial numbers.
14. Device identifiers and serial numbers.
15. Web universal resource locators (URLs).
16. Internet protocol (IP) address numbers.
17. Biometric identifiers, including finger and voice prints.
18. Full face photographic images and any comparable images.
19. Any other unique identifying number, characteristic or code.

In addition, even if all the listed identifiers have been removed, if the health plan can identify an individual from the remaining information, the information is not de-identified.

V. Disclosure of PHI

A. General Rule

Covered Entities are prohibited from “using” or “disclosing” PHI except:

- With the “consent” or “authorization” of the patient; or
- As explicitly permitted or required by the Privacy Rule.

Health information is “used” when shared within the entity that holds the information (internal), while health information is “disclosed” when it is shared outside the entity (external).

B. Consents and Authorizations

A “consent” and “authorization” are not the same and the Private Rule establishes an important distinction between them. A consent is a broad, general permission granted by the individual. An authorization is a specific and detailed permission granted by an individual.

C. Consents and TPO

With the exception of psychotherapy notes, a health plan does not need to obtain an individual’s consent for the use and disclosure of PHI for routine health care delivery purposes; otherwise known as “treatment, payment or health care operations” (“TPO”).

“**Treatment**” means the provision, coordination or management of health care and related services by one or more health care providers. It also includes coordination or management of health care by a health provider and a third party and consultation or referrals between one health care provider and another.

“**Payment**” includes activities undertaken by the health plan or provider to obtain or provide reimbursement or premiums for the provision of health care and other activities, such as determinations of eligibility of coverage (including coordination of benefits), risk adjustments, billing, claims management, collections, medical necessity reviews and utilization review.

“**Health Care Operations**” includes certain services or activities necessary to carry out the covered functions of the health plan with respect to treatment and payment such as case management, pre-certification and care coordination, contacting providers and patients with information about treatment alternatives, underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess loss insurance), deciding claim appeals, conducting or arranging for medical review and auditing functions, and business planning and development such as conducting cost-management and planning-related analyses related to managing and operating the plan.

D. Consents and Enrollment

A health plan does not need to obtain consent from each plan participant to use and disclose his PHI to carry out TPO, however a plan may obtain such consent if the plan sponsor so chooses. The plan may even condition enrollment in the plan on the individual’s consent.

E. Authorization

Authorizations from individuals are required in order to use PHI in most cases other than for carrying out TPO. Some cases where written individual authorizations are required include marketing of health and non-health items and services and the use of

PHI by a non-health related division of the same corporation, e.g., for use in marketing or underwriting life or casualty insurance. In addition, health care providers are not permitted to disclose psychotherapy notes for carrying out TPO, nor are providers permitted to release PHI for the underwriting purposes of another Covered Entity unless a specific authorization is obtained from the individual.

Authorizations are not needed to use or disclose PHI for specified public and public policy related purposes, including public health, research, health oversight, law enforcement and use by coroners. In addition, PHI may be used or disclosed when the plan is required to do so by other law such as mandatory reporting under state law or pursuant to a search warrant.

F. Plan Sponsor Actions Regarding Consents and Authorization

As noted above, with the exception of psychotherapy notes, a plan does not need to obtain an individual's consent for carrying out TPO. Plan sponsors will need to keep in mind, however, that if the plan uses PHI for anything other than plan administration functions, the plan must first obtain an authorization from the individual whose information the plan seeks to view.

G. Required Disclosures

Plans are required to disclose PHI only in two instances:

1. to the individual who is the subject of the PHI when the individual requests it, and
2. to the Secretary of the Department of Health and Human Services when the Secretary is investigating a complaint of determining a plan's compliance with the Privacy Rule.

H. Permitted Disclosures

Plans are permitted to use and disclose PHI without consent or authorization, or without allowing the individual to obtain or agree to the use or disclosure if:

1. the PHI is used by or disclosed to the individual who is the subject to PHI;
2. the use of disclosure is for carrying out TPO (except regarding psychotherapy notes as noted above);
3. the use or disclosure is pursuant to a valid authorization; and
4. the use or disclosure is based on an agreement.

In addition, the Privacy Rule allows incidental uses and disclosures of PHI that occur as a result of an otherwise permitted use or disclosure. An "incidental use

or disclosure” is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure of the Privacy Rule. For example, if employees of the health plan are discussing a health claim in accordance with and as allowed by the plan’s privacy policies, but a person who should not be privy to the information inadvertently overhears the discussion, this would be considered an incidental disclosure.

I. Plan Sponsor Actions Regarding Permitted Disclosures

The plan sponsor will need to limit the employees who may receive PHI to only those employees performing plan administrative functions (i.e., payments and health care operations). The plan sponsor may designate a class of employees (e.g., all employees assigned to a particular department) or individual employees. The plan sponsor may identify these employees in whatever way best reflects the sponsor’s business needs as long as participants can reasonably identify who will have access. For example, persons may be identified by naming individuals, job titles (e.g., Director of Human Resources), functions (e.g., employees with oversight responsibility for the TPA), divisions of the company (e.g., Employee Benefits) or other entities related to the plan sponsor.

J. Minimum Necessary

Even if the plan may use or disclose PHI in accordance with the Privacy Rule, the plan must make reasonable efforts to limit PHI to the “minimum necessary” to accomplish the intended purpose of use, disclosure, or the request for PHI.

The minimum necessary standard is intended to make Covered Entities evaluate their practices and enhance protections as needed to prevent unnecessary or inappropriate access to PHI.

For routine uses of information, the Privacy Rule permits a plan to adopt general procedures for determining what the minimum necessary information is, then applying the general procedures. For example, a health plan may take two steps:

First: identify persons or classes of persons in its workforce who need access to PHI to carry out their duties and job responsibilities; and

Second: for each person or classes of persons, identify the category or categories of PHI to which access is needed and any conditions appropriate to that access.

For example, a health plan could develop procedures that allow certain employees or classes of employees unrestricted access to aggregate claims information for rating/accounting/budgeting purposes. However, the procedures could require approval from the departmental manager to obtain an individual’s specific identifiable claims records to determine the cause of the claims that can influence the rates/accounting/budgeting decisions.

For non-routine disclosures, individual determinations of “minimum necessary” would then only be required in specific cases to be determined by the plan’s privacy officer.

The minimum necessary standards of the Privacy Rule do not apply to the following:

- (a) Disclosures to or requests by a health care provider for treatment purposes.
- (b) Disclosures to the individual who is the subject of the information.
- (c) Uses or disclosures made pursuant to an authorization request by the individual.
- (d) Uses or disclosures required for compliance with EDI transactions.
- (e) Disclosures to the DHHS when disclosure is required under the rule for enforcement purposes.
- (f) Uses or disclosures that are required by other law.

VI. Plan Document Requirements

In order for a plan to use and disclose PHI as permitted by the Privacy Rule, the plan sponsor must abide by specific requirements and amend the plan documents to include the following provisions:

- (a) Explain the permitted and required uses and disclosures of PHI.
- (b) Include a statement that the plan sponsor agrees to:
 - (i) Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
 - (ii) Ensure that any agents, to whom it provides PHI agree to the same restrictions and conditions that apply to the plan sponsor;
 - (iii) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit plan of the plan sponsor;
 - (iv) Be vigilant of any use or disclosure of PHI that is inconsistent with the permitted or required uses or disclosures.
 - (v) Make PHI available to individuals;
 - (vi) Provide individuals with the opportunity to amend PHI;
 - (vii) Provide individuals with an accounting of the disclosure of their PHI;
 - (viii) Make the plan’s internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Resources for compliance purposes; and
 - (ix) Ensure that adequate separation exists between employees who are authorized to use PHI and those who are not; describe those employees or classes of employees to be given access to the PHI; restrict the access to and use of PHI to these employees; provide an

effective mechanism for resolving any issues of noncompliance by persons who have access to PHI.

The plan sponsor is required to provide a certification to the health plan that the plan documents have been amended to incorporate all of the above provisions. As such, the plan sponsor must certify to itself that the plan document has been amended.

