TOWN OF HARDWICK

HIPAA PRIVACY RULE POLICIES AND PROCEDURES

Approved by the Select Board on April 8, 2004

Effective April 14, 2004

Introduction to HIPAA Privacy Rule Policies and Procedures

I. Status as a Covered Entity

The Town of Hardwick sponsors at least one (1) employee benefit plan that:

(A) satisfies the definition of an "employee welfare benefit plan" under the Employee Retirement Income Security Act of 1974 ("ERISA");

(B) provides or pays for "medical care" (as that term is defined in the Public Health Service Act);

(C) to employees or their dependents, directly or through insurance, reimbursement, or otherwise; and

(D) has at least fifty (50) participants (as that term is defined by ERISA) **or** is administered by a third party.

Each such employee benefit plan arguably qualifies as a "group health plan" under the Standards for Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164 ("Privacy Rule"), which was promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

A "group health plan" is a HIPAA Privacy Rule covered entity, and as a result, it is obligated to comply with the Privacy Rule.

II. HIPAA Group Health Plan(s)

More specifically, the Medical, and Dental each arguably meet the definition of a "group health plan".

III. HIPAA Privacy Rule Policies and Procedures

Any questions or concerns regarding the Policies and Procedures should be directed to the HIPAA Privacy Official, Joyce Chase, Office Manager at Hardwick, Vermont, 05843 (802) **472-6120** (Phone No.), or (802) **472-3793** (Facsimile No.).

IV. HIPAA Hybrid Entity

Employee welfare benefit plans that are subject to the Employee Retirement Income Security Act of 1974 ("ERISA") are considered separate and distinct legal entities from the employer who sponsors the plans. However, no such distinction exists for non-ERISA plans. Accordingly, the Town of Hardwick has designated a HIPAA hybrid entity, to more precisely focus and isolate its compliance activities, and to segregate the group health plan functions from the non-group health plan functions. See, Hybrid Entity Designation.

V. Privacy Official

These Policies and Procedures require the Privacy Official to oversee all compliance efforts, and to be integrally involved in privacy related issues.

VI. Other Important Information

The Town of Hardwick has arranged for its employees to receive health and other benefits through VLCT Health Trust. Some of these benefits are delivered through individual programs that may be "group health plans" under the Privacy Rule.

There is some question as to whether the Town of Hardwick is obligated to comply with HIPAA regulations (including the Privacy Rule), as it concerns those programs that are established and maintained by VLCT Health Trust. These programs arguably include the medical and dental plans that are made available to the Town of Hardwick as a result of its participation in VLCT Health Trust.

The Privacy Rule relies heavily upon ERISA in establishing obligations for group health plans. Unfortunately, the Privacy Rule is not as clear as it otherwise might be with respect to the link between ERISA and Privacy Rule health plan issues, especially as it concerns those plans that are or may be exempt from ERISA coverage.

The Privacy Rule defines a "group health plan" as an "employee welfare benefit plan," as that term is defined by ERISA, and ERISA defines an "employee welfare benefit plan" as:

> [a]ny plan, fund or program which was heretofore or is hereafter established or maintained by an employer . . . to the extent that such plan, fund or program was established or is maintained for the purpose of providing for its participants or their beneficiaries, through the purchase of insurance or otherwise . . . [certain benefits].

This definition makes no reference to governmental plans. Consequently, even an ERISA exempt plan, such as a governmental plan, can satisfy the ERISA employee welfare benefit plan definition.

The term "employer" in the foregoing definition means:

> [a]ny person acting directly as an employer, or indirectly in the interest of an employer, in relation to an employee benefit plan; and includes a group or association of employers acting for an employer in such capacity.

The Department of Labor (a governmental agency overseeing ERISA issues) and United States courts have engaged in detailed factual analyses to determine, in given situations, whether a specific group or association of employers "acts for an employer."

One could potentially argue that VLCT Health Trust is the "employer" that sponsors the group health plans that it established and maintains, as a bona fide group or association of employers. Further, one could then argue that it is VLCT Health Trust, and not the Town of Hardwick, who is obligated to comply with the Privacy Rule. VLCT Health Trust has made it clear that there is no certainty or guarantee with respect to this conclusion.

Nevertheless, there appears to be a good faith argument that VLCT Health Trust is the entity that must comply with the Privacy Rule with respect to those plans that it established and maintained. As a result, the Town of Hardwick is not attempting to achieve compliance with the Privacy Rule for those specific plans. More specifically, the Town of Hardwick is not attempting to achieve compliance with the Privacy Rule with respect to medical, dental, wellness, and EAP.

However, the Town of Hardwick notes that even if it were the entity that was responsible for compliance with the Privacy Rule with respect to these plans, then at least the medical and dental plans would arguably be considered to be plans that provide benefits solely through an insurance contract with a health insurance issuer or HMO, and as a result, could be entitled to lesser compliance obligations under the Privacy Rule with respect to those plans. As it concerns those plans:

(A) The medical plan provides health benefits solely through an insurance contract with a health insurer issuer, Blue Cross and Blue Shield of Vermont, and the dental plan provides health benefits solely through an insurance contract with a health insurance issuer, Northeast Delta Dental.

(B) The plans do not create or receive any protected health information, with the exception of summary health information or information on whether an individual is participating in the plans, or is enrolled in or has disenrolled from the health insurance issuers that provide the plans.

(C) More specifically, plan sponsor employees will receive invoices containing information on specific persons who are enrolled in the plans, their specific coverage selections, and the premiums due for those persons. In addition, plan sponsor employees may occasionally engage in advocacy activities for a plan participant, but they do not receive any PHI from the health insurance issuer or other third party, without a properly completed authorization form permitting the health insurance issuer or other third party to disclose PHI to the plan sponsor.

(D) The plans, even if the Town of Hardwick had to pursue Privacy Rule compliance, would have minimal compliance obligations under the Privacy Rule, because they provide health benefits solely through an insurance contract with a health insurance issuer, and because they do not create or receive PHI in addition to summary health information, or information on whether an individual is participating in the plans, or is enrolled in or has disenrolled from the plans.

(E) Nevertheless, these plans would be obligated to comply with Paragraphs 4, 5 and 7 of the Administrative Requirements Policy and Procedure, which they will do.

(F) In addition, there is some confusion on whether the obligations to enter into business associate contracts and to amend plan documents apply to plans of this type (See, Policies and Procedures on Business Associates and Disclosures to Plan Sponsor). In light of the argument that the compliance obligations for these plans exist at the VLCT Health Trust level, and because there is truly confusion on the applicability of these specific obligations to such plans, the Town of Hardwick does not believe it necessary to pursue these obligations.

(G) The Town of Hardwick will consider revising its positions on the issues identified above, to the extent that the Department of Health and Human Services, a court or other third party provides guidance with respect to these issues that would lead the Town of Hardwick to reconsider these positions.

IMPORTANT DEFINITIONS

Privacy Rule Sections: 45 CFR 160.103, 164.103, 164.501, and 164.504

Effective Date: April 14, 2004

The following terms are defined by HIPAA, and are used in these Policies and Procedures. In most cases, the definitions below are the same as they appear in HIPAA, though in some cases definitions have been modified, for ease in use or for contextual purposes.

Business Associate:

Generally, a business associate is any person or entity who:

On behalf of a covered entity, performs, or assists in the performance of, functions or activities involving the use or disclosure of individually identifiable health information (e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re- pricing).

To or for a covered entity, provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where the service involves the disclosure of individually identifiable health information from a covered entity (or another business associate) to the business associate.

A member of a covered entity's workforce is not a business associate.

Covered Entity:

Among others, a health plan is a covered entity. The definition of "health plan" includes a "group health plan".

De-Identified Health Information (the following is the second category of de-identified health information, which is referenced in the definition of "summary health information" below): Information from which the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

Names;

All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such

age, except that such ages and elements may be aggregated into a single category of age 90 or older;

Telephone numbers;
Fax numbers;
Electronic mail addresses;
Social security numbers;
Medical record numbers;
Health plan beneficiary numbers;
Account numbers;
Certificate/license numbers;
Vehicle identifiers and serial numbers, including license plate numbers;
Device identifiers and serial numbers;
Web Universal Resource Locators (URLs);
Internet Protocol (IP) address numbers;
Biometric identifiers, including finger and voice prints;
Full face photographic images and any comparable images; and
Any other unique identifying number, characteristic, or code, except as permitted by the Privacy Rule (more specifically, by Section 164.514(c)); **and**

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Designated Record Set:

A group of records maintained by or for a covered entity that is:

The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a group health plan; or

Used, in whole or in part, by or for a group health plan to make decisions about individuals.

"Records" include any item, collection, or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a group health plan.

Disclosure:

Release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Group Health Plan:

An employee welfare benefit plan (as defined in section 3(1) of ERISA, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to

employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

Is administered by an entity other than the employer that established and maintains the plan.

Health Care Component:

A component or combination of components of a hybrid entity designated by the hybrid entity in accordance with Section 164.105(a)(2)(iii)(C).

Health Care Operations:

Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, 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 claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) of the Privacy Rule (pertaining to underwriting and related purposes) are met, if applicable;

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 entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

Business management and general administrative activities of the entity, including, but not limited to:

Management activities relating to implementation of and compliance with the requirements of the Privacy Rule;

Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;

Resolution of internal grievances;

The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

Consistent with the applicable requirements of Section 164.514 of the Privacy Rule, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Hybrid Entity:

A single legal entity:

That is a covered entity;

Whose business activities include both covered and non-covered functions; and

That designates health care components in accordance with Section 164.105 (a)(2)(iii)(C).

Individual:

The person who is the subject of PHI.

Marketing:

To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, **unless the communication is made**:

To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:

the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;

For treatment of the individual; or

For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Payment:

The activities undertaken by:

A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

The activities identified above relate to the individual to whom health care is provided and include, but are not limited to:

Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

Risk adjusting amounts due based on enrollee health status and demographic characteristics;

Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:

Name and address;

Date of birth;

Social security number;

Payment history;

Account number; and

Name and address of the health care provider and/or health plan.

PHI:

Protected Health Information, means any information, whether oral or recorded and whether transmitted or maintained in any form or medium, that:

Is created or received by a health care provider, health plan, employer or health care clearinghouse;

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI includes demographic information collected from an individual.

PHI does not include employment records held by a covered entity in its role as an employer; it also does not include certain student health records.

Plan Administration Functions:
Administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Plan Sponsor:
As defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Psychotherapy Notes:

Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Psychotherapy notes *exclude*:

Medication prescription and monitoring;

Counseling session start and stop times;

Modalities and frequencies of treatment furnished;

Results of clinical tests; and

Summaries of diagnosis, functional status, treatment plans, symptoms, prognosis and progress to date.

