GOVERNMENT OF THE DISTRICT OF COLUMBIA

D.C. Office of Personnel

This instruction should be filed behind the divider for Part III of DPM Chapter (s) 31A

Personnel Manual Issuance System

DPM Instruction No. 31A-3

SUBJECT: Health Information Privacy Policies and Procedures **Date:** April 14, 2003

1. Purpose

The purpose of this instruction is to inform employees under the personnel authority of the Mayor of the Health Information Privacy Policies and Procedures under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, published at 45 C.F.R. Parts 160 and 164 (Privacy Rules). Under the implementing provisions of the HIPAA, the District government is required to protect the privacy of individually identifiable health information that the health care components of the District government create, receive or maintain in their respective roles as health care provider or as health plan.

2. Authority

The Authority is the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations (45 Code of Federal Regulations Parts 160 and 164) ("Privacy Rules").

3. Applicability

This instruction is applicable to all District government employees. Employees are required to follow the Health Information Privacy Policies and Procedures. Failure to comply with the policy would subject the employee to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements.

4. Definitions

When used in this instruction, the following terms shall have the meaning ascribed:

Act means the Social Security Act.

Agency means any agency or department of the District of Columbia designated as a *health care component* in the District's *hybrid entity* declaration on file in the Privacy Official's office.

***Note**: DPM Instructions that are strictly procedural in nature have direct applicability only to agencies and employees under the personnel authority of the Mayor. Other personnel authorities or independent agencies may adopt any or all of these procedures or guidance materials for agencies and employees under their respective jurisdictions. [See DPM Chapter 2, Part II, Subpart 1, § 1.3.]*

Inquiries: Gerry Roth, Privacy Official, HIPPAA Office, Office of Deputy Mayor for Children, Youth, Families and Elders, 1350 Pennsylvania Ave., NW, Suite 307, Washington, D.C. 20004, (202) 727-8001
Distribution: Heads of Departments and Agencies, HR Advisors, and DPM Subscribers
Retain Until Superseded

***Business associate*:** (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(1) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of the Privacy Rule) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of the Privacy Rule), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated

delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Designated record set means:

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

> (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
>
> (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
>
> (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

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

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (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 (PHS 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:

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

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

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of section §164.504 of the Privacy Rule.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) 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;

(2) 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;

(3) 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 are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) 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

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

> (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
>
> (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
>
> (iii) Resolution of internal grievances;
>
> (iv) 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
>
> (v) Consistent with the applicable requirements of § 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.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health insurance issuer **(**as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. Chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i) – (xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(*1*) The direct provision of health care to persons; or

(*2*) The making of grants to fund the direct provision of health care to persons.

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of section §164.504 of the Privacy Rule.

Individual means the person who is the subject of protected health information.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

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

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

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

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

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

(iii) 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;

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

(v) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

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

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of the Transactions and Code Sets Rule; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

Psychotherapy notes means 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* does not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Researc*h* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

Treatment means 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 means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means 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.

4. Provisions

TABLE OF CONTENTS

I. USE AND DISCLOSURE POLICIES AND PROCEDURES

1. Fundamental Policies on Use and Disclosure of Protected Health Information

a) **POLICY—No Use or Disclosure.** We (as a covered entity) and you (as a member of our workforce) must not use or disclose protected health information except as these Privacy Policies and Procedures permit or require.

b) **Treatment, Payment, Health Care Operations.**

i) **POLICY—Our Activities.** We may use and disclose protected health information, without the individual's permission, for our own treatment activities, our own payment activities and our own health care operations.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Minimum Necessary. You must limit your use of protected health information to the minimum necessary to accomplish our treatment activities. See **Section 26–Standard Procedure for Minimum Necessary Determination**. You are not required to limit the protected health information disclosed to other health care providers for their treatment activities to the minimum necessary.