Attached as Exhibit A is a sample plan amendment, as Exhibit B a sample summary plan description (including sample privacy notice) and Exhibit C a sample certificate.

VII. Privacy Notice

The Privacy Rule provides that the individuals have a right to an adequate notice of the information practices of their health plan. Plans must issue such privacy notices which are intended to inform individuals about what is done with their PHI and about any rights they may have with respect to that information.

Plans must provide privacy notices to individuals covered under the plan no later than April 14, 2003 for “large” health plans and by April 14, 2004 for “small” health plans. Thereafter, the notice must be provided to new enrollees at the time of enrollment and within 60 days of a material revision to the notice to the individuals currently covered under the plan. No less frequently than once every three years, the plan must notify individuals covered by the plan of the availability of the notice and how to obtain the notice.

VIII. Individual’s Rights to PHI

A. Right to Request Restrictions of PHI

Plans must permit individuals to request restrictions on the uses and disclosures of their PHI beyond the basic protections already granted under the Privacy Rule. For instance, an individual may request a restriction on information given to persons involved in the individual’s care, or an individual may request a restriction regarding disclosures to family members. Plans are not required to agree to the requested restrictions, however, and may deny the request for any reason.

If the plan agrees to a restriction, the plan may not use or disclose PHI in violation of the restriction, except in the case of emergency treatment where the restricted PHI is needed to provide the emergency treatment. If the restricted PHI is disclosed to a health care provider for emergency treatment, the plan must request that such provider not further use or disclose the information.

B. Right to Access to PHI

Plans must give individuals the opportunity to inspect or obtain copies of their PHI. Only information held in the plan’s “designated record set” must be made available.

A “designated record set” includes information such as medical records, billing records, enrollment, payment, claims adjudication, case or medical management record systems or records used to make decisions about individuals. There are exceptions to this requirement, however, including information maintained in psychotherapy notes and information compiled for use in a civil criminal, or administrative action. In the case of the exceptions, plans may deny individuals access to their PHI without providing the individual with an opportunity for review.

C. Right to Amend and Correct PHI

Plans must provide individuals with the opportunity to amend or correct their PHI held in the plan’s designated record set for as long as the plan maintains the PHI. A plan may, however, deny an individual’s request for amendment or correction if the information is accurate and complete or if the plan determines that the PHI was not created by the plan. Since medical records are not created by plans but, rather, are created by health care providers, the amendment process should not have a significant effect on health plans.

D. Right to Receive an Accounting of Disclosures

Upon request, individuals have a right to receive an accounting of instances where their PHI is disclosed by the plan or by one of the plan’s Business Associates (such as the TPA) for purposes other than for carrying out TPO. This right applies to disclosures made in the 6 years prior to the date on which the accounting of the disclosure is requested. Plans must have procedures to give individuals an accurate accounting of the disclosures. Such accounting must include the following: (i) the date of each disclosure; (ii) the name and address of the organization or person who received the PHI; (iii) a brief description of the information disclosed; and (iv) for disclosures other than those made at the request of the individual, the purpose for which the information was disclosed. The accounting must be provided as soon as possible, but no later than 60 days after receipt of the request.

E. Right to Request Confidentiality in Communications

Individuals have the right to request that a plan communicate to them regarding their PHI either by an alternative means or at an alternative location, if such requests are reasonable. “Reasonableness” is based upon the administrative difficulty in accommodating the request, not on the perceived merits of the request. A plan must accommodate such reasonable requests only if the individual clearly states that disclosing all or part of the information could put him or her in danger.

Plans may require that the confidentiality request be in writing and may condition its accommodation on what alternative address or method of contact an individual wants to use. A plan can also require an explanation of PHI that could endanger the individual, but the plan cannot require the details of the potential danger.

IX. Administrative Requirements for Covered Entities to Ensure Privacy

Covered Entities are required to develop and document policies and procedures relating to the use, disclosure and access to PHI. This documentation should serve as a tool for educating the entity's personnel about its policies and procedures and should also be the primary source of information for the entity's privacy notice.

The Privacy Rule does not provide for all of the specific procedures that a Covered Entity must adopt, however, there are certain minimum administrative requirements set forth. As a Covered Entity, health plans must abide by the following requirements:

1. **Privacy Official:** The plan must designate a privacy official who is responsible for the development and implementation of the privacy policies, as well as designate a contact person or office who is responsible for receiving complaints about privacy violations. The privacy officer should have a sufficiently senior position with the organization such that he can impose sanctions for privacy violations and require training. The privacy officer should also review the uses and disclosures of PHI for compliance with the "minimum necessary" standard, however routine disclosures should be listed by type to streamline this process.
2. **Training:** The plan must train members of its workforce (*i.e.*, the employees of the employer) regarding its privacy requirements and document that the training has been provided. The initial training must be completed no later than the Privacy Rule's effective date. Each new employee must be trained within a reasonable period of time after they are hired.
3. **Safeguards:** The plan must have in place appropriate administrative, technical, and physical safeguards to protect PHI from intentional or accidental disclosure or misuse.¹
4. **Complaints:** The plan must provide an avenue for individuals to make complaints concerning the plan's privacy policies and procedures regarding the use or disclosure of PHI and must document all complaints received and how they were handled.

¹ This requirement overlaps with the proposed security rules which are not yet final. Nonetheless, the proposed security rules provide that security measures must include: administrative procedures to guard data integrity and confidentiality, including documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission and disposal of health information, as well as security procedures and awareness training for all personnel; physical safeguards to guard data integrity, including formal policies that govern the receipt and removal of hardware/software (such as diskettes and tapes) into and out of a facility, as well as secure workstations; technical security services including procedures to ensure that data has not been altered or destroyed in an unauthorized manner, entity authentication and mechanisms to protect data that is transmitted over a communications network.

5. **Sanctions**: The plan must develop and apply appropriate sanctions against employees who fail to comply with the plan's privacy policies and procedures, as well as document the sanctions that are applied.
6. **Mitigation**: The plan must mitigate any harmful effect that is known of the use or disclosure of PHI in violation of its policies and procedures.
7. **Retaliatory Actions**: The plan may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against any individual who files a complaint with the Secretary of Health and Human Services.
8. **Waiver of Rights**: The plan may not require individuals to waive their rights to complain to the Secretary of Health and Human Services as a condition of the provision of treatment, payment, enrollment in the plan, or eligibility for benefits.
9. **Retention Period**: The plan must retain documentation of its policies and procedures for 6 years from the date when the policies and procedures were last in effect.

X. Enforcement and Penalties

The Secretary of Health and Human Services can bring enforcement actions against Covered Entities. HIPAA establishes civil as well as criminal penalties for any person who knowingly uses a unique health identifier, or who obtains or discloses individually identifiable health information. The penalties include: (i) a fine of not more than \$50,000 and/or imprisonment of not more than 1 year; (ii) if the offense is under false pretenses, a fine of not more than \$100,000 and/or imprisonment of not more than 5 years; and (iii) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years. The Secretary may conduct compliance reviews of Covered Entities. As such, health plans will be subject to such reviews.

The Privacy Rules does not provide for private rights of action for wrongful disclosure violations. As such, individuals may not sue a Covered Entity for such violations. An individual may, however, report violations to the Secretary of the DHHS in order for DHHS to investigate and bring enforce actions against the Covered Entity on behalf of the individual.

As a Covered Entity, a health plan is generally not liable for the privacy violations of a Business Associate, however the plan will be held liable if it knew of a Business Associate's wrongful activity and failed to take action. If the plan "knew of a pattern of activity of practice of the Business Associate" that constituted a material breach of violation of the Business Associates obligation under the contract, then the plan is required to take action by implementing "reasonable steps" to cure the breach or to end the violation. If such steps are not successful, the plan must terminate the contract with

the Business Associate if feasible. If contract termination is not feasible, the plan must report the problem to DHHS. In addition, the plan is not required to actively monitor and ensure protection by its Business Associates, however the plan must investigate credible evidence of a violation by a Business Associate and act upon any such knowledge.

XI. How Does the Plan Sponsor Comply – A Practical Roadmap

The Exhibits at the end of this outline provide a roadmap for HIPAA compliance with the privacy rules.