Summary Health Information

Information, that may be individually identifiable health information, and:

That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

From which the information described at Section 164.514(b)(2)(i) has been deleted, except that the geographic information described in Section 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

TPO:

Treatment, **P**ayment or Health Care **O**perations

Treatment:

The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use:

The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.

Workforce:

Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

HYBRID ENTITY DESIGNATION

As a hybrid entity under the Privacy Rule, the Town of Hardwick will ensure that its designated health care components comply with the Privacy Rule.

The Town of Hardwick designates the plan(s) identified in Section II of the Introduction to these Policies and Procedures as the health care component(s) of the hybrid entity.

In addition, there are certain departments within the Town of Hardwick that perform, or assist in the performance, of functions or activities on behalf of the health care component(s), or perform services to or for the health care component(s), where such performance, assistance or service would make the departments HIPAA business associates to the component(s), if the departments and the component(s) were separate legal entities.

The Town of Hardwick designates these departments as part of the health care component(s), but only with respect to the specific performance, assistance, or services that would make the departments such HIPAA business associates, if the departments and the component(s) were separate legal entities. These departments are Personnel and Accounts Payable.

Additional health care components may be designated by the Privacy Official after April 14, 2004, depending upon the circumstances. The Privacy Official will monitor the activities of the departments identified above, and will update or modify the list of designated health care component(s), as needed.

The Town of Hardwick understands that it is required to create adequate separation, in the form of firewalls, between the health care component(s) and other components of the Town of Hardwick, and further understands that transfers of PHI held by the health care component(s) to other components of the Town of Hardwick continues to be a disclosure under the Privacy Rule, and, thus, allowed only to the same extent such a disclosure is permitted to a separate entity.

As for such adequate separation and firewalls, the Town of Hardwick makes reference to the amendment to plan documents attached as part of the Disclosure to Plan Sponsor Policy and Procedure.

POLICY AND PROCEDURE: General Uses and Disclosures of PHI

Privacy Rule Sections: 45 CFR 164.506

Effective Date: April 14, 2004

Policy

Each group health plan will use and disclose PHI in accordance with the Privacy Rule, and will not obtain an authorization before using or disclosing PHI, unless the Privacy Rule expressly so requires.

Procedure

1. The Privacy Rule permits a plan to use and disclose PHI, without enrollee authorization, for its own payment and health care operations activities. In this context, and throughout these Policies and Procedures, "enrollee" means a named insured or a covered dependent, and "enrollees" means all named insureds and dependents.
2. Of course, a plan has no actual employees, but instead relies upon plan sponsor employees and third parties for administration. Consequently, the rights identified in Paragraph 1 above (i.e., to use and disclose PHI without enrollee authorization) are implemented through the conduct of plan sponsor employees and third parties.
3. The plan sponsor employees perform plan administration functions when they engage in activities that are identified in the payment or health care operations definitions.
4. A plan does not require an authorization from an enrollee before permitting the plan sponsor to proceed with plan administration functions, if the plan amends its plan documents, in accordance with Section 164.504(f) of the Privacy Rule. The amendment designates the specific plan sponsor employees, by job type, authorized to engage in plan administration functions.
5. Each plan (other than _____) has so amended its plan documents. See, Policy and Procedure on Disclosures of PHI to Plan Sponsor.
6. Technically, a plan is also permitted by the Privacy Rule to use and disclose PHI for its own treatment activities, without enrollee authorization. However, and of course, a plan does not engage in treatment activities.
7. A plan is also permitted by the Privacy Rule to disclose PHI for the treatment activities of a health care provider, without enrollee authorization, although this is an unlikely activity.
8. A plan is also permitted by the Privacy Rule to disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information, without enrollee authorization. For example, a third party administrator could disclose PHI to a health plan (e.g., a health insurance company) for the payment activities of that health plan.
9. Very technically, a plan is also permitted by the Privacy Rule, without enrollee authorization, to disclose PHI to another covered entity for the health care operations activities of the entity that receives the information, if the plan and the other entity

either have or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to that relationship, and the disclosure is for a purpose listed in paragraph (1) or (2) of the definition of health care operations, or for the purpose of health care fraud and abuse detection or compliance. It seems unlikely that any plan would rely on this right.

POLICY AND PROCEDURE: Authorizations

Privacy Rule Sections: 45 CFR 164.508

Effective Date: April 14, 2004

Policy

The Privacy Rule requires that a group health plan obtain an authorization from an enrollee before using or disclosing PHI in certain situations. For example, authorizations are generally required before most marketing activities can take place.

An authorization will also generally be required before a plan sponsor employee may assist an enrollee with respect to coverage inquiries or in advocacy situations, as explained further below. However, it is important to note that in this context, the plan sponsor employee does not appear to be acting on behalf of a plan (i.e., he/she is not performing plan administration functions), but rather, is acting for and on behalf of the employer. Nevertheless, and although this is far from clear under the Privacy Rule, a plan may not permit a third party administrator, health insurance issuer, or HMO to disclose PHI to the plan sponsor for such inquiries or situations, without enrollee authorization.

Procedure

1. An authorization is not required when an enrollee requests the right to inspect or copy his/her own PHI directly (i.e., an authorization is not necessary when a plan is providing PHI directly to the enrollee).
2. An authorization is also not required when a plan uses and discloses PHI for its own payment or health care operation activities, or for other uses and discloses of PHI identified in the General Uses and Disclosures of PHI Policy and Procedure as permissible without enrollee authorization.
3. A plan sponsor employee will use an authorization when assisting an enrollee with respect to a coverage inquiry or in an advocacy situation. The Privacy Rule appears to consider such activities to be employment based, rather than plan based. In other words, they are not plan administration functions, the significance of which is that the Privacy Rule does not regulate the "front-end" of the activity (i.e., obtaining information from the enrollee), but does regulate the "back-end" (the provision of PHI by a third party administrator, health insurance issuer, or HMO, to the plan sponsor). The need for an authorization can be avoided if the plan sponsor employees assisting with the coverage inquiry or advocacy do not receive any PHI from a third party, but rather merely direct the enrollee to such third party.
4. In the event that the plan sponsor employee participating in the coverage inquiry or advocacy situation will receive PHI from a third party, then the plan sponsor employee will obtain an authorization from the enrollee, and will share that completed authorization with the third party, before the plan sponsor employee receives PHI from the third party. As for the form of the authorization, the plan sponsor employee can use the document attached to this Policy and Procedure, or can use a form provided by the third party, if that form meets the requirements of Section 164.508 of the Privacy Rule.
5. Significantly, the use of authorizations in the context of coverage inquiries or advocacy situations is unclear, and each plan will revisit this portion of this Policy and Procedure in

the event that clear guidance on the issue is provided by the Department of Health and Human Services, or if a more clear industry position develops.

6. Each plan has trained members of its workforce regarding:

   A. When an authorization is required by the Privacy Rule;

   B. The information that must be included within an authorization;

   C. The fact that any use or disclosure that the plan makes of PHI under an authorization must be expressly permitted by the specific terms of the authorization; and

   D. The fact that the permissions granted in the authorization may not be acted upon, to any extent, if the authorization has been revoked or has expired.

7. A form authorization is attached to this Policy and Procedure.

8. In most situations, an enrollee is not obligated to sign an authorization, and the enrollee can refuse to sign the authorization, without any negative repercussions. However, a plan may condition enrollment or eligibility for benefits on execution of an authorization that is requested by the plan prior to the individual's enrollment in the plan, if the authorization sought is for the plan's eligibility or enrollment determinations relating to the individual, or for its underwriting or risk rating determinations, and the authorization is not for a use or disclosure of psychotherapy notes. If a person refuses to sign an authorization in this context, he/she may be denied enrollment in the plan or eligibility for health care benefits.

9. In each case, the enrollee will be given a copy of the authorization that he/she signs, and the plan will keep the original authorization.

10. The enrollee may revoke the authorization at any time. A plan may not act upon the permissions granted in the authorization if the authorization has been revoked or if it has expired.

11. A plan must retain each signed authorization for a period of six (6) years after it was created or expired, whichever date is later. For example, if an enrollee signs an authorization on January 1, 2005, and by its terms the authorization expires on January 1, 2006, then the plan must retain the signed authorization until January 1, 2012.

Authorization Form

Name: _____ **Date of Birth:** _____

DO NOT SIGN A BLANK FORM. You or your personal representative should read the descriptions below before signing this form.

(1) Who will use or disclose the information? The person(s) or classes of persons authorized to use or disclose the information are described below.

_____

_____

(2) To whom may the information be disclosed? The person(s) or classes of persons authorized to receive the information are described below.

_____

_____

(3) What information will be used or disclosed? The specific information that may be used or disclosed is described below.

_____

_____

(4) What is the purpose of each use or disclosure? The purposes for which the information will be used or disclosed are described below.

_____

_____

(5) When will this authorization expire? The date or event that will trigger the expiration of this authorization must be described below.

_____

SPECIFIC UNDERSTANDINGS

By signing this authorization form, you authorize the use and/or disclosure of your protected health information as described above. You understand that the information identified above could be re-disclosed by the recipients and, if so, may not be subject to federal or state laws protecting its confidentiality.

You have a right to refuse to sign this authorization. Your health care, the payment for your health care, and your enrollment or eligibility for health care benefits will not be affected if you do not sign this form.

You have a right to receive a copy of this form after you have signed it.

If you sign this authorization, you will have the right to revoke it at any time, except to the extent that we have already taken action based upon your authorization. To revoke this authorization, you must write to _____.

SIGNATURE

I have read this form and all of my questions about this form have been answered. By signing below, I acknowledge that I have read and accept all of the above.

_____ Signature of Individual or Personal Representative

_____ Print Name of Individual or Personal Representative

_____ Date

Description of Personal Representative's Authority

Instruction Sheet

General Instructions

1. Complete each blank in the form – the authorization is not valid unless all required information has been identified.
2. If an authorization is for marketing, you must add a paragraph to the authorization indicating whether you will receive direct or indirect remuneration in connection with the authorization. This paragraph should be added as section (6) of the form, and should state:

   We will/will not receive direct or indirect remuneration in connection with the use or disclosure of the information identified above.
3. Do not combine a single authorization for the use or disclosure of health information with any other document (such as a consent form or any other authorization form).
4. You may not condition the provision of health care, payment for health care, or health care benefits on the execution of an authorization, with certain limited exceptions. You should seek the review of counsel in any situation where such conditioning is proposed (especially because the authorization will need to be modified in such instances).
5. The authorization must be signed and dated by the enrollee/personal representative. If the form is signed and dated by the personal representative, then there must be a statement of that person's authority to act for the enrollee (e.g., legal guardian).