You must limit your use and disclosure of protected health information to the minimum necessary to accomplish our payment activities and health care operations. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

ii) **POLICY—Another Health Care Provider's Treatment Activities.** We may disclose protected health information, without the individual's permission, for any health care provider's treatment activities.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Verification. You must verify that a person or entity is a health care provider seeking protected health information for treatment of an individual before you may disclose protected health information to that person or entity for treatment. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary the protected health information you may disclose to health care providers for treatment.

iii) **POLICY—Another Covered Entity's or Health Care Provider's Payment Activities.** We may disclose the minimum necessary protected health information, without the individual's permission, for the payment activities of another covered entity or any health care provider.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Verification. You must verify that a person or entity seeking protected health information for a payment activity is a covered entity or a health care provider before you may disclose protected health information to that person or entity. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You must limit the protected health information disclosed to the covered entity or health care provider to the minimum necessary for the payment activity. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

iv) **POLICY—Another Covered Entity's Health Care Operations.** We may disclose the minimum necessary protected health information, without the individual's permission, for the health care operations of another covered entity if:

(1) **Relationship to Individual.** The protected health information to be disclosed pertains to the relationship that both we and the other covered entity have or had with the individual who is the subject of the protected health information; and

(2) **Nature of the Health Care Operations.** The health care operation for which the disclosure is to be made involves one of the following:

a. **Quality Assurance.**

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines; or
- Population–based activities relating to improving health or reducing health care costs, protocol development, case management, care coordination, contacting health care providers and patients with information about treatment alternatives; or
- Related functions that do not include treatment.

b. **Competency Assurance.**

- Reviewing the competence or qualifications of health care professionals; or
- Evaluating practitioner, health care provider or health plan performance; or
- Conducting training programs in which health care students, trainees, or practitioners learn under supervision to practice or improve their skills, and training non–health care professionals; or
- Accreditation, certification, licensing, or credentialing activities.

c. **Fraud and Abuse Control.** Health care fraud and abuse detection or compliance.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Verification. You must verify that a person or entity seeking protected health information for a health care operation is a covered entity who has or had a relationship with the individual who is the subject of the protected health information and that the protected health information pertains to that relationship, before you may disclose the protected health information to that person or entity. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You must limit the protected health information disclosed to the covered entity to the minimum necessary for the health care operation. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

v) **POLICY—Organized Health Care Arrangement's Health Care Operations.** When we participate in an organized health care arrangement, we may disclose the minimum necessary protected health information to other covered entity participants in the organized health care arrangement for the health care operations of the organized health care arrangement. See **Section 12–Covered Entity Structures** for information about organized health care arrangements in which we, as a health care provider, may participate.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Organized Health Care Arrangement's Health Care Operations. Before making any disclosure with respect to an organized health care arrangement, you must confirm with our Privacy Official that:

- We participate in the organized health care arrangement; and
- The intended recipient of the protected health information is a covered entity participant in the organized health care arrangement; and
- The protected health information to be disclosed is for a health care operation of the organized health care arrangement.

PROCEDURE—Verification. You must verify that a person or entity seeking protected health information for a health care operation of an organized health care arrangement of which we are a participant is also a covered entity participant in the organized health care arrangement before you may disclose the protected health information to that person or entity. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You must limit the protected health information disclosed to other covered entity participants in one of our organized health care arrangements to the minimum necessary for the health care operation of the organized health care arrangement. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

vi) **POLICY—Fundraising for Our Organization.** We may, without the individual's permission, use and disclose to a business associate or institutionally–related foundation an individual's demographic data (i.e., name, address, age, gender) and dates the individual received health care from us, for the health care operation of raising funds for our own organization, provided:

- We state in our Privacy Practices Notice that we may contact the individual to solicit funds for our organization; and
- We explain in our fundraising materials how the individual may opt out of receiving further fundraising solicitations from us, and we make reasonable efforts to ensure that individuals who opt out no longer receive our fundraising solicitations.

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Fundraising for Our Organization. Our Privacy Official must give prior approval for any use or disclosure of an individual's demographic data and dates of health care obtained from the individual's protected health information for fundraising purposes.

vii) **POLICY—Underwriting and Other Insurance Function Health Care Operations.** We may use and disclose the minimum necessary protected health information for underwriting, premium rating or other activities

relating to creation, renewal or replacement of a contract of health insurance or health benefits, provided that any protected health information we receive for these purposes may not be further used or disclosed, except as required by law, if we do not obtain the contract. We may also use and disclose the minimum necessary protected health information to cede, secure or place a contract for reinsurance of risk for health care claims (including stop-loss and excess loss coverage).

NOTE: Mental health information may only be disclosed pursuant to a joint consent, see Section 23A.