A. Plan Document

Under HIPAA's privacy rules, health plan sponsors must amend their plan documents, including flexible spending arrangements, to establish the permitted and required uses and disclosures of PHI. In order to amend the plan document, the plan sponsor must:

- (1) determine which PHI uses and disclosures the group health plan and plan sponsor must make to effectively administer the plan; and
- (2) include language in the plan documents indicating it will comply with the permitted and required PHI uses and disclosures.

Attached as Exhibit A is a model plan amendment to be in compliance with the law. Furthermore, attached as Exhibit B is a model SPD and required "privacy notice". The privacy notice must be provided by: April 14, 2003, when plan participants enroll in the Plan, and within 60 days of a material change in the Notice. Also, every three years the Plan must remind existing Plan participants about the privacy notice's availability. For the sake of efficiency and administrative ease, the privacy notice and SPD changes have been incorporated into the one document.

B. Certification of Compliance

In addition to HIPAA's requirement to amend the Plan and SPD, the privacy rules added a certification requirement for plan sponsors. Certification is designed to ensure that plan sponsors will safeguard PHI. The certification is attached as Exhibit C hereof, which an officer of the plan sponsor must execute, and which must be provided to the privacy officer of the Plan (likely, the Director of Human Resources) and retained by the Corporation in its files.

C. Employee Confidentiality Agreement

HIPAA's privacy rules require covered entities to train their "workforce" on policies and procedures regarding protected health information. The proposed privacy rules would have required workforce members to sign statements certifying that they had completed privacy training. Although the final rules eliminated this requirement, a covered entity still must prove that its workforce is trained. Employers may wish to

require some certification from those who have completed the training. Thus, all employees with access to PHI should execute Confidentiality Agreements as provided in Exhibit D hereto, which shall be retained by the Director of Human Resources.

At a minimum, the trainees should be employees who may have contact with PHI and who are identified in plan documents. Employers may wish to include other employees who may not engage in plan functions but may have access to PHI for other reasons, such as human resource functions. Even employees who do not normally come into contact with PHI should be made aware, through training or other methods, of the employer's privacy policies.

The goals of training are to inform employees about HIPAA's technical requirements and raise general awareness about privacy issues.

Employers should provide detailed training to employees engaged in benefit administration – both health and other benefits, such as disability, flexible spending account administration and pension. Supervisors should receive training so they know how to handle inquires from employees about health issues and to enforce the employer's privacy policies.

The U.S. Department of Health and Human Services ("HHS") has stated that training methods should be both flexible and manageable for the covered entity. For example, a small employer could satisfy the training requirements by providing each employee with access to PHI with a copy of its policies and requiring existing employees to acknowledge that they have reviewed the policies. A larger organization could have a training program with an instructor. In addition, one person (probably the privacy officer) should be identified as the contact for privacy questions and problems.

Regardless of the type of training, employees should receive information that applies the privacy rules to real situations at work. Training should include examples of possible privacy rule breaches, how breaches can be prevented and steps that employees should take if they become aware of a breach.

If you need the assistance of this law firm to develop a training procedure or manual, we would be happy to do so.

D. Business Associate Contracts

A group health plan is responsible for ensuring that all health plan service providers – called “business associates” – take steps to avoid inappropriate uses and disclosures of PHI. HIPAA’s privacy rules require these business associates to enter into written contracts stating that they will honor HIPAA’s privacy policies and procedures. The sample contract attached as Exhibit E (instructions) and Exhibit F (Business Associate Addendum) should be executed by all business associates and retained by the Director of Human Resources.

E. Authorization for Release of Health Information

Under HIPAA’s privacy rules, an authorization allows the use and disclosures of PHI both by the covered entity requesting the authorization and a third party. It must be written in specific terms to allow PHI use and disclosure for purposes other than those of treatment, payment and health care operations.

The Authorization Form attached hereto as Exhibit G should be used for such purpose.

F. Individual Rights Forms

Under HIPAA’s privacy rules, an individual can ask a covered entity’s permission to see and copy his or her PHI. A covered entity does not have to give an individual all of the information; only information held in the entity’s “designated record set” must be made available. A “designated record set” includes information such as medical records; billing records; enrollment, payment, claims adjudication; or records used to make decisions about individuals. Individuals have the right to see and obtain a copy of their PHI for as long as it is maintained in the designated record set. Individuals must request such access, which a covered entity can require to be in writing.

Furthermore, individuals can amend PHI. If their amendment request is denied, they can provide a “statement of disagreement” to the covered entity, which must be distributed with future PHI disclosures. Finally, individuals can request restrictions on PHI use and disclosure beyond basic protections already granted under the rules.

The following Forms are attached hereto:

Exhibit H – Individual Request to Inspect Health Information;

Exhibit I – Health Plan’s Response to Inspection Request;

Exhibit J – Individual Request Not to Use or Disclose Health Information;

Exhibit K – Individual Request to Correct or Amend a Record;

Exhibit L– Health Plan’s Response to Amendment or Correction Request;
and

Exhibit M – Sample Internal Log of Medical Record Disclosures.

G. Appointment of Privacy Officer

Attached as Exhibit N hereto is an Acceptance of Appointment of Privacy Officer. Oftentimes, there will be two (2) privacy officers, one for the health plan and one for the FSA, including the medical expense reimbursement plan.

H. Board Votes

The Board of Directors should vote to approve, authorize and adopt necessary plan amendments and appoint one or more privacy officers. Attached as Exhibit O is a sample Board vote.

I. HIPAA Security and Safeguards to Protect PHI – Developing the Privacy Policy

1. Firewalls and Access Controls

Covered Entities are required to erect “firewalls” to prevent PHI from being used impermissibly. Health plans and FSAs must therefore:

- (1) Evaluate the roles of all employees to determine which employees are involved in the administration of such benefit plans.
- (2) Implement a procedure to ensure that only these designated employees have access to PHI, and even then, that they have access only to the minimum PHI necessary to perform their duties for the plans.
- (3) Implement a mechanism for ensuring that these employees do not use or disclose PHI in a way prohibited by the privacy regulations. This might entail providing educational training for employees concerning the HIPAA privacy rules, the statutory penalties associated with violations of the rules, and the company’s internal policies for dealing with such violations.

Access controls that determine who can use PHI are key components of a firewall. The proposed security rules require that access controls be in place across the system – in

its administrative processes, technical systems and physical plan. There are three types of access controls:

- (1) “Role-based” access permits access to information based on an employee’s role in the organization. Under this system, an organization must review the various roles in its system, assign a role to an individual employee and create authorization lists linked to those roles. For example, a benefits manager probably would have access to most PHI in his or her office. However, an individual who is responsible for processing claims from a flexible spending account (“FSA”) would only have access to the FSA claims and coordinating health plan materials (such as explanation-of-benefits (“EOB”) forms related to those claims).

An access control system that includes role-based access could be set up so that the computer systems only recognize that type of access and only persons with certain roles can use certain offices.

- (2) “User-based” access permits access to information based on the user’s identity. This might be something an individual knows (a user ID or password), something a person is (biometric identifier or fingerprint) or something a person has (a token, ID badge or key).
- (3) “Context-based” access is based on external factors related to a transaction’s context, such as the time of day that an employee is working or the employee’s location. For example, employees on duty on a certain shift will have access to a specific type of information.

The plan sponsor may find that user-based access is the most efficient; if the benefits staff is limited, they may need access to any PHI that is used for plan administration purposes in that office. On the other hand, role-based access may be easy to implement and potentially more secure due to the various tasks involved and potentially for personnel changes. The corporation must document whichever system it chooses.

In addition, plan sponsor may want to consider implementing physical access controls on information, including the following steps.

- Control physical access to the Human Resources Department.
- Ensure that a private space is available for employee discussions about benefit plan issues. While physically redesigning an office is not required, installing a separate cubicle for private conversations or erecting similar barriers may be reasonable.