Specific Instructions (relating to the numbered paragraphs in the form)

1. Identify the specific class of persons who will use, or disclose, the health information. Remember that if you are using the authorization in the context of a coverage inquiry or an advocacy situation, the authorization is to allow a third party (e.g., a third party administrator) to disclose PHI to the plan sponsor.
2. Identify the specific class of persons to whom the information will be disclosed.
3. Identify the health information at issue in a specific and meaningful fashion.
4. Identify the purpose of each use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an enrollee initiates the authorization and does not, or elects not to, provide a statement of the purpose.
5. Identify the expiration date or expiration event that relates to the enrollee or the purpose of the use or disclosure. You may identify a specific date, a specific time period, or an event directly related to the enrollee or the purpose of the authorization.

POLICY AND PROCEDURE: Business Associates

Privacy Rule Sections: 45 CFR 164.502(e) and 504(e)

Effective Date: April 14, 2004

Policy

A group health plan has relationships with certain third parties that are considered business associates under the HIPAA Privacy Rule. A plan is required to enter into written contacts with these business associates, to ensure the business associates appropriately use and disclose PHI.

Procedure

1. As of April 14, 2004, the following are plan business associates:
   A. Sullivan, Powers and Company, with respect to the auditing services provided for the Town of Hardwick;
   B. _____, with respect to _____ services provided for _____;
   C. _____, with respect to _____ services provided for _____;
   D. _____, with respect to _____ services provided for _____; and
   E. _____, with respect to _____ services provided for _____.
2. A plan has or will enter into written contracts with these business associates. The contracts were drafted to comply with the requirements of the Privacy Rule and the requirements that the HIPAA Security Rule imposes with respect to business associate contracts.
3. The potential business associates have been identified through meetings with persons who would be aware of the existence of business associate relationships.
4. Each plan will closely examine new service relationships to determine if they require the use or disclosure of PHI, and whether they give rise to business associate obligations.
5. Each plan has provided training to those groups who might be responsible for the development, negotiation, and execution of business associate contracts in the future. The training has focused on the identification of business associates, and the specific obligations business associates are required to accept under the Privacy Rule.
6. Each plan is aware that it may be obligated to terminate the underlying relationship with a business associate if the business associate breaches any material term or condition of the business associate contract. Consequently:

   A. Appropriate personnel have been informed to promptly notify the Privacy Official of any suspected breach of a business associate contract.

B. The Privacy Official will promptly advise counsel of the situation, upon learning of the breach, and will seek guidance from counsel on how to address the matter in accordance with Section 165.504(e) of the Privacy Rule.

C. A plan will take reasonable steps to cure any such breach and will seek the assistance of the business associate in that effort.

D. A plan will terminate the underlying relationship with the business associate if the breach cannot be cured and termination of that relationship is otherwise feasible. In this context, "underlying relationship" means the relationship under which the business associate provides services to the plan.

E. The Privacy Official will work closely with counsel to determine whether a termination would be "feasible" under any given circumstance. In the event a termination would not be feasible, the plan must notify the Secretary of the Department of Health and Human Services of the situation (i.e., of the breach and the failure to resolve the breach).

F. Each business associate contract requires the business associate, upon termination of such underlying relationship, to return or destroy all PHI received from the plan, or created or received by the business associate on behalf of the plan. The Privacy Official will closely monitor such return or destruction of PHI by a business associate.

POLICY AND PROCEDURE: Disclosures to Plan Sponsor

Privacy Rule Sections: 45 CFR 164.504(f)

Effective Date: April 14, 2004

Policy

A group health plan will only disclose PHI to the plan sponsor (or permit a health insurance issuer or HMO with respect to the plan to make such a disclosure) after following the requirements of the Privacy Rule.

Procedure

1. Except as set forth below, a plan may not disclose PHI, or permit a health insurance issuer or HMO with respect to the plan, to disclose PHI, to the plan sponsor, unless the plan documents under which the plan is established or operated are amended, in accordance with Privacy Rule requirements.

2. Notwithstanding the foregoing, a plan can disclose PHI, and can permit a health insurer or HMO with respect to the plan, to disclose PHI, to the plan sponsor, without amending plan documents, in the following situations:
   - A. A plan, or a health insurance issuer or HMO with respect to the plan, receives written authorization from an enrollee to disclose PHI to the plan sponsor.
   - B. A plan, or a health insurance issuer or HMO with respect to the plan, discloses summary health information to the plan sponsor, at the request of the plan sponsor, for the purpose of obtaining premium bids from health insurance issuers or HMOs for providing health insurance coverage under the plan.
   - C. A plan, or a health insurance issuer or HMO with respect to the plan, discloses summary health information to the plan sponsor, at the request of the plan sponsor, for the purpose of modifying, amending or terminating the plan.
   - D. A plan, or a health insurance issuer or HMO with respect to the plan, discloses information to the plan sponsor on whether an individual is participating in the plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
3. Otherwise, a plan may not disclose PHI, and may not permit a health insurance issuer or HMO with respect to the plan to disclose PHI to the plan sponsor, unless:

   The plan receives certification from the plan sponsor that the plan documents have been modified as required by the Privacy Rule; and

   The uses and disclosures of PHI by the plan sponsor will be restricted to plan administration functions performed by the plan sponsor on behalf of the plan, in accordance with the plan documents.

4. The applicable amendment and certification are attached to this Policy and Procedure.
5. The amendment of plan documents is one area where the distinctions between ERISA covered plans and non-ERISA covered plans becomes very important. In the ERISA context, there are plan documents (e.g., the bargaining agreement, trust

agreement, contract or other instrument under which the plan is established or operated, and a summary plan description). In the non-ERISA context, there are not necessarily any "plan documents" to amend. Nevertheless, each plan will proceed with the amendment, and will, if necessary, prepare a short document identifying the benefits it provides to serve as the "plan document."

6. A primary purpose of the certification, and the plan document amendment, is to restrict the plan sponsor from using PHI for any employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the plan sponsor.
7. The Notice of Privacy Practices includes a statement informing enrollees that PHI may be disclosed to the plan sponsor.

AMENDMENT TO PLAN DOCUMENTS, EFFECTIVE APRIL 14, 2004

This Amendment is intended to bring the Group Health Plan(s) (as such term is defined at 45 CFR 160.103) identified below into compliance with the requirements of the Standards for Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164 (the "Privacy Rule"), and the requirements of the Security Rule, at 45 CFR Parts 160 and 164 (the "Security Rule"), each of which were promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996, by establishing the extent to which the Plan Sponsor identified below will receive, use and/or disclose Protected Health Information (as such term is defined at 45 CFR 160.103).

IN WITNESS WHEREOF, Plan Sponsor executes this amendment to be effective as of the day and year written above.

Plan Sponsor: _____

By: _____

Name: _____

Title: _____

Accordingly, the Plan Documents, as defined below, of the Plan, as defined below, are amended as follows:

I. Definitions

A. All capitalized terms used in this Amendment shall have the meanings provided by this Amendment or 45 CFR Parts 160 or 164.

For purposes of this Amendment:

1. **"Plan"** means each of the following Group Health Plans:

(a) ;

(b) ;

(c) ;

(d) ; and

(e) .

but only to the extent a Plan satisfies the definition of a "Group Health Plan" (e.g., if the Department of Health and Human Services determines that a specific Plan is not subject to the Privacy Rule as a Group Health Plan, then this amendment will be deemed automatically modified to the extent necessary to remove such Plan from the scope of this Amendment).

2. **"Plan Documents"** means all governing documents and instruments (i.e., all documents under which each Plan was established or is operated), including, but not limited to, any summary plan description applicable to any such Plan.

3. **"Plan Sponsor"** means _____.

4. **"PHI"** means Protected Health Information.

5. **"Electronic PHI"** means Electronic Protected Health Information.

II. Effect of Amendments

A. These amendments are made, on a separate and individual basis, with respect to each Plan.

III. Disclosure of PHI to the Plan Sponsor

A. A Plan shall disclose PHI, or permit a health insurance issuer or HMO with respect to the Plan, to disclose PHI, to the Plan Sponsor, only to the extent necessary for the Plan Sponsor to perform Plan Administration Functions, such as those activities that meet the definition of Payment or Health Care Operations under the Privacy Rule (See, 45 CFR 164.501).

IV. Use and Disclosure of PHI by Plan Sponsor

A. Plan Sponsor may use and/or disclose PHI only to the extent necessary to perform the Plan Administration Functions.

V. Plan Sponsor Certification

A. The Plan agrees that it will only disclose PHI to the Plan Sponsor upon receipt of a certification by the Plan Sponsor that this Amendment has been adopted and that the Plan Sponsor agrees to abide by the following:

1. The Plan Sponsor will not use or disclose any PHI received from the Plan, other than as permitted or required by this Amendment or as Required by Law.
2. The Plan Sponsor will ensure that any agents, including a subcontractor, to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such PHI.
3. The Plan Sponsor will not use or disclose such PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor.
4. The Plan Sponsor will report to the Plan any use or disclosure of such PHI that is inconsistent with the uses or disclosures provided for in this Amendment, of which it becomes aware.

5. The Plan Sponsor will make available PHI to the Plan, to permit the Plan to respond to a request for access, in accordance with Section 164.524 of the Privacy Rule.

6. The Plan Sponsor will make available PHI for amendment and incorporate any amendments to PHI in accordance with Section 164.526 of the Privacy Rule.

7. The Plan Sponsor will make available to the Plan the information required to provide an accounting of disclosures in accordance with Section 164.528 of the Privacy Rule.

8. The Plan Sponsor will make its internal practices, books and records relating to the use and disclosure of PHI received from the Plan available to the Secretary for purposes of determining compliance by the Plan with the Privacy Rule.

9. The Plan Sponsor, if feasible, will return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, the Plan Sponsor will limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

10. The Plan Sponsor will ensure that the adequate separation identified below is established.

VI. Adequate Separation

A. In accordance with Section 164.504 of the Privacy Rule, this section describes the employees or classes of employees or other persons under the control of the Plan Sponsor who may be given access to PHI disclosed to the Plan Sponsor.

Department	Class	Plan Affected
Payroll/Personnel		Medical/Dental
Accounts Payable		Medical/Dental

B. This list reflects the employees, classes of employees, or other workforce members of the Plan Sponsor who receive PHI related to Payment under, Health Care Operations of, or other matters pertaining to Plan Administration Functions that the Plan Sponsor provides for the Plan. These individuals will have access to and use PHI solely to perform the Plan Administration Functions, and they will be subject to disciplinary action and/or sanctions (including termination of employment or affiliation with the Plan Sponsor) for any use or disclosure of PHI in violation of, or noncompliance with, the provisions of this Amendment.

C. The Plan Sponsor will promptly report any such violation or noncompliance to the Plan and will cooperate with the Plan to correct the violation or noncompliance, to impose appropriate disciplinary action and/or sanctions, and to mitigate any deleterious effect thereof.

VII. Security Rule Issues

As of the Security Rule compliance date:

A. The Plan Sponsor will implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of the Plan.

B. The Plan Sponsor will ensure that the adequate separation identified above is supported by reasonable and appropriate Security Measures.

C. The Plan Sponsor will ensure that any agent, including a subcontractor, to whom it provides Electronic PHI agrees to implement reasonable and appropriate Security Measures to protect the Electronic PHI.

D. The Plan Sponsor will report to the Plan any Security Incident pertaining to such Electronic PHI of which it becomes aware.

CERTIFICATION PURSUANT TO 45 CFR 164.504(f)

I. The Town of Hardwick is the Plan Sponsor of each Plan identified in the attached Amendment to Plan Documents, as the terms Plan and Plan Documents are defined in such Amendment.

II. Plan Sponsor performs Plan Administration Functions for each such Plan, as set forth in the Amendment, and needs access to Protected Health Information to carry out those functions, as the terms Plan Administration Functions and Protected Health Information are defined at 45 CFR 164.504 and 45 CFR 160.103, respectively.

III. Plan Sponsor hereby certifies that the Plan Documents have been amended effective April 14, 2004 to comply with Section 164.504(f) of the Standards for Privacy of Individually Identifiable Health Information, and Section 164.314(b) of the Security Standards.

IV. Plan Sponsor adopts such Amendment, and will comply with its terms.

By: _____

Name: _____

Title: _____

Date: _____

POLICY AND PROCEDURE: Access to PHI

Privacy Rule Sections: 45 CFR 164.524

Effective Date: April 14, 2004

Policy

Each group health plan will comply with the Privacy Rule provisions regarding access to PHI contained in a designated record set.

Procedure

1. Plan sponsor employees who perform plan administration functions do not maintain significant amounts of enrollee PHI. A third party administrator will likely maintain more PHI.
2. A plan will request that a third party administrator respond to most, if not all, requests to access PHI contained in a designated record set.
3. As a general rule, plan sponsor employees performing plan administration functions desire to limit their access to PHI whenever and wherever reasonably possible. As a result, they do not wish to have an active role in responding to requests for access to PHI, to the extent the requests pertain to information held by a third party administrator. In other words, they do not wish to be "in the middle" of such requests, and thus potentially receive more PHI than they otherwise would or need to receive.
4. Nevertheless, those plan sponsor employees will take reasonable steps to ensure that a third party administrator does not inappropriately deny any request to access PHI by an enrollee/personal representative.
5. A plan will take steps to coordinate requests for access to PHI with a third party administrator, to ensure that the administrator includes any PHI held by such employees in their response to the requests. Otherwise, a plan will need to take steps to ensure that it directly responds to such requests, as it concerns the information held by such plan sponsor employees.
6. The remainder of this Procedure provides guidance in the event that a plan must directly respond to an access request, with respect to the PHI held by those plan sponsor employees who perform plan administration functions.
7. A plan requires that all requests for access to PHI by an enrollee/personal representative be made in writing (See, the Notice of Privacy Practices).
8. A plan will review each written request for access with the Privacy Official to determine whether an access request should be granted.
9. A plan will attempt to respond to each request for access to PHI within ten (10) business days, though, if necessary, the plan may have more time. More specifically:

    A. The plan must respond to a request for access to PHI within thirty (30) days after receipt of the access request.

B. The plan may extend the response period for an additional thirty (30) days, but only if it notifies the enrollee/personal representative, in writing, of the delay, the reason for the delay, and the date by which it will respond to the request. The plan must ensure that the writing is delivered within the original response period (i.e., within thirty (30) days after receipt of the access request).

C. The plan may not have any additional extensions of time to respond to an access request.

10. If an access request is accepted, the plan will notify the enrollee/personal representative of that fact, in writing.

11. A plan will permit the enrollee/personal representative to inspect the PHI on premises, to obtain a copy of the PHI, or both.

12. A plan will provide access in the form or format requested by the enrollee/personal representative, if it is readily reproducible in such form or format (if not, the plan will provide access in a readable, hard copy form, or in such other form or format as the plan and the enrollee/personal representative may agree upon).

13. A plan may provide the enrollee/personal representative with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to a summary or explanation and to the fees imposed, if any, by the plan for the summary or explanation.

14. A plan may charge the following fees when responding to access requests:

A. A reasonable cost based fee for copying, including labor and supplies (for instance, paper, computer disks).

B. The cost of postage when an enrollee/personal representative requests that the information be mailed.

C. A nominal fee for preparing an explanation or summary of the requested PHI if the enrollee/personal representative is informed of and agrees to receive such summary or explanation and is willing to pay the fee.

15. A plan will not charge for the cost of retrieving or handling PHI or for processing an access request.

16. If an access request is denied, in whole or in part, a plan will notify the enrollee/personal representative of the denial, in writing.

17. The denial letter must be sent within the time periods set forth above (i.e., thirty (30) days from the date the original request was received, or sixty (60) days from the date the original request was received, if the extension identified above in Paragraph 9 is properly obtained).

18. A plan may deny access for the reasons identified below.

19. A plan must, to the extent possible, afford the enrollee/personal representative access to any PHI requested, after excluding the PHI for which the plan has a ground to deny access.

20. A plan may deny access to PHI for the following reasons (*these denials are not subject to review, are final, and may not be appealed by the enrollee/personal representative*):

A. If the PHI requested is psychotherapy notes.

B. If the PHI requested was compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

C. If the PHI requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

21. A plan may deny access to PHI for the following reasons (*these denials are subject to review and the enrollee/personal representative may appeal the denial*):

A. If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the enrollee or another person.

B. If the PHI makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person.

C. If the request for access is made by a personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that access is reasonably likely to cause substantial harm to the enrollee or another person.

22. If a denial is for a reason set forth in Paragraph 21 A, B, or C, then the enrollee/personal representative may request a review of the denial by sending a written request to the Privacy Official. In that event:

A. The plan will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny access;

B. The plan will promptly refer the request to this designated review official, and the review official will determine within a reasonable period of time whether the denial is appropriate; and

C. The plan will provide the enrollee/personal representative with written notice of the determination of the designated reviewing official, and will abide by that determination.

23. A plan must document, in electronic or written format, and retain, for a period of six (6) years from the date of creation or the date when last in effect, whichever is later, the following:

A. The designated record sets that are subject to access by enrollees/personal representatives; and

B. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

24. Each plan documents its designated record sets as follows: Enrollment, Disenrollment, Claims Information. In addition, each plan confirms that its Privacy Official is the person responsible for receiving and process access requests.

25. A plan will maintain a log book indicating the date of each access request, and:

A. For requests that were granted: the date access was provided, the specific PHI at issue, and the means by which access was provided (e.g., in-person inspection, in-person copying, or mailing); and

B. For requests that were denied: the date access was denied, the specific PHI at issue, and the specific reason for the denial.

POLICY AND PROCEDURE: Amendment to PHI

Privacy Rule Sections: 45 CFR 164.526

Effective Date: April 14, 2004

Policy

Each group health plan will comply with the Privacy Rule provisions regarding amendment to PHI contained in a designated record set.

Procedure

1. Plan sponsor employees who perform plan administration functions do not maintain significant amounts of enrollee PHI. A third party administrator will likely maintain more PHI.
2. A plan will request that a third party administrator respond to most, if not all, requests to amend PHI contained in a designated record set.
3. As a general rule, plan sponsor employees performing plan administration functions desire to limit their access to PHI whenever and wherever reasonably possible. As a result, they do not wish to have an active role in responding to requests for amendment to PHI, to the extent the requests pertain to information held by a third party administrator. In other words, they do not wish to be "in the middle" of such requests, and thus potentially receive more PHI than they otherwise would or need to receive.
4. Nevertheless, those plan sponsor employees will take reasonable steps to ensure that a third party administrator does not inappropriately deny any request to amend PHI by an enrollee/personal representative.
5. A plan will take steps to coordinate requests for amendment to PHI with a third party administrator, to ensure that the administrator considers any PHI held by such employees in their response to the requests. Otherwise, a plan will need to take steps to ensure that it directly responds to such requests, as it concerns the information held by such plan sponsor employees.
6. The remainder of this Procedure provides guidance in the event that a plan must directly respond to an amendment request, with respect to the PHI held by those plan sponsor employees who perform plan administration functions.
7. A plan requires that all requests for amendment to PHI by an enrollee/personal representative be made in writing, and that they include a reason to support the requested amendment (See, the Notice of Privacy Practices).
8. A plan will contact an enrollee/personal representative in any situation where the amendment request is not clear from the writing submitted to the plan.
9. The Privacy Official will review each amendment request to determine whether the request should be granted.
10. A plan will attempt to respond to each request within thirty (30) days, though, if necessary, the plan may have more time. More specifically:

A. The plan must respond to an amendment request within sixty (60) days after receipt of the request.

B. The plan may extend the response period for an additional thirty (30) days, but only if it notifies the enrollee/personal representative, in writing, of the delay, the reason for the delay, and the date by which it will respond to the request. The plan must ensure that the writing is delivered within the original response period (i.e., within sixty (60) days after receipt of the request).

C. The plan may not have any additional extensions of time to respond to an amendment request.

11. If a plan grants an amendment request, the plan will notify the enrollee/personal representative of that fact, in writing.

12. If a plan grants an amendment request, the plan must make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment, and appending or otherwise providing a link to the location of the amendment.

13. A plan must inform the enrollee/personal representative in a timely manner (i.e., within the time frame set forth in Paragraph 10 above) that the amendment has been accepted, and obtain:

A. Identification, from the enrollee/personal representative, of relevant persons with whom the amendment needs to be shared; and

B. Agreement, from the enrollee/personal representative, to have the plan notify those persons of the amendment.

14. A plan must make reasonable efforts to inform and provide the amendment within a reasonable time to:

A. Persons identified by the enrollee/personal representative as having received PHI about him/her and needing the amendment; and

B. Persons, including business associates, that the plan knows have the PHI that is the subject of the amendment and that may have relied (or could foreseeably rely) on such PHI to the detriment of the enrollee/personal representative.