- Shield computer monitors from the view of staff who do not need to know about the onscreen information. Make sure that monitors are not located in high traffic areas.
- Make sure that computers are turned off when an individual leaves for break, lunch or the end of the day. Place an automatic log-off in the system (for example, if no activity occurs, the computer logs off after 10 minutes).
- Protect hardware to ensure that only authorized personnel have access to the hardware, and that the hard drive is cleared of all data when the hardware is discarded.
- Implement facility safeguard plans, including the reasonable prevention of threats such as fire and burglary.
- Install backup systems for emergencies and consider off-site storage of backup data.
- Implement policies regarding telephone discussions of PHI with individuals, relatives and service providers (e.g., no using of cellular phones). Ensure that names are used as little as possible and that medical diagnoses are not discussed. Prohibit leaving voice-mail messages discussing PHI.
- Consider purchasing a dedicated fax machine for PHI transmissions. Place it in a secure location. In the alternative, ensure that a qualified individual monitors the fax for confidential transmissions. Eliminate or minimize the use of outbound faxing, or verify the fax number and request immediate pick-up if information is faxed.
- Consider implementing a policy to ensure that e-mail is confidential. Determine how and when e-mail and attachments will be encrypted.

2. The Internal Complaint Process

Covered entities must provide a complaint process for individuals regarding the entities' privacy policies, procedures and compliance efforts.

Under the complaint process, covered health plans and providers must:

- (1) identify a contact person or office for receiving these complaints; and
- (2) maintain a record of complaints and, if applicable, a brief explanation of their resolution.

The privacy rules do not dictate how the complaint process must be established or require a dedicated staff for this purpose. Therefore, a covered entity can establish a complaint process appropriate for its size and capabilities. The preamble to the proposed

privacy rules provided an example of a small medical practice that could assign:

- (1) a clerk to log in written and/or verbal complaints; and
- (2) an officer to review complaints monthly, address the situation and make any necessary changes to the privacy policies and procedures.

A larger plan or provider could have a more formal appeals process with standard timeframes for responding to complaints.

Most plans should develop a complaint process somewhere between these two extremes. The complexity of the process will depend on the availability resources. Employers and plan sponsors may want to establish a process, supervised by the privacy official, in which all complaints are reviewed and resolved in a timely fashion. They also may consider using human resource professionals with expertise in resolving employee grievances.

Internal protocols should be developed for complaint investigations that include investigatory techniques such as interviews and reviews of relevant documents. Procedures can be borrowed from practices used to review and investigate discrimination complaints or denial-of-benefit claims.

The key is to establish a process that is fair, responsive, consistent, easy to use and confidential. Although an employee can file a complaint with the U.S. Department of Health and Human Services (“HHS”) at any time, one of the goals of the complaint process is to provide a resolution that avoids HHS involvement.

An attempt to resolve complaints is not legitimate unless it is combined with a policy of imposing sanctions against violators of the privacy rules. Employees must know that any breach of the privacy policy will be taken seriously. While the privacy rules require covered entities to provide for sanctions, they do not give any examples of possible disciplinary action. Sanctions can range from an oral warning to temporary loss of privileges to termination. Sanctions should be noted in employment policies and procedures, and standards should be established for first and subsequent offenses.

A complaint process also should include procedures for addressing breaches of the privacy policy. Covered entities must mitigate, to the greatest extent possible, any damages that may result from a breach. Therefore, privacy policies and procedures should include specific actions that must be taken in response to a privacy breach. Different standards will apply depending on the type of breach. For example, discovering an improper disclosure to a third party may require, at a minimum, that the subject of the PHI be notified. The extent of the violation and the PHI’s nature also may affect what type of corrective action is used.

The plan sponsor might consider requesting this law firm to develop a protocol for corrective action.

DG2930

Amendment Regarding
The Use and Disclosure of Protected Health Information

_____, having adopted the _____ Health Plan (the “Plan”), and having reserved to itself the right to amend the Plan at any time and from time to time, hereby amends the Plan, effective as of April 14, 2003, as follows:

A. Use and Disclosure of Protected Health Information

The Plan will use protected health information (“PHI”) to the extent of and in accordance with the uses and disclosures permitted by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Specifically, the Plan will use and disclose PHI for purposes related to health care treatment, payment for health care and health care operations.

Payment includes activities undertaken by the Plan to obtain premiums or determine or fulfill its responsibility for coverage and provision of plan benefits that relate to an individual to whom health care is provided. These activities include, but are not limited to, the following:

- determination of eligibility, coverage and cost sharing amounts (for example, cost of a benefit, plan maximums and copayments as determined for an individual’s claim);
- coordination of benefits;
- adjudication of health benefit claims (including appeals and other payment disputes);
- subrogation of health benefits claims;
- establishing employee contributions;
- risk adjusting amounts due based on enrollee health status and demographic characteristics;
- billing, collection activities and related health care data processing;
- claims management and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to participant inquiries about payments;
- obtaining payment under a contract for reinsurance (including stop-loss and excess of loss insurance);
- medical necessity reviews or reviews of appropriateness of care or justification of charges;

- utilization review, including precertification, preauthorization, concurrent review and retrospective review;
- disclosure to consumer reporting agencies related to the collection of premiums or reimbursement (the following PHI may be disclosed for payment purposes: name and address, date of birth, Social Security number, payment history, account number and name and address of the provider and/or health plan); and
- reimbursement to the Plan.

Health Care Operations include, but are not limited to, the following activities:

- quality assessment;
- population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, disease management, contacting health care providers and patients with information about treatment alternatives and related functions;
- rating provider and Plan performance, including accreditation, certification, licensing or credentialing activities;
- underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to health care claims (including stop-loss insurance and excess of loss insurance);
- conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
- business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Plan, including formulary development or improvement of payment methods or coverage policies;
- business management and general administrative activities of the Plan, including, but not limited to:
 - (a) management activities relating to the implementation of and compliance with HIPAA's administrative simplification requirements, or
 - (b) customer service, including the provision of data analyses for policyholders, plan sponsors or other customers;
- resolution of internal grievances; and
- due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a "covered entity" under HIPAA or, following completion of the sale or transfer, will become a covered entity.

B. The Plan will Use and Disclose PHI as Required by Law and as Permitted by Authorization of the Participant or Beneficiary

With an authorization, the Plan will disclose PHI to pension plans, disability plans, reciprocal benefit plans, and workers' compensation insurers, for purposes related to administration of this Plan.

C. For Purposes of This Section _____ Is the Plan Sponsor

The Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification from the Plan Sponsor that the Plan documents have been amended to incorporate the following provisions.

D. With Respect to PHI, the Plan Sponsor Agrees to Certain Conditions

The Plan Sponsor agrees to:

- not use or further disclose PHI other than as permitted or required by the Plan document or as required by law;
- ensure that any agents, including subcontractors, to whom the Plan Sponsor provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such PHI;
- not use or disclose PHI for employment-related actions and decisions unless authorized by an individual;
- not use or disclose PHI in connection with any other benefit or employee benefit plan of the Plan Sponsor unless authorized by an individual;
- report to the Plan's designee any PHI use or disclosure that it becomes aware of which is inconsistent with the uses or disclosures provided for;
- make PHI available to an individual in accordance with HIPAA's access requirements;
- make PHI available for amendment and incorporate any amendments to PHI in accordance with HIPAA;
- make available the information required to provide an accounting of disclosures;
- make internal practices, books and records relating to the use and disclosure of PHI received from Plan available to the HHS Secretary for the purposes of determining the Plan's compliance with HIPAA;
- ensure that adequate separation between the Plan and the Plan Sponsor is established as required by HIPAA (45 CFR 164.504(f)(2)(iii)); and
- if feasible, return or destroy all PHI received from the Plan that the Plan Sponsor maintains in any form, and retain no copies of such PHI when no longer needed for the purpose for which disclosure was made (or if return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction infeasible).

E. Adequate Separation Between the Plan and the Plan Sponsor Must Be Maintained

In accordance with HIPAA, only the following employees or classes of employees may be given access to PHI:

- _____;
- _____;
- _____; and
- _____.

F. Limitations of PHI Access and Disclosure

The persons described in Section E may only have access to and use and disclose PHI for plan administration functions that the Plan Sponsor performs for the Plan.