15. A plan may deny an amendment request, if the plan determines that the PHI or record that is the subject of the request:

A. Was not created by the plan, unless the enrollee/personal representative provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

B. Is not part of the designated record set;

C. Would not be available for inspection (See, Policy and Procedure on Access to PHI); or

D. Is accurate and complete.

16. If an amendment request is denied, in whole or in part, a plan will notify the enrollee/personal representative of the denial, in writing.

17. The denial letter must be sent within the time frame set forth above in Paragraph 10 for responding to an amendment request.

18. A plan must permit an enrollee/personal representative to submit to the plan a written statement disagreeing with the denial of all or part of a requested amendment and the basis for the disagreement. The plan may reasonably limit the length of a statement of disagreement (e.g., the statement may be limited to no more than five (5) pages).

19. A plan may prepare a written rebuttal to any statement of disagreement issued by an enrollee/personal representative, and must provide a copy of the rebuttal, if any, to the enrollee/personal representative.

20. A plan must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the following to the designated record set:

A. The amendment request;

B. The written denial of the amendment request;

C. The statement of disagreement issued by the enrollee/personal representative, if any; and

D. The rebuttal statement issued by the plan, if any.

21. If an enrollee/personal representative issues a statement of disagreement, the plan must include with any subsequent disclosure of PHI to which the disagreement relates, the appended material per Paragraph 20 above, or at the plan's election, an accurate summary of such information.

22. If an enrollee/personal representative has not submitted a written statement of disagreement, the plan must include with any subsequent disclosure of PHI (*but only if the enrollee/personal representative has requested such action*), the request for amendment and its denial, or an accurate summary of such information.

23. If a plan is informed by another covered entity of an amendment to PHI, then the plan must correspondingly amend the PHI in its designated record sets.

24. The Privacy Official is responsible for receiving and processing amendment requests.

POLICY AND PROCEDURE: Accountings of Disclosures

Privacy Rule Sections: 45 CFR 164.528

Effective Date: April 14, 2004

Policy

Each group health plan will comply with the Privacy Rule provisions regarding accounting for certain disclosures of PHI.

Procedure

1. Plan sponsor employees who perform plan administration functions do not disclose any significant amount of enrollee PHI. Certainly, there is no reason to believe that these employees make many disclosures of PHI that are subject to the Privacy Rule accounting obligation. However, a third party administrator of a plan may, more frequently, make the kinds of disclosures of enrollee PHI that are subject to the accounting obligation.
2. A plan will request that a third party administrator respond to most, if not all, accounting requests.
3. As a general rule, plan sponsor employees performing plan administration functions desire to limit their access to PHI whenever and wherever reasonably possible. As a result, they do not wish to have an active role in responding to accounting requests, to the extent the requests pertain to disclosures made by a third party administrator. In other words, they do not wish to be "in the middle" of such requests, and thus potentially receive more PHI than they otherwise would or need to receive.
4. Nevertheless, those plan sponsor employees will take reasonable steps to ensure that a third party administrator does not inappropriately deny any accounting request by an enrollee/personal representative.
5. A plan will take steps to coordinate accounting requests with a third party administrator, to ensure that the administrator includes any disclosures of PHI made by such employees in their response to the requests. Otherwise, a plan will need to take steps to ensure that it directly responds to such requests, as it concerns the disclosures of PHI made by such plan sponsor employees.
6. The remainder of this Procedure provides guidance in the event that a plan must directly respond to an accounting request, with respect to the disclosures of PHI made by those plan sponsor employees who perform plan administration functions.
7. An enrollee/personal representative has the right to receive in writing an accounting of disclosures of PHI made by a plan or its business associates for up to six (6) years before the date on which the accounting is requested. However, there are many exceptions to the accounting obligation, including for disclosures made:

   A. Prior to April 14, 2004;

   B. To carry out treatment, payment or health care operations;

   C. To the enrollee about himself/herself;

D. Pursuant to a HIPAA authorization;

E. To family members, other relatives, or close personal friends, of PHI directly relevant to such persons involvement with an enrollee's care or payment related to the enrollee's care; or

F. To family members, a personal representative of the enrollee, or another person responsible for the care of the enrollee, of PHI, for notification purposes.

8. A plan will assemble the information necessary to provide an accounting, if requested by an enrollee/personal representative, in connection with each disclosure of PHI it makes (through plan sponsor employees) in connection with any disclosure that is not exempted from the accounting requirement by the Privacy Rule.

9. A plan will attempt to respond to each accounting request within thirty (30) days, though, if necessary, a plan may have more time. More specifically:

A. The plan must respond to an accounting request within sixty (60) days after receipt of the accounting request.

B. The plan may extend the response period for an additional thirty (30) days, but only if it notifies the enrollee/personal representative, in writing, of the delay, the reason for the delay, and the date by which it will respond to the request. The plan must ensure that the writing is delivered within the original response period (i.e., within sixty (60) days after receipt of the accounting request).

C. The plan may not have any additional extensions of time to respond to an accounting request.

10. A plan will not charge an enrollee/personal representative a fee for the first accounting of disclosures in any twelve (12) month period. The plan may impose a reasonable, cost based fee for each subsequent request for an accounting by the same enrollee/personal representative within the same twelve (12) month period, provided that the plan informs the enrollee/personal representative in advance of the fee and provides an opportunity to withdraw or modify the request to avoid or reduce the fee.

11. A plan will track each disclosure of PHI made by such plan sponsor employees to someone other than the enrollee, without a "HIPAA" authorization, and for something other than payment or health care operations.

12. The disclosures subject to the accounting requirement generally include any disclosure *by a plan to a business associate, by the plan to any other person or entity*, or *from a business associate*, where a disclosure is:

A. Required by any Vermont or federal law;

B. For any public health activity;

C. About victims of abuse, neglect or domestic violence;

D. For any health oversight activity;

E. For any judicial or administrative proceeding (e.g., in response to a court order);

F. For any law enforcement purpose;

G. About a decedent (e.g., to a coroner or medical examiner to determine a cause of death);

H. For cadaveric organ, eye or tissue donation;

I. For any research disclosure without enrollee authorization;

J. To avert a serious threat to health or safety;

K. For specialized government functions;

L. For workers compensation (e.g., as authorized by and to the extent necessary to comply with workers compensation laws);

M. To the Secretary of the Department of Health and Human Services (e.g., in connection with a compliance review); or

N. For any wrongful or inappropriate disclosure (e.g., any disclosure that should NOT have occurred).

13. We stress that this list is general, and most of the identified categories have important sub-categories that include disclosures that are subject to the accounting requirement. For more information on the sub-categories, see 45 CFR 164.512 of the Privacy Rule. Nevertheless, a plan will be overly inclusive in the information that it retains regarding disclosures of PHI, so that if an accounting request is made, the plan has a sufficient pool of information from which to prepare a formal response.

14. A plan will meet the goal of being overly inclusive by following the rule identified in Paragraph 11 above.

15. As noted above, a plan must provide a written response to an accounting request. The writing must include the following elements, for each disclosure subject to the accounting requirement:

A. The date of the disclosure;

B. The name of the entity or person who received the PHI and the address of such entity or person (if known);

C. A brief description of the PHI disclosed; and

D. A brief statement of the purpose of the disclosure that reasonably informs the enrollee/personal representative of the basis for the disclosure.

16. The Privacy Rule permits an abbreviated response to an accounting request in some situations. More specifically, the Privacy Rule permits an abbreviated response where multiple disclosures of PHI are made by a plan during the applicable accounting period to the same person or entity for a single purpose under 45 CFR 164.502(a)(2)(ii) (i.e., disclosures made to the Secretary of the Department of Health and Human Services for compliance reviews) or 164.512 (e.g., public health, health oversight, and law enforcement disclosures). In these situations, the plan need only provide the following:

A. The elements required for the first disclosure during the accounting period as described in Paragraph 15;

B. The frequency, periodicity or specific number of disclosures made during the accounting period; and

C. The date of the last such disclosure during the accounting period.

The plan sponsor employees performing plan administration functions only rarely disclose PHI for purposes other than payment or health care operations. Consequently, this option will likely not be available very often for them.

17. A plan must account for disclosures that should not have been made. In other words, the plan must track all disclosures that were mistakenly made, or that were otherwise in violation of the Privacy Rule.

18. Each plan understands that "disclosure" is broadly defined under the Privacy Rule, and includes situations where PHI is made accessible to a third party.

19. As set forth above, the plan sponsor employees performing plan administration functions will coordinate any request for an accounting with any business associate engaged in any activity for which an accounting would be required. A plan must provide an accounting of disclosures *to the business associate* (if the business associate is assisting the plan in an activity that is subject to an accounting requirement) and *from a business associate* (if the business associate disclosed PHI for any type of disclosure that is subject to the accounting requirement).

20. All requests for an accounting will be coordinated with the Privacy Official, to ensure that timely responses are provided, and to properly make any permitted charge.

21. The Privacy Official is responsible for all necessary record-keeping.

22. A plan must document in electronic or written format and retain for six (6) years from the date of its creation or the date when it was last in effect, whichever is later, the following:

A. The information required to be in an accounting per Paragraph 15, for each disclosure subject to the accounting requirement;

B. Each written accounting provided to an enrollee/personal representative; and

C. The titles of the persons or offices responsible for receiving and processing requests for accountings by individuals (i.e., the Privacy Official).

POLICY AND PROCEDURE: Restrictions

Privacy Rule Sections: 45 CFR 164.522

Effective Date: April 14, 2004

Policy

Each group health plan will comply with the Privacy Rule provisions regarding restrictions on the use or disclosure of PHI.

Procedure

1. Plan sponsor employees who perform plan administration functions do not use or disclose significant amounts of enrollee PHI. A third party administrator will likely use and disclose more PHI.
2. A plan will request that a third party administrator respond to most, if not all, restriction requests.
3. As a general rule, plan sponsor employees performing plan administration functions desire to limit their access to PHI whenever and wherever reasonably possible. As a result, they do not wish to have an active role in responding to restriction requests, to the extent the requests pertain to information held by a third party administrator. In other words, they do not wish to be "in the middle" of such requests, and thus potentially receive more PHI than they otherwise would or need to receive.
4. Nevertheless, those plan sponsor employees will take reasonable steps to ensure that a third party administrator does not grant any request for a restriction on the use or disclosure of PHI that it is not in a position to subsequently honor.
5. A plan will take steps to coordinate requests for restrictions with a third party administrator, to ensure that the administrator considers the uses and disclosures of PHI made by plan sponsor employees who perform plan administration functions in the context of the restriction request. Otherwise, the plan will need to take steps to ensure that it directly responds to such requests, as it concerns the uses and disclosures of PHI made by such plan sponsor employees.
6. The remainder of this Procedure provides guidance in the event that a plan must directly respond to a restriction request, with respect to the uses and disclosures of PHI made by those plan sponsor employees who perform plan administration functions.
7. A plan must permit an enrollee/personal representative to request that the plan restrict:

   A. uses or disclosures of PHI to carry out treatment, payment or health care operations;

   disclosures to:

   i. A family member, other relative, or a close personal friend, of PHI directly relevant to such person's involvement with the enrollee's care or payment related to the enrollee's care;

ii. A family member, a personal representative of the enrollee, or another person responsible for the care of the enrollee, of PHI, for notification purposes.

8. A plan informs all enrollees/personal representatives of their right to request restrictions on the use and disclosure of PHI in the Notice of Privacy Practices.

9. **A plan is not required to agree to any requested restriction.** As a matter of course, the plan will **not** grant any requested restriction, because of the administrative difficulties in tracking and subsequently honoring a request. However, an enrollee/personal representative is free to make any desired request.

10. Workforce members or business associates may not grant a request for restrictions without prior authorization from the Privacy Official. Each plan has trained its workforce to this effect, and so instructed its business associates (where necessary).

11. If a plan agrees to a restriction, it may not use or disclose PHI in violation of the restriction, except that, if the enrollee/personal representative who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the plan may disclose such PHI to a health care provider, to provide such treatment. If restricted PHI is disclosed to a health care provider for emergency treatment, the plan must request that such health care provider not further use or disclose the information.

12. If the Privacy Official grants a request:

    A. The enrollee/personal representative will be notified of any potential consequences of the restriction.

    B. A notation will be made in the enrollee's record.

    C. A plan will not use or disclose PHI inconsistent with the agreed restriction, nor will the plan's business associates.

    D. The enrollee/personal representative will be informed that the plan is not required to comply with the agreed restriction in emergency treatment situations when the restricted PHI is necessary for treatment (in that event, the plan will request that any health care provider to whom it discloses the restricted PHI not further use or disclose the information).

    E. If the agreed upon restriction hampers treatment, the plan will ask the enrollee/personal representative to modify or revoke the restriction and get written agreement to the modification or revocation or document an oral agreement.

13. A restriction may be terminated:

    A. If the enrollee/personal representative agrees to or requests the termination in writing.

B. The enrollee/personal representative orally agrees to the termination and the oral agreement is documented.

C. A plan notifies the enrollee/personal representative that it is terminating the restriction, except that the termination is only effective with respect to PHI created or received after it has so informed the enrollee/personal representative.

14. A restriction agreed to by a plan is not effective to prevent uses or disclosures permitted or required under 45 CFR 164.502(a)(2)(ii) (i.e., disclosures to the Secretary of the Department of Health and Human Services for compliance reviews), or 45 CFR 164.512.

15. A plan will document any agreed restriction in either electronic or written form and retain such documentation for a period of six (6) years from the date of its creation or when it last was in effect, whichever is later.

16. If the Privacy Official denies a request, then the enrollee/personal representative will be given the opportunity to discuss his or her privacy concerns, if desired.

POLICY AND PROCEDURE: Confidential Communications

Privacy Rule Sections: 45 CFR 164.522

Effective Date: April 14, 2004

Policy

Each group health plan will comply with the Privacy Rule provisions regarding confidential communications of PHI.

Procedure

1. Plan sponsor employees who perform plan administration functions do not use or disclose significant amounts of enrollee PHI. A third party administrator will likely use and disclose more PHI.
2. A plan will request that a third party administrator respond to most, if not all, confidential communication requests.
3. As a general rule, plan sponsor employees performing plan administration functions desire to limit their access to PHI whenever and wherever reasonably possible. As a result, they do not wish to have an active role in responding to confidential communication requests, to the extent the requests pertain to information held by a third party administrator. In other words, they do not wish to be "in the middle" of such requests, and thus potentially receive more PHI than they otherwise would or need to receive.
4. Nevertheless, those plan sponsor employees will take reasonable steps to ensure that a third party administrator does not inappropriately deny any confidential communications request by an enrollee/personal representative.
5. A plan will take steps to coordinate requests for confidential communications with a third party administrator, to ensure that the administrator considers the uses and disclosures of PHI made by plan sponsor employees who perform plan administration functions in the context of the confidential communications request. Otherwise, the plan will need to take steps to ensure that it directly responds to such requests, as it concerns the uses and disclosures of PHI made by such plan sponsor employees.
6. The remainder of this Procedure provides guidance in the event that a plan must directly respond to a confidential communications request, with respect to the uses and disclosures of PHI made by those plan sponsor employees who perform plan administration functions.
7. A plan must permit an enrollee/personal representative to request and must accommodate a reasonable request by an enrollee/personal representative to receive communications of PHI from the plan by alternative means or at alternative locations, if the enrollee/personal representative clearly states that disclosure of all or part of that PHI could endanger the enrollee/personal representative.

8. A plan requires an enrollee/personal representative who makes such a request, to do so in writing, and to specify the alternative location or other method of communication. The plan may also require that the written request contain a statement that disclosure of all or part of the PHI to which the request pertains could endanger the enrollee.

9. A plan may condition the provision of a reasonable accommodation on the following:

A. When appropriate, information as to how payment, if any, will be handled; and

B. Specification of an alternative address or other method of contact.

10. Based upon the foregoing, a plan will grant all such requests for confidential communications, unless a request imposes an unreasonable administrative burden (in that event, the request will be reviewed with the Privacy Official before any denial of the request is communicated to the enrollee/personal representative). The plan understands that a purpose of this Privacy Rule provision is to enable persons who are subject to abuse to potentially avoid that abuse. Consequently, a request will rarely be denied.

11. A plan will place written documentation of a request, whether granted or refused, in the enrollee's file, along with any other documentation associated with the request (e.g., any correspondence to the enrollee/personal representative communicating the decision on the request).

12. If a request is granted, a plan will inform all staff of the new communication requirement, and that they must adhere to the requirement.

POLICY AND PROCEDURE: Decedents

Privacy Rule Sections: 45 CFR 164.502(f) and (g)(4)

Effective Date: April 14, 2004

Policy

Each group health plan will protect the PHI of a deceased enrollee as it did before the enrollee died, and will treat an executor, administrator, or other person with authority to act on behalf of a deceased individual or of the individual's estate, as a personal representative under the Privacy Rule, with respect to the PHI relevant to such personal representation.

Procedure

1. A plan will protect the privacy of a deceased enrollee's PHI, in accordance with the requirements of the Privacy Rule, for as long as the plan maintains the PHI.
2. A person with the express legal authority to act for a decedent or his/her estate, such as an executor or administrator, is a personal representative under the Privacy Rule, with respect to the PHI relevant to such personal representation. Accordingly, a plan will permit such a person to exercise the individual rights made available under the Privacy Rule (e.g., the right to access PHI, the right to amend PHI, and the right to an accounting of disclosures of PHI), on behalf of the decedent, with respect to the PHI that pertains to such personal representation.

POLICY AND PROCEDURE: Marketing

Privacy Rule Sections: 45 CFR 164.501 and 508

Effective Date: April 14, 2004

Policy

Each group health plan does not engage in marketing activities. However, if a plan does pursue such activities in the future, it will obtain a properly completed authorization from an enrollee/personal representative, before pursuing the marketing.

Procedure

1. Each plan has closely examined its activities and it does not engage in any function that would meet the Privacy Rule marketing definition.

2. In the unlikely situation where a plan might engage in marketing, the plan will obtain authorization from an enrollee/personal representative before using or disclosing his/her PHI for marketing, unless the communication at issue takes place during a face-to-face encounter between the plan and an enrollee/personal representative, or involves a promotional gift of nominal value provided by the plan. In addition, the plan will indicate in the authorization whether it receives direct or indirect remuneration from a third party in connection with the marketing.

POLICY AND PROCEDURE: Notice of Privacy Practices

Privacy Rule Sections: 45 CFR 164.520
Effective Date: April 14, 2004

Policy

Each group health plan is obligated to prepare and deliver a Notice of Privacy Practices ("Notice") to its enrollees. The Notice describes how the plan uses and discloses PHI, identifies individual rights under the Privacy Rule, and specifies how an individual may complain of alleged privacy violations to the plan, or to the Department of Health and Human Services.

Procedure

1. By April 14, 2004, a plan will distribute the Notice to all individuals then covered by the plan.
2. Thereafter, at the time of enrollment, the plan will distribute the Notice to individuals who are new enrollees.
3. Within sixty (60) days of a material revision to the Notice, the plan will distribute the revised Notice to individuals then covered by the plan.
4. No less frequently than once every three (3) years, the plan must notify individuals then covered by the plan of the availability of the Notice and how they may obtain a copy.
5. A plan satisfies the requirements of Paragraphs 2, 3 and 4 above by delivering the Notice to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.
6. A plan will provide the Notice to anyone who requests a copy, and will make a paper copy of the Notice available, if requested, to any enrollee, even if that enrollee had received the Notice electronically.
7. A plan will address the contents of the Notice with those workforce members who undergo training, in accordance with the Policy and Procedure on Training.
8. A plan will update and revise the Notice to reflect revisions in privacy practices, and will make the revised Notice available in accordance with the requirements of the Privacy Rule.
9. The Privacy Official understands that he/she is obligated to keep a copy of each Notice used by a plan, for six (6) years from the date of creation of the Notice, or the date when it was last in effect, whichever is later.

POLICY AND PROCEDURE: Minimum Necessary Rule

Privacy Rule Sections: 45 CFR 164.502(b) and 514(d)

Effective Date: April 14, 2004

Policy

Each group health plan will make every reasonable effort to only use, disclose and request the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, as required by the Privacy Rule.

Procedure

1. The Privacy Rule is less than clear regarding its regulation of group health plans. One area of confusion exists with respect to those group health plans that have no employees, but rather rely on the services of plan sponsor employees to perform plan administration functions. In this situation, there is some doubt as to whether the minimum necessary rule applies to "uses" of PHI, as there are no employees to actually "use" the PHI.
2. However, Section 164.504(f) would apply in this context, as it concerns the amendment of plan documents (See, Policy and Procedure on Disclosures to Plan Sponsors). One of the amendment requirements is very much akin to the minimum necessary restrictions on the use of PHI (i.e., the requirement of adequate separation). Nevertheless, each plan, for the sake of thoroughness, has created this Policy and Procedure on the minimum necessary rule.
3. The HIPAA minimum necessary rule does not apply to:

    A. Disclosures to or requests by a health care provider for treatment.

    B. Uses or disclosures made to an enrollee (e.g., when exercising rights to access PHI, or to obtain an accounting of disclosures of PHI). For example, if an enrollee requests access to his/her PHI, and a plan is required by the Privacy Rule to provide that access, then the plan cannot limit the amount of PHI it makes available to the enrollee based on a minimum necessary assertion.