G. Noncompliance Issues

If the persons described in Section E do not comply with this Plan document, the Plan Sponsor shall provide a mechanism for resolving issues of noncompliance, including disciplinary sanctions.

* * * * *

IN WITNESS WHEREOF, _____ has caused this First Amendment to be executed by a duly authorized officer in its name and on its behalf, this _____ day of _____, 2003.

By: _____

Print or Type Name:

Title:

ATTEST:

Addendum to _____ Health Plan SPD

A federal law, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), requires that health plans protect the confidentiality of your private health information. A complete description of your rights under HIPAA can be found in the Plan’s Privacy Notice, which follows immediately and is also available from the _____.

Neither this Plan nor _____ will use or further disclose information that is protected by HIPAA (“protected health information”) except as necessary for treatment, payment, health plan operations and plan administration, or as permitted or required by law. By law, the Plan has required all of its business associates to also observe HIPAA’s privacy rules. In particular, the Plan will not, without authorization, use or disclose protected health information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of _____.

Under HIPAA, you have certain rights with respect to your protected health information, including certain rights to see and copy the information, receive an accounting of certain disclosures of the information and, under certain circumstances, amend the information. You also have the right to file a complaint with the Plan or with the Secretary of the U.S. Department of Health and Human Services if you believe your rights under HIPAA have been violated.

This Plan maintains a Privacy Notice, as follows, which provides a complete description of your rights under HIPAA’s privacy rules. For another copy of the Privacy Notice, please contact _____. If you have questions about the privacy of your health information please contact _____. If you wish to file a complaint under HIPAA, please contact _____.

NOTICE OF PRIVACY PRACTICES

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 _____ Health Plan (the “Plan”) uses health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. Your health information is contained in a medical record that is the physical property of the Plan.

How Your Health Information May be Used or Disclosed

For Treatment. The Plan may use your health information to provide you with medical treatment or services. For example, information obtained by a health care provider, such as a physician, nurse, or other person providing health services to you, will be recorded as it relates to your treatment. This information is necessary for health care providers to determine what treatment you should receive. Health care providers will also record actions taken by them in the course of your treatment and note how you will respond to the actions.

For Payment. The Plan may use and disclose your health information to others for purposes of receiving payment and services that you receive. For example, a bill may be sent to you or a third-party payor, such as an insurance company or health plan. The information on the bill may contain information that identifies you, your diagnosis, and treatment of supplies used in the course of treatment.

For Health Care Operations. The Plan may use and disclose health information about you for operational procedures. For example, your health information may be disclosed to members of the medical staff, risk or quality improvement personnel, and others to:

- evaluate the performance of staff;
- assess the quality of care and outcomes in your case and similar cases;
- learn how to improve facilities and services; and
- determine how to improve the quality and effectiveness of the provided health care.

Appointments. The Plan may use your information to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest.

Required by Law. The Plan may use and disclose information about you as required by law. For example, the Plan may disclose any information for the following purposes:

- for judicial and administrative proceedings pursuant to legal authority;
- to report information related to victims of abuse, neglect or domestic violence; and
- to assist law enforcement officials in their official duties.

Public Health. Your health information may be used or disclosed for public health activities such as assisting public health authorities or other legal authorities to prevent or control disease, injury, or disability, or for other health oversight activities.

Decedents. Health information may be disclosed to funeral directors or coroners to enable them to carry out their lawful duties.

Organ/Tissue Donation. Your health information may be used or disclosed for cadaveric organ, eye or tissue donation purposes.

Research. The Plan may use your health information for research purposes when an institutional review board or privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your health information.

Health and Safety. Your health information may be disclosed to avert a serious threat to the health or safety of you or any other person pursuant to applicable law.

Government Functions. Specialized government functions, such as protection of public officials or reporting to various branches of the armed services, may require use or disclosure of your health information.

Workers' Compensation. Your health information may be used or disclosed in order to comply with laws and regulations related to workers' compensation.

Your Health Information Rights

You have the right to:

- request a restriction on certain uses and disclosures of your information; however, the Plan is not required to agree to a requested restriction;
- obtain a paper copy of the Notice of Privacy Practices upon request;
- inspect and obtain a copy of your health record;
- amend your health record;
- request communications of your health information by alternative means or at alternative locations;

- revoke your authorization to use or disclose health information except to the extent that action has already been taken; and
- receive an accounting of disclosures made of your health information.

Complaints

You may make a formal complaint to _____ and/or to the Department of Health and Human Services if you believe your privacy rights have been violated. You will not be retaliated against for filing a complaint.

Obligations of the Plan

The Plan is required to:

- maintain the privacy of protected health information;
- provide you with this notice of its legal duties and privacy practices with respect to your health information;
- abide by the terms of this Notice;
- notify you if the Plan is unable to agree to a requested restriction on how your information is used or disclosed;
- accommodate reasonable requests you may make to communicate health information by alternative means or at alternative locations; and
- obtain your written authorization to use or disclose your health information for reasons other than those listed above and permitted under law.

The Plan reserves the right to change its information practices and to make the new provisions effective for all protected health information it maintains. Revised notices will be made available to you by e-mail and/or in hard copy within 60 days of any change.

Contact Information

If you have any questions or complains, please contact:

Certification of _____

WHEREAS _____ (“Plan Sponsor”) is the sponsor of an employee welfare benefit plan for its employees and their dependents; and

WHEREAS Plan Sponsor’s employee welfare benefit plan is a “group health plan” within the meaning of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and

WHEREAS _____ Health Plan (“Health Plan”) provides health insurance coverage to the participants and beneficiaries in the Plan Sponsor’s group health plan; and

WHEREAS Health Plan and Plan Sponsor desire to exchange health information protected under HIPAA (“protected health information” or “PHI”) for purposes related to administration of the group health plan;

THEREFORE BE IT RESOLVED, that Plan Sponsor hereby certifies to Health Plan the following, as required by Section 45 CFR 164.504(f) of HIPAA:

The Plan documents that govern Plan Sponsor’s group health plan have been amended to incorporate the following provisions and Plan Sponsor agrees to:

- not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law;
- ensure that any agents, including subcontractors, to whom it provides PHI received from Health Plan agree to the same restrictions and conditions that apply to Plan Sponsor with respect to such PHI;
- not use or disclose PHI for employment-related actions and decisions unless authorized by the affected individual;
- not use or disclose PHI in connection with any other benefit or employee benefit plan of Plan Sponsor, unless authorized by the affected individual;
- report to Health Plan’s designee any PHI use or disclosure that it becomes aware of which is inconsistent with the uses or disclosures provided for;
- make PHI available to an individual based on HIPAA’s access requirements;
- make PHI available for amendment and incorporate any PHI amendments based on HIPAA’s amendment requirements;

- make available the information required to provide an accounting of disclosures;
- make its internal practices, books and records relating to the use and disclosure of PHI received from the Health Plan available to the Secretary of the U.S. Department of Health and Human Services to determine the Health Plan's compliance with HIPAA;
- ensure that adequate separation between the Health Plan and the Plan Sponsor is established as required by HIPAA (45 CFR 164.504(f)(2)(iii)); and
- if feasible, return or destroy all PHI received from the Health Plan that Plan Sponsor maintains in any form and retain no copies of such PHI when no longer needed for the specified disclosures to those purposes that make the return or destruction infeasible.

* * * * *

IN WITNESS WHEREOF, this Certification is hereby executed this _____ day of _____, 2003.

On behalf of the Plan Sponsor

Title: Privacy Official

EMPLOYEE CONFIDENTIALITY AGREEMENT

I, _____, have read and understand _____ policies regarding the privacy of individually identifiable health information (or protected health information (“PHI”)), as mandated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). In addition, I acknowledge that I have received training in _____ policies concerning PHI use, disclosure, storage and destruction as required by HIPAA.

In consideration of my employment or compensation from _____, I hereby agree that I will not at any time – either during my employment or association with _____ or after my employment or association ends – use, access or disclose PHI to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities with _____, as set forth in _____ privacy policies and procedures or as permitted under HIPAA. I understand that this obligation extends to any PHI that I may acquire during the course of my employment or association with _____, whether in oral, written or electronic form and regardless of the manner in which access was obtained.