    C. Disclosures made to the Secretary of the Department of Heath and Human Services (or his/her designee) in connection with an investigation or compliance review. A plan cannot limit the amount of PHI accessible by the Secretary in the context of an investigation or compliance review, at least not based on a minimum necessary assertion.

    D. Uses or disclosures made pursuant to an authorization. A properly completed authorization identifies the precise PHI that may be used or disclosed. Consequently, there is no need for a minimum necessary analysis.

    E. Uses or disclosures that are compelled by law (e.g., in response to a court order or a state statute).

4. A plan will limit access to PHI to those members of its workforce who need access to carry out their duties. The following table identifies the workforce members who need access to PHI to perform their jobs. The table also describes the specific categories or types of PHI to which those members need access, and the conditions that apply to such access.

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
Office Manager	Enrollment/Disenrollment Advocacy-coverage info; Responding to claims. Payment info.	Whatever is made available to employees.
Administrative Assistant	Enrollment/Disenrollment Advocacy-coverage info; Responding to claims. Payment info.	Whatever is made available to employees.

5. A plan will limit access to PHI to the above-identified workforce members, and to the identified PHI, based on its reasonable determination of the persons or classes of persons who require PHI, and the nature of the information they require, consistent with their job responsibilities.

6. Each plan has attempted to identify below those disclosures of PHI that are subject to the minimum necessary rule, and that the plan makes on a routine and recurring basis. In those situations, the plan will limit its disclosures to only the information needed for the intended purpose of the disclosure, as described below.

Intended Recipient	Purpose of Disclosure	Information Reasonably Necessary to Accomplish Purpose
Blue Cross Blue Shield of Vermont	Enrollment and Disenrollment	Enrollment forms. Pre approved forms. Additions and deletions.

7. A plan will make a minimum necessary determination for non-routine and recurring disclosures of PHI, on a case-by-case basis, in consultation with the Privacy Official. Such non-routine disclosures will be discussed with the Privacy Official to determine if the amount of PHI at issue is the minimum necessary to achieve the purpose of the disclosure, according to established criteria (in short, those criteria require that only the minimum amount of PHI necessary to accomplish the purpose of the disclosure be disclosed).

8. Each plans has attempted to identify below those requests for PHI that are subject to the rule, and that the plan makes on a routine and recurring basis. In those situations, the plan will limit its requests to only the information needed for the intended purpose of the request, as described below.

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
N/A		

9.A plan will make a minimum necessary determination for non-routine and recurring requests for PHI, on a case-by-case basis, in consultation with the Privacy Official. Such non-routine requests will be discussed with the Privacy Official to determine if the amount of PHI at issue is the minimum necessary to achieve the purpose of the request, according to established criteria (in short, those criteria require that only the minimum amount of PHI necessary to accomplish the purpose of the request be requested)..

10.A plan does not envision the need to use, disclose or request an entire medical record for any purpose, and will not do so, unless a specific justification for such a use, disclosure or request is documented by the plan, and approved by the Privacy Official.

POLICY AND PROCEDURE: Training

Privacy Rule Sections: 45 CFR 164.530(b)

Effective Date: April 14, 2004

Policy

Each group health plan will require that all of its workforce members who have access to PHI receive the training required by the Privacy Rule.

Procedure

1. Each plan has trained, and will continue to train, all workforce members, as is necessary and appropriate for such members to carry out their duties and responsibilities, in the proper use and disclosure of PHI and the Privacy Policies and Procedures implemented by the plan.
2. A plan will require that all new workforce members undergo privacy training within a reasonable time after beginning work with the plan. These persons will receive such training as part of their new employee orientation.
3. All workforce members who change positions will receive new privacy training (as necessary and appropriate for such new job duties and responsibilities) at or about the time of the change.
4. Training will be provided to all workforce members whose job duties and responsibilities are affected by a material change in the Policies or Procedures, within a reasonable period of time after the material change becomes effective.
5. The Privacy Official or his/her designee will conduct all privacy training.
6. A plan will keep records to confirm that its workforce members received training, and will keep copies of the training materials used. This documentation must be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

POLICY AND PROCEDURE: Sanctions

Privacy Rule Sections: 45 CFR 164.530(e)

Effective Date: April 14, 2004

Policy

Each group health plan applies appropriate sanctions against any workforce member who violates its privacy practices or the Privacy Rule. Each plan will follow a sanction policy that is fair, and that is consistent with the requirements of any existing labor contracts.

Procedure

1. A plan must have and apply appropriate sanctions against members of its workforce who fail to comply with its Privacy Rule Policies and Procedures or the requirements of the Privacy Rule.
2. A plan trains, and will continue to train, its workforce members, to reasonably ensure such members understand and comply with applicable Privacy Rule Policies and Procedures.
3. Appropriate sanctions are determined based on the nature of a violation, its severity, whether it was intentional or unintentional, whether it indicates a pattern of improper access, use or disclosure of PHI, and other, similar factors.
4. In all cases, sanctions will be determined after review of pertinent facts and consideration by relevant management, in consultation with the Privacy Official.
5. A plan will inform a workforce member suspected of having violated a Privacy Rule Policy or Procedure, or the Privacy Rule, that certain violations may result in notification to law enforcement officials as well as regulatory, accreditation, and licensure organizations.
6. Sanctions may include verbal warnings, written warnings, probationary periods or termination of employment.
7. A plan will document the sanctions it applies, if any, and retain such documentation for six (6) years from the date of their creation or when they were last in effect, whichever is later.
8. This Policy and Procedure does not apply to a workforce member with respect to actions that are covered by and that meet the following conditions:

    A. The workforce member believes in good faith that a plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by a plan potentially endangers one or more patients, workers, or the public, and the workforce member discloses PHI to:

        i. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the plan;

ii. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the plan; or

iii. An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the workforce member with regard to the foregoing conduct;

B. The workforce member, who is the victim of a criminal act, discloses PHI to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the criminal act, and is limited to the information listed in 45 CFR 164.512(f)(2)(i);

C. The workforce member:

i. Filed a compliant with the Secretary of the Department of Health and Human Services with respect to a Privacy Rule issue;

Testified, assisted, or participated in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

Opposed any act or practice made unlawful by the Privacy Rule, provided the workforce member has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Rule.

POLICY AND PROCEDURE: Complaints

Privacy Rule Sections: 45 CFR 164.530(d)

Effective Date: April 14, 2004

Policy

Each group health plan must provide a process for persons to make complaints about these Policies and Procedures, compliance with the Policies and Procedures, and compliance with the Privacy Rule. Each plan will promptly and fairly respond to all complaints.

Procedure

1. A plan must provide a process for individuals to make complaints concerning its Policies and Procedures, compliance with such Policies and Procedures, and the requirements of the Privacy Rule.

2. A plan must designate a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the Notice of Privacy Practices. A plan must document this personnel designation, and retain such documentation, for at least six (6) years from the date of its creation, or the date when it was last in effect, whichever is later. The Privacy Official is the designated contact for persons to file such complaints (and to respond to any inquiries regarding the Notice of Privacy Practices).

3. A plan will receive and review complaints about any aspect of its privacy practices.

4. A plan will implement the following process upon receipt of a complaint:

   A. The Privacy Official will investigate the complaint, directly or by designating the conduct of the investigation to an appropriate person, which will in all cases be a person who had no involvement in the facts surrounding the complaint, and is not in the direct chain of management of any person alleged to have committed any wrongdoing.

   B. In the course of the investigation, the Privacy Official/designee will conduct any interviews and review any documentation that he/she believes necessary to ensure a full understanding of all relevant facts.

   C. The Privacy Official/designee will review the results of the investigation with counsel, and will work with counsel to document the results of the investigation, and any appropriate follow-up (e.g., any necessary discipline).

   D. The Privacy Official/designee will discuss the outcome of the investigation with the individual who made the complaint.

5. In all cases, a plan will endeavor to complete the investigation of a complaint in an expeditious manner.

6. A plan will not require individuals to waive any rights to file a complaint with the plan or the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

7. A plan will document all complaints received, and their disposition, if any. The plan will retain such documentation for at least six (6) years from the date of their creation, or the date when they were last in effect, whichever is later.

POLICY AND PROCEDURE: Administrative Requirements

Privacy Rule Sections: 45 CFR 164.530

Effective Date: April 14, 2004

Policy

Each group health plan will comply with all administrative requirements imposed by the Privacy Rule.

Procedure

1. The Privacy Official is responsible for the development and implementation of these Policies and Procedures.
2. Each plan has implemented, and will continue to implement, reasonable administrative, technical and physical safeguards to protect the privacy of PHI, and to limit incidental uses or disclosures of PHI made pursuant to otherwise permitted uses and disclosures. By way of example, but not limitation, each plan has implemented the following safeguards:

   A. Administrative Safeguards: Compliance with these Policies and Procedures.
   B. Technical Safeguards: We don't send information via E Mail. Fax transmittal sheets have a disclaimer on them.
   C. Physical Safeguards: Locked file cabinets.

3. A plan advises its workforce members that violations of these Policies and Procedures must be brought to the attention of the Privacy Official. A plan will also commit its business associates to report violations of business associate contracts to the plan. The Privacy Official will require that all alleged violations are investigated, and if valid, the plan will seek to mitigate the effects of such violations.
4. A plan will not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual for exercising any right under, or participating in any process established by, the Privacy Rule, including the filing of a complaint with the plan.
5. A plan will not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual or other person for:

   A. Filing a complaint with the Secretary of the Department of Health and Human Services;

   B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

   C. Opposing any act or practice made unlawful by the Privacy Rule, provided the individual or other person has a good faith belief that the act or practice

opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Rule.

6.A plan does not violate the Privacy Rule if a member of its workforce or a business associate discloses PHI, provided that the workforce member or business associate believes in good faith that the plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the plan potentially endangers one or more patients, workers or the public; and

A. The disclosure is made:

i. To a health oversight agency or public health authority authorized by law to investigate or oversee the relevant conduct or conditions of the plan;

ii. To an appropriate health care accreditation organization to report the alleged failure to meet professional standards or misconduct by the plan; or

iii. To an attorney retained by or on behalf of the workforce member or business associate to determine the legal options of the workforce member or business associate with regard to the conduct described above.

B. A plan does not violate the Privacy Rule if a workforce member who is the victim of a criminal act discloses PHI to a law enforcement official, provided that:

The PHI disclosed is about the suspected perpetrator of the criminal act; and

The PHI disclosed is limited to:

A.Name and address;

B.Date and place of birth;

C.Social security number;

D.ABO blood type and RH factor;

E.Type of injury;

F.Date/time of treatment;

G.Date/time of death (if applicable); and

H.A description of distinguishing physical characteristics including weight, height, gender, race, hair or eye color, presence or absence of facial hair, and scars or tattoos.

7. A plan will communicate, through training and otherwise, that it will not, and cannot, require enrollees to waive any rights available to them under the Privacy Rule.
8. Each plan has prepared and implemented Policies and Procedures to comply with the Privacy Rule.
9. The Notice of Privacy Practices ("Notice") includes a statement reserving the right to make changes in privacy practices. Thus, such changes will apply to all PHI created or received by a plan, including PHI created or received before the effective date of the change to the Notice.

10. The Privacy Official will work closely with counsel to ensure that changes in law are evaluated to determine whether they necessitate changes to any Policy, Procedure, or the Notice. A plan will require review from counsel before any changes are made to its Policies, Procedures, or Notice.

11. The Privacy Official is responsible for ensuring that all documentation required by the Privacy Rule is maintained in accordance with the Privacy Rule requirements (i.e., for six (6) years from the date of creation or the date when last in effect, whichever is later).

POLICY AND PROCEDURE: De-Identified Information

Privacy Rule Sections: 45 CFR 164.514(a), (b) and (c)

Effective Date: April 14, 2004

Policy

Each group health plan will use and disclose de-identified information, wherever reasonably possible.

Procedure

1. A plan may determine that health information is not individually identifiable health information if:

   A. The following identifiers of an enrollee, or of relatives, employers or household members of the enrollee have been removed:

      i. Names;

      ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geo codes, except for the initial 3 digits of a zip code if, according to current publicly available data from the Bureau of the Census:

         A. The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people; and

         B. The initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to "000".

      iii. All elements of dates (except year) related to an individual including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of date indicative of such age (including year), except that such ages and elements may be aggregated into a single category of age 90 or older;

      iv. Telephone numbers;

      v. Fax numbers;

      vi. E-mail addresses;

      vii. Social security numbers;

      viii. Medical record numbers;

      ix. Health plan beneficiary numbers;

x. Account numbers;

xi. Certificate/license numbers;

xii. Vehicle identifiers and serial numbers (including license plate numbers);

xiii. Device identifiers and serial numbers;

xiv. Web Universal Resource Locators (URLs);

xv. Internal Protocol (IP) address numbers;

xvi. Biometric identifiers, including finger/voice prints;

xvii. Full face photographic images and any comparable images; and

xviii. Any other unique identifying number, characteristic or code (except as permitted below).

AND

B. The plan does not have actual knowledge that the information could be used alone or in combination with other information to identify an enrollee who is the subject of the information.

2. A plan may assign a code or other means of record identification to allow information de-identified to be re-identified, provided that:

A. The code or other means of record identification is not derived from or related to information about the enrollee and cannot be translated to identify the enrollee; and

B. The plan does not use or disclose the code or other means of record identification for any other purpose, and do not disclose the mechanism for re-identification.

3. A plan will seek to use and/or disclose de-identified information where it is reasonable to do so.

POLICY AND PROCEDURE: Personal Representatives

Privacy Rule Sections: 45 CFR 164.502(g)

Effective Date: April 14, 2004

Policy

Each group health plan will treat personal representatives as "individuals," where required by the Privacy Rule.

Procedure

1. A personal representative generally has the authority to exercise all of the rights and benefits that are made available under the Privacy Rule and these Policies and Procedures, in those situations where the representative has the authority to act on behalf of the enrollee with respect to a health care issue. For example, the personal representative could:

   A. Request access to PHI.

   B. Request amendment to PHI.

   C. Request an accounting of disclosures of PHI.

   D. Request restrictions on the use and disclosure of PHI.

   E. Request confidential communications of PHI.

   Sign (or not sign) an authorization.

2. A plan must treat a person who is authorized under applicable law to make decisions relating to health care on behalf of an enrollee who is an adult or an emancipated minor, as a personal representative of the enrollee, with respect to the PHI relevant to such representation. In this context, a guardian or a person with a durable power of attorney for health care could be such a personal representative. In the event an enrollee who is less than 18 years of age asserts that he/she is "emancipated", the issue will be reviewed with the Privacy Official. In Vermont, certain requirements must be satisfied before such emancipation exists (See, 12 VSA 7151).
3. A plan must treat a parent, guardian or other person acting in *loco parentis* as a personal representative of an enrollee who is an unemancipated minor, with respect to PHI relevant to such representation, if the parent, guardian or other person acting *in loco parentis* has authority under applicable law to act on behalf of such unemancipated minor in making decisions related to health care.

4. However, an unemancipated minor has the authority to exercise rights under the Privacy Rule, with respect to PHI pertaining to a health care service, if:
   A. Circumstance A
      i. The minor consents to such health care service.

ii. No other consent for such health care service is required by law (regardless of whether the consent of another person has also been obtained).

iii. The minor has not requested that a parent, guardian or other person acting in *loco parentis* be treated as the personal representative.

B. Circumstance B

i. The minor may lawfully obtain such health care service without the consent of a parent, guardian or other person acting in *loco parentis.*

ii. The minor, a court or other person authorized by law consents to such service.

C. Circumstance C

i.A parent, guardian or other person acting in *loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

5. Generally, an un-emancipated minor can exercise the rights made available by the Privacy Rule where some law (state, federal or case law) permits the minor to consent to the health care service, without parental permission. Some examples of such laws are:

A. 18 VSA 4226, *Minors; consent; treatment*, which permits minors age 12 or older to consent to treatment for drug or alcohol dependency, or venereal disease, without parental permission.

B. 18 VSA 7503, *Application for Voluntary Admission*, which permits minors age 14 or older to apply for admission to a designated hospital for mental health examination or treatment.

C. Minors have a constitutional right to confidential abortion services. See, *Planned Parenthood v. Danforth*, 428 U.S. 52 (1976); *Bellotti v. Baird*, 443 U.S. 622 (1979).

D. Minors have a constitutional right to privacy, including the right to make reproductive health care decisions. See, *Planned Parenthood v. Danforth*, 428 U.S. 52 (1976). This right includes the right to non-prescription contraceptives. See, *Carey v. Population Services Int'l*, 431 US 678 (1977) and may include the right to consent to prescription contraceptives. See, *Planned Parenthood v. Matheson*, 582 F. Supp. 1001 (D. Utah 1983).

E. Courts have interpreted the Public Health Service Act and the Medicaid law to require the provision of confidential contraceptive services to teens. See, 42 USC §300(a); 42 USC §1396d (a)(4)(C). Thus, when providers offer contraceptives to Medicaid patients or through programs funded by the Public Service Act, they may not require parental consent or notification. See, e.g., *PPFA v. Heckler*, 712 F. 2d 650 (2d Cir. 1983); *Planned Parenthood of Utah v. Dandoy*, 810 F2d 984 (10th Cir. 1987).

Notwithstanding Paragraphs 4 and 5 above, there may be situations where a parent, guardian or other person acting in *loco parentis* is permitted to have access to the PHI of a minor, under Section 164.524 of the Privacy Rule – even where the minor has the authority to act as an "individual" under the Privacy Rule. However, the analysis that must be undertaken is extremely complex, and is based on Section 164.502(g)(3)(ii) of the Privacy Rule. In short:

A. The advice of counsel should be sought in the event a minor seeks to exercise any of the rights made available by the Privacy Rule (e.g., seeks to obtain a copy of his/her PHI); and

B. The advice of counsel should be sought in the event that a parent, guardian or other person acting in *loco parentis* seeks to obtain access to PHI in a situation where the minor had the authority to act as an individual under the Privacy Rule.

7. A plan must treat an executor, administrator, or other person as a personal representative, with respect to PHI relevant to such personal representation, if such person has, under applicable law, the authority to act on behalf of a deceased individual or of the individual's estate.

8. Notwithstanding any state law or Privacy Rule provision to the contrary, a plan may elect not to treat a person as a personal representative of an enrollee if:

A. The plan has a reasonable belief that:

i. The enrollee has been or may be subjected to domestic violence, abuse or neglect by such person; or

ii. Treating such person as the personal representative could endanger the enrollee; and

iii. The plan, in the exercise of professional judgment, decides that it is not in the best interest of the enrollee to treat such person as the personal representative.

9. Relevant personnel will be instructed to review any situation of suspected abuse, neglect or endangerment with the Privacy Official. These situations arise when a person who would otherwise be a personal representative seeks to exercise rights (e.g., the right to access PHI or seek an accounting of disclosures of PHI) under the Privacy Rule and these Policies and Procedures, but there is a suspicion that this person may be abusing, neglecting, or endangering an enrollee.

POLICY AND PROCEDURE: Family and Friends

Privacy Rule Sections: 45 CFR 164.510(b)

Effective Date: April 14, 2004

Policy

Each group health plan understands the situations under which it may disclose PHI to a family member, other relative, close personal friend, or other person identified by an enrollee.

Procedure

1. A plan may disclose to a family member, other relative, or a close personal friend of an enrollee, or any other person identified by the enrollee, the PHI directly relevant to:

   A. Such person's involvement with the enrollee's care; or

   B. Payment related to the enrollee's care.

2. A plan may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the enrollee, or another person responsible for the care of the enrollee, of the enrollee's location, general condition, or death.

3. When an enrollee is present for, or otherwise available prior to, a use or disclosure permitted by Paragraphs 1 or 2, and has the capacity to make health care decisions, a plan may use or disclose PHI if it:

   A. Obtains the enrollee's agreement;

   B. Provides the enrollee with the opportunity to object to the disclosure, and the enrollee does not express an objection; or

   C. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the enrollee does not object to the disclosure.

4. If the enrollee is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the enrollee's incapacity or an emergency circumstance, a plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the enrollee and, if so, disclose only the PHI that is directly relevant to the person's involvement with the enrollee's health care. As a general matter of course, a plan will not disclose any PHI to family members, other relatives, or close personal friends, because the plan does not have all information necessary to determine whether, in any given circumstance, the disclosure would be in the best interests of the enrollee.

5.A plan may use or disclose PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by Paragraph 2.