I understand and acknowledge my responsibility to apply _____ policies and procedures during the course of my employment or association. I also understand that unauthorized use or disclosure of PHI will result in disciplinary action, up to and including the termination of employment or association with _____ and the imposition of civil penalties and criminal penalties under applicable federal and state law, as well as professional disciplinary action as appropriate.

I understand that this obligation will survive the termination of my employment or end of my association with _____, regardless of the reason for such termination.

Signature: _____

Date:

HIPAA and Business Associates: Basic Requirements and Instructions for “HIPAA Addendum”.

A. Basic requirements.

HIPAA requires _____ Health Plan and Flexible Spending Arrangement to have “satisfactory assurance” that any “business associate” will “appropriately safeguard” “protected health information” received or created by the business associate in the course of performing services for _____ Health Plan and Flexible Spending Arrangement. _____ Health Plan and Flexible Spending Arrangement must document the satisfactory assurances through a written contract (which may be part of another contract). Any business associate arrangement which is entered into, renewed or modified on or after April 14, 2003, must include mandated business associate provisions.

1. What is protected health information?

Protected health information is identifiable health information that _____ Health Plan and Flexible Spending Arrangement have acquired in the course of serving patients. Data elements that make health information identifiable include: name, address, employer, relatives’ names, date of birth, telephone and fax numbers, e-mail addresses, social security numbers, member or account numbers, certificate or license numbers, voice recordings, fingerprints, photographs, or any other linked number, code or characteristic.

2. “What is a “business associate”:

A business associate is a person or entity that performs or assists _____ Health Plan and Flexible Spending Arrangement in performing any function or activity that involves use or disclosure of protected health information.

3. What are some examples of business associate functions?

Some examples are claims processing, claims administration, data analysis or processing, utilization review, quality assurance, billing, and pricing, service arrangements which include access to protected health information, strategic analysis, and practice management functions – provided these functions are done by the business associate on behalf of _____ Health Plan and Flexible Spending Arrangement.

The following services are also business associate services, if they involve any use or disclosure of protected health information: legal, accounting, actuarial, consulting, data aggregation, management, administrative, accreditation, and financial services.

A business associate can be a business, another clinical provider, or a payer if it is performing relevant services or functions on behalf of _____ Health Plan and Flexible Spending Arrangement.

A business associate contract is required whether the use of or access to protected health information is momentary, temporary or long-term; whether it is on _____ premises or elsewhere; or whether the business associate will store health information or indicates that it will immediately destroy it.

B. Instructions for Attached HIPAA Addendum.

The HIPAA Addendum should be added to any contract you are negotiating with a business associate. So that you can adapt the Addendum to your circumstances, it provides various options, each of which is discussed below.

The contract to which you are adding the Addendum is referred to in the Addendum as “the Agreement”. Referring to the underlying Agreement is necessary because HIPAA imposes some requirements on the Agreement as a whole, and the Addendum does that by explicitly superceding conflicting terms in the main Agreement.

First, fill in the name of the business associate in the first blank (before the word “Company”). For the rest of the Addendum, Company will refer to the party with whom you are contracting. You also need to add the business associate name to the last page of the Addendum above the signature line.

Second, fill in the blank in Paragraph 1 where you specify the purposes for which the business associate will have access to protected health information. If such purposes are already specifically stated in the underlying Agreement, you can line through and initial; but otherwise, you should list the specific purposes for access. For example, if a software maintenance agreement requires live access for testing, you can put “database testing”; of if the contract is for coding, you can just insert “coding”.

Third, as notes above, HIPAA requires the contractor to give “satisfactory assurances” of protecting health information – i.e., protecting BOTH its privacy, and its security. HIPAA does not define “satisfactory assurances”, except to indicate that the steps a business associate should take should be reasonable and effective under the circumstances, and that those steps should be spelled out in the business associate contract.

This means that you will need to understand from the contractor how health information will be protected, and judge that those steps are reasonable and effective. You need to know what measures will be used to ensure it stays private and how it will be kept secure from unauthorized intruders. To help you, the

Addendum gives you options you can discuss with the business associate. Cross out and initial the options that are not applicable. Be sure to address both security and privacy. Call or e-mail Marcia Wagner (617-725-8811; marcia@mwagner.net) if you need help or advice deciding what options are appropriate.

The first of these options comes up in bolded language in paragraph 1: you have the option of requiring the business associate to identify all employees and/or subcontractors who will have further access. This will seldom be necessary; but if the dangers presented by the form of access are significant, or the data is especially sensitive, it is an option to consider. For example, this would be a good option to consider for an organization providing data aggregation services for an HIV drug trial.

The major options come up in paragraph 2, which lists a set of alternatives, ranging in comprehensiveness. An onsite database tester which has only temporary access may not need a comprehensive privacy and security program; but a company performing a detailed billing audit of charges for all inpatient information for a year may need one to give you adequate comfort that information will remain entirely secure. Every business associate, however, should be able to identify concrete steps that it is taking to protect health information, and help you assess whether those steps will be adequate under the circumstances.

Another option comes up in paragraph 6. _____ is required to provide patients with a retrospective log of certain disclosures of protected health information. If you expect the business associate to be making disclosures, then it is a good idea to require the company to keep track of them and make them available to _____ upon request. You can also use this option for especially sensitive information, where you want to know exactly how it has been disclosed or used.

Please do not make changes or deletions in the Addendum, other than as notes above, without talking with Marcia Wagner. HIPAA is very prescriptive concerning mandated contractual terms, and although the Addendum seems long, it adheres closely to the HIPAA mandates.

HIPAA and Business Associate Addendum

WHEREAS, pursuant to the Agreement to which this is an addendum, _____ (hereafter “Company”) will be receiving or creating Protected Health Information (“PHI”) as that term is defined in 45 C.F.R. 164.501, to perform services on behalf of _____ Health Plan (“the Health Plan”) or _____ Flexible Spending Arrangement (“FSA”), each of which is a “covered entity” for purposes of 45 C.F.R. Part 160;

WHEREAS, the parties acknowledge that Company is therefore a “Business Associate”, as that term is defined in 45 C.F.R. 160.103;

WHEREAS, 45 C.F.R. 164.502(e) and 45 C.F.R. 164.504(e) require that a written agreement between Company and the Health Plan or FSA include certain terms and establish satisfactory assurances that PHI will be protected in accordance with applicable laws and regulations;

NOW, THEREFORE, the parties agree as follows:

1. PHI received or created by Company may be used or disclosed by Company, including any of its employees and agents, only for purposes described in the Agreement, and only to other individuals or organizations, including any Company subcontractors, [who are identified on the attached Exhibit B and] whose further use and disclosure is identically restricted by a written agreement containing provisions that are substantially similar to the provisions of this Addendum. Those purposes include:
_____. Company will not otherwise use or disclose PHI except as required by law, and then only on advance notice received by the Health Plan and/or FSA, as the case may be.

2. **Company shall use appropriate and effective safeguards to ensure that PHI is used and disclosed only as permitted by this Agreement, and that the minimum amount of PHI is used or disclosed to accomplish those purposes. Federal regulations require a privacy and security program with administrative, technical and physical safeguards appropriate to the size and complexity of the Company's operations and the nature and scope of its activities. Company's safeguards and procedures are described in Exhibit A to this Addendum, which is hereby incorporated by reference. As more fully described on Exhibit A, those safeguards include (*delete or cross out, and initial, those not present or applicable*):**

- **written confidentiality and security policies and procedures, as attached or described in Exhibit A, governing: computer portal security, data security, maintaining data integrity, information management, access controls, use of the minimum amount of PHI necessary, employee confidentiality obligations, contracting and sharing information with subcontractors or other independent contractors, procedures for reporting breaches of security or privacy to the designated privacy officer of the Health Plan and FSA (as applicable);**
- **designation of a privacy and/or security officer, or a compliance officer with responsibility for implementing or coordinating Health Plan's and FSA's privacy and security program or procedures;**
- **employee training in HIPAA requirements and company policies and procedures;**
- **signed employee confidentiality statements;**
- **effective employee discipline for breaches of security or privacy;**
- **job descriptions which clearly state employee and managerial responsibilities for privacy and security;**
- **employee access controls;**
- **information systems access controls;**
- **deidentification, or full or partial masking of PHI;**
- **encryption of PHI or identifying characteristics;**

- **periodic monitoring for privacy and security breaches;**
 - **periodic privacy or security assessments;**
 - **compliance with federal electronic transaction standards for PHI; and**
 - **a comprehensive privacy and security compliance program.**
3. **Company shall notify the Health Plan's and FSA's designated privacy officer, immediately upon discovering any breach of this Agreement, including any use or disclosure of PHI, whether intentional or inadvertent, by Company or any contractor of Company, that is inconsistent with the Agreement. Company shall immediately implement effective steps to mitigate the effect of such breach, and to prevent other breaches. Company's notice shall specify the steps it is taking to investigate and remediate any breach. The results of any investigation shall be made fully available to the designated privacy officer within five (5) business days of completion. In the event the designated privacy officer accepts the remediation efforts as adequate, Company shall also from time to time, at the designated privacy officer's request, provide a written update on the status and effectiveness of the remediation.**
4. **The parties acknowledge that federal regulations give patients certain rights to access their PHI, including PHI held or created by Business Associates, and that time is of the essence in responding to such requests. Company will immediately notify the designated privacy officer of any request by any person for PHI, and cooperate with the designated privacy officer as directed by the designated privacy officer in responding to the request. The parties anticipate that typically the designated privacy officer will respond to such a request, and may require immediate information from Company for that purpose, but Company shall, upon the designated privacy officer's request, respond to such request directly in a manner consistent with the designated privacy officer's directions. In addition, Company will promptly comply with any information request by the**

- designated privacy officer necessary for the designated privacy officer to respond to a request to access Company-held or created PHI. The decision whether and how to respond to such a request shall be in the designated privacy officer's sole and absolute discretion.**
- 5. The parties acknowledge that federal regulations give patients certain rights to request that their PHI be amended or corrected, including PHI held or created by Business Associates. Upon notice from the designated privacy officer, Company shall immediately make PHI held or created by Company available to the Health Plan or FSA as the privacy officer may require to fulfill its obligations to evaluate and respond to such a request. In the event that the privacy officer determines to grant the request, in whole or in part, Company shall, as directed by the privacy officer, incorporate any such amendments or corrections into all PHI for that patient maintained by Company. The decision whether to agree to such a request, and the manner of response, shall be in the privacy officer's sole discretion.**
- 6. The parties acknowledge that under certain circumstances, patients may have a right to a six-year retrospective log of all disclosures other than for treatment, payment or health care operations, as those terms are defined and employed in 45 C.F.R. Parts 160 and 164. Upon the privacy officer's request, Company shall immediately provide such information concerning such disclosures, in such form, as the privacy officer reasonably requires to respond to such a patient request. In addition, Company shall maintain an ongoing log of all disclosures of PHI it makes, including the person or organization receiving the PHI, the recipient's address, a description of the PHI disclosed, and the reason for the disclosure. Company shall make a copy of such log available to the Health Plan or FSA upon request.**

- 7. Consistent with and subject to applicable law, Company shall make its internal practices, books and records relating to the use and disclosures of PHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with 45 C.F.R. Parts 160 and 164. Company shall also make such practices, books and records, together with copies of any contracts with third parties (such as subcontractors performing services or functions within the scope of this Agreement) available to the Health Plan and FSA for inspection or copying upon reasonable notice. Neither this provision, nor the manner of its implementation or non-implementation by the Health Plan and FSA, shall be deemed to relieve Company of its obligations under this Addendum or the Agreement.**

- 8. Termination. The parties acknowledge that federal regulations mandate certain provisions with respect to termination in the event Company breaches the provisions of this Addendum. To implement those provisions, the parties agree as follows: A breach of this Addendum shall be considered a material breach of the Agreement. In addition to any other remedies the Health Plan and FSA have under the Agreement, and notwithstanding any inconsistent provision (including without limitation any provision of the Agreement with respect to cure, requiring alternative dispute resolution, or purporting to limit the Health Plan's and FSA's remedies for breach), the Health Plan and FSA retain sole discretion to terminate the Agreement, in whole or in part, for breach of the provisions of this Addendum, and/or to determine whether the Health Plan's and FSA's remediation is satisfactory, and/or to report such breach to the Secretary of Health and Human Services. The Health Plan and FSA may also terminate this Agreement immediately if Company is sanctioned or named as a defendant in any civil or criminal proceeding based upon allegations that Company has wrongfully used or disclosed confidential information, whether or not that information is PHI.**

- 9. Within two (2) business days of the expiration or termination of this Agreement, or of any part that relates to PHI if such part is separately terminated, Company shall return or destroy all PHI received from the Health Plan or FSA or created by Company, including any PHI that through processing or otherwise has been incorporated in other forms or databases of Company for any purpose, including without limitation data aggregation, operations or management of Company.**
- 10. Company shall not release or transfer any PHI to any third party for a fee.**
- 11. Notwithstanding any provision of the Agreement, or any other agreement between the parties, Company may not assign any rights or obligations which involve the receipt, storage, processing or creation of PHI to any other party without the Health Plan's or FSA's express written permission.**
- 12. This Agreement shall be construed to comply with 45 C.F.R. Parts 160 and 164, as amended from time to time, and other regulations currently or hereafter in effect which implement the privacy, security and transaction standards provisions of the Health Insurance Portability and Accountability Act. It shall not be construed to authorize Company disclosures or uses inconsistent with more restrictive laws or regulations, including without limitation laws or regulations protecting the confidentiality of information relating to HIV status or substance abuse treatment.**
- 13. The parties acknowledge that laws and regulations with respect to PHI, transaction standards, and data security are in flux. Company agrees that upon the Health Plan's or FSA's request it will promptly negotiate in good faith to amend this Addendum if required to conform it to changes in such laws or regulations. If Company fails to do so upon the Health Plan's or FSA's written request, the Health Plan or FSA may, at its election, treat this Agreement as so amended to conform to applicable laws and regulations, with**

binding effect, or the Health Plan or FSA may terminate this Agreement upon 30 days written notice.

- 14. Company agrees that it will perform its obligations under this Addendum without charge to the Health Plan or FSA.**
- 15. Company's obligations hereunder are absolute and unconditional. Under no circumstances will Company excuse or delay performance of any obligations under this Addendum based upon any asserted breach by the Health Plan or FSA of this Addendum or the Agreement.**
- 16. Notwithstanding any inconsistent provision of the Agreement, Company shall indemnify and hold harmless the Health Plan or FSA, its affiliates, and the trustees, officers, employees and agents of either, against any claim, action, suit or proceeding, civil or criminal, and any damages, costs, fees and penalties, arising from any alleged act or omission by Company in complying with this Addendum or applicable law.**
- 17. The obligations of Company under Sections One through Five above shall remain in effect for as long after the termination of the Agreement as Company has PHI in its possession. Company's obligation under Section Six above to provide information relevant to an accounting shall remain in effect for six years after the later of the destruction or return of all PHI or the termination of the Agreement. Company's obligations under Sections Seven and Sixteen above shall survive without end.**

By:

Date

[COMPANY]

By:

Date

AUTHORIZATION FOR RELEASE OF HEALTH INFORMATION

I, _____, [Employee Name] hereby authorize the use or disclosure of my health information as described in this authorization.

(1) *Specific person/organization (or class of persons) authorized to provide the information:*

(2) *Specific person/organization (or class of persons) authorized to receive and use the information:*

(3) *Specific description of the information:*

[For example, medical examination report and conclusions related to a fitness-to-work exam, results of drug testing for employment-related purposes].

(4) *Right to revoke:* I understand that I have the right to revoke this authorization at any time by notifying the Health Plan in writing to [Name], [Company], [Address], [City], [State] [Zip]. I understand that the revocation is only effective after it is received and logged by [Name]. I understand that any use or disclosure made prior to the revocation under this authorization will not be affected by a revocation.

(5) I understand that after this information is disclosed, federal law might not protect it and the recipient might redisclose it.

(6) I understand that I am entitled to receive a copy of this authorization.

(7) I understand that this authorization will expire when my employment terminates.

Signature of Employee _____ Date _____

INDIVIDUAL REQUEST TO INSPECT HEALTH INFORMATION

I, _____, (Employee Name) request to review health information held about me in the Health Plan’s “designated record set” in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A “designated record set” includes information such as medical records; billing records; enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used to make decisions about individuals.

I understand that the Plan has 30 days to respond to this request, and that if someone else holds the information or it is off-site, the response time is 60 days.

I request that the information be provided in the following format:
(circle one) paper electronic

I agree that the Plan may provide a summary of the health information instead of allowing me to review the information.

I agree to pay any fees for copying or summarizing health information. Fees will be reasonable and cost-based, and include only the cost of copying, postage, and preparation of a summary (if I agree to a summary).

I understand that this request does not apply to certain health information, including: (1) information that is not held in the designated record set; (2) psychotherapy notes; (3) information compiled in reasonable anticipation of or for litigation; and (4) other information not subject to the right to access information under HIPAA.

Signature _____ Date _____

**HEALTH PLAN'S
RESPONSE TO INSPECTION REQUEST**

Grant

Your request to access your health information has been granted. Access will be provided at [state the manner in which access will be provided].

[If a summary has been created, state that the summary has been created based on the advance agreement provided by the individual].

Need for Extension of Time

The Plan received your request to access health information on _____ . The Plan has evaluated your request to access health information. A delay in providing the information is necessary for the following reason.

The group health plan will respond to your request by _____ [list date that is no later than 60 days from the date of the request].

Denial of Access

The Plan received your request to access health information on _____. Your request is denied for the following reason [state the basis for the denial]:

You may file a complaint regarding this decision with the designated privacy officer, [Name], [Company], [Address], [Telephone] or the U.S. Department of Health and Human Services.

In certain cases you are entitled to appeal the denial of access. You are entitled to an appeal if access was denied because in the opinion of a licensed health care professional, granting access is likely to endanger the life or physical safety of you or another person. If you appeal, your appeal will be reviewed by a licensed health care professional designated by the Plan who did not participate in the original decision. The appeal and notice of the appeal decision will be conducted promptly.

INDIVIDUAL REQUEST NOT TO USE OR DISCLOSE HEALTH INFORMATION

I understand that the Health Plan may use and disclose protected health information about me for purposes of health care treatment, payment and health operations without my consent. I request to restrict use and disclosure of protected health information concerning health care treatment, payment or health care operations about me by the Health Plan in accordance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

Group Health Plan Not Required To Agree

I understand that the Plan is not required to agree to this restriction.

Termination of Restriction

I understand that if the Plan agrees to this restriction, either the Plan or I may terminate this restriction at any time. The termination of the restriction is only effective for future uses and disclosures.

Emergency Treatment Exception

I understand that if protected health information must be used or disclosed to provide emergency treatment for me, then this restriction is void.

Questionnaire

Requestor: Please complete all of the following questions. If the question is not applicable, mark N/A on the answer line.

(1) I request the following information be restricted [description of information]:

(2) I request that use and disclosure of the above described information be restricted in the following manner [description of restriction]:

(3) I request that my protected health information not be disclosed to the following individuals or entities [list individuals or entities to which information would not be disclosed]:

I understand that if a restriction is not specifically listed above and agreed to in writing by the Plan, it will not be effective.

Signature: _____

Date: _____

INDIVIDUAL REQUEST TO CORRECT OR AMEND A RECORD

I, _____, [Employee Name] request the Health Plan to amend the protected health information in its designated record set.

Specific Statement of Amendment Request

Specific Reason for Amendment Request

I understand that if the protected health information was not created by the Health Plan, the Health Plan is not required to honor my request. For example, if the information I wish to amend is in a medical report created by my physician, I must ask the physician – not the Plan – to amend the report. I also understand that if the information is not available for my inspection, is not part of the Plan’s designated record set or is already accurate and complete, I cannot amend the information.

I understand that the Health Plan will respond to my request within 60 days.

Signature _____ Date _____

HEALTH PLAN'S RESPONSE TO AMENDMENT OR CORRECTION REQUEST

Grant

Your request to amend or correct your health information has been granted. The Plan will make an appropriate amendment to the designated record set.

You must provide the Plan with the names of any persons to which you wish to provide the amended information. The Plan then will make reasonable efforts to inform these individuals – and persons that the Plan knows may have relied or could rely on the information – of the amendment within a reasonable time.

Needs for Extension of Time

The Plan received your request to amend health information on _____. The Plan has evaluated your request to amend health information. A delay in action is necessary for the following reasons:

The Plan will respond to your request by _____ [list date that is no later than 60 days from the date of the request].

Denial of Amendment

The Plan received your request to amend health information on _____. Your request is denied for the following reason [state the basis for the denial]:

Statement of Disagreement

You have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement must be limited to two single-sided 8-1/2 x 11 pages. [The length restriction may be established by the plan and must be reasonable.] The statement of disagreement should be filed within 60 days of this notice with [Name], [Company], [Address], [Telephone]. The Plan has the right to prepare a rebuttal statement to your statement of disagreement. If it does so, you will receive a copy.

If you do not submit a statement of disagreement, you may request that the Plan provide your request for amendment and this denial of amendment with any future disclosures of protected health information that is the subject of this request.

You may file a complaint regarding this decision with the group health plan or the U.S. Department of Health and Human Services. If you file a complaint with the Plan, please file it in writing with the following person: [Name], [Company], [Address], [Telephone].

SAMPLE INTERNAL LOG OF MEDICAL RECORD DISCLOSURES

Date	Name of Individual	Name of Party to Which Information Was Disclosed	Summary of Disclosed Information	Date of Authorization
1/1/2004	Jane Doe	Employer's disability insurer	Records relating to hospitalization length of stay.	Authorization dated 5/1/2003
1/2/2004	John Doe	Employer's workers' compensation insurer	Records showing amounts paid by employer's self-insured group health plan for injuries claimed as a result of 12/1/2003 accident	Authorization dated 4/1/2003

MEDICAL CLAIMS SERVICE, INC.

**ACCEPTANCE OF APPOINTMENT
AS PRIVACY OFFICER**

_____, having been duly appointed by the Board of Directors of Medical Claims Service, Inc. to serve as the privacy officer as required under the Health Insurance Portability and Accountability Act of the Medical Claims Service, Inc. Flexible Benefits Plan, and _____, having been duly appointed by the Board of Directors of Medical Claims Service, Inc. to serve as the privacy officer as required under the Health Insurance Portability and Accountability Act of the Medical Claims Service, Inc. Health Plan, hereby accept such appointment and agree to serve as such with all responsibilities and obligations attendant thereto.

ATTEST:

ATTEST:

RECOMMENDED VOTES FOR BOARD OF TRUSTEES

March _____, 2003

VOTED: That the Corporation hereby approves, authorizes and adopts, effective as of April 14, 2003, the First Amendment to the _____ Flexible Benefits Plan.

VOTED: That the Corporation hereby approves, authorizes and adopts, effective as of April 14, 2003, the First Amendment to the _____ Health Plan.

VOTED: That the Corporation hereby approves, authorizes and adopts, effective as of April 14, 2003, the First Amendment to the _____ Medical Expense Reimbursement Plan.

VOTED: That the Corporation hereby appoints _____ as the privacy officer of the _____ Flexible Benefits Plan (which would include the _____ Medical Expense Reimbursement Plan) and _____ as the privacy officer of the _____ Health Plan, as required under the Health Insurance Portability and Accountability Act.

VOTED: That the President of the Corporation be, and hereby is, authorized and directed to execute the foregoing Amendments for and on behalf of the Corporation.

VOTED: That the officers of the Corporation be, and each of them hereby is, authorized and directed to take all such actions and execute all such documents as may be necessary or appropriate to implement the foregoing votes.