PROCEDURE—Underwriting and Other Insurance Functions. You must not use or disclose protected health information that we received for underwriting, premium rating or other activities relating to creation, renewal or replacement of a contract of health insurance or health benefits unless we obtained the contract. You must consult with our Privacy Official before you use or disclose protected health information we received for underwriting, premium rating or other activities relating to creation, renewal or replacement of a contract for health insurance or health benefits not ultimately placed with us, even if the use or disclosure appears to be required by law.

c) **POLICY—Individual or Personal Representative.** We may disclose protected health information to the individual who is the subject of the protected health information and to that individual's personal representative as relevant to the scope of the representation. See **Section 9–Personal Representatives** for information about personal representative determination and status.

PROCEDURE—Verification. You must verify the identity of an individual and the identity and authority of a personal representative seeking protected health information before you may disclose the protected health information to that individual or personal representative. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary the protected health information you disclose to an individual who is its subject, or to the individual's personal representative.

d) **POLICY—Incidental Use or Disclosure.** We may make the minimum necessary use or disclosure of protected health information that is incidental to an otherwise permitted or required use or disclosure of the protected health information, as long as we:

i) **Minimum Necessary Compliance.** Comply with all minimum necessary limitations applicable to the otherwise permitted or required use or disclosure. See **Section 6–Minimum Necessary** for information on the minimum necessary limitations.

ii) **Information Safeguards.** Implement appropriate administrative, physical, and technical safeguards to preserve the privacy of protected health information from any intentional or unintentional improper use or disclosure. See **Section 21–Data Safeguards** for information about our data safeguard obligations.

iii) **Incidental Use and Disclosure Safeguards.** Implement appropriate administrative, physical, and technical safeguards to limit incidental use or disclosure to reasonable levels.

NOTE: Incidental use and disclosure of mental health information is prohibited under the MHIA, see Section 23A.

PROCEDURE—Incidental Use and Disclosure. You must employ common sense and good judgement when using or disclosing protected health information in conversation, by mail, electronic transmission or any other means, and when recording and storing protected health information in any medium, to ensure that any incidental use or disclosure of the protected health information in connection with an otherwise permitted or required use or disclosure is kept to a reasonable minimum.

2. Informal Permission for Certain Uses and Disclosures.

a) POLICY—Informal Permission for Certain Uses and Disclosures.

i) Persons Involved In Health Care or Payment. We may use with and disclose to an individual's family members, other relatives or close personal friends, and any other person that the individual identifies, the individual's minimum necessary protected health information directly relevant to that person's involvement with the individual's health care or payment related to that health care if we follow all applicable procedures.

ii) Notification of Persons Involved in Health Care. We may use or disclose the minimum necessary protected health information to notify or assist in notifying (including identifying and locating) an individual's family members, personal representatives or other persons responsible for the individual's health care, of the individual's location, general condition or death if we follow all applicable procedures.

iii) Notification for Disaster Relief. We may use with and disclose to a public or private entity, authorized by law or charter to assist in disaster relief, the minimum necessary protected health information to coordinate notifying (including identifying or locating) an individual's family members, personal representatives or other persons responsible for the individual's health care, of the individual's location, general condition or death. We must follow all applicable procedures unless we determine, in our professional judgment that following the applicable procedures will interfere with the public or private entity's ability to respond to the emergency circumstances.

FORM—Informal Permission. Use FORM 1–Family or Notification Disclosure to document the individual's informal permission for uses with and disclosures to family members, other relatives or close personal friends, and any other person that the individual identifies.

PROCEDURE—Individual Present to Receive Advance Notice. Before you may use or disclose the minimum necessary protected health information of an individual who is present or available and has the capacity to make health care decisions, you must inform the individual of your intent to use the individual's protected health information with or disclose it to a person involved in the individual's health care or payment related to that health care. You may make the use or disclosure if:

- The individual agrees; or
- The individual does not object after a reasonable opportunity to do so; or

- You infer from the situation that, in your professional judgment, the individual does not object.

You must comply with any restriction or prohibition the individual imposes. You may inform the individual orally, and the individual's response may be oral. You do not need to have the individual sign an acknowledgment or other writing. You must complete FORM 1–Family or Notification Disclosure. Include the completed FORM 1 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Verification You may rely on your professional judgment to verify the identity and authority of any person who is not known to you when disclosing protected health information to persons involved in an individual's health care, payment related to that health care, or disaster relief. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You must limit the protected health information disclosed to persons involved in an individual's health care, payment related to that health care or disaster relief to the minimum necessary directly relevant to the person's involvement or the disaster situation. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

PROCEDURE—Individual Not Present or Emergency. When (a) the individual is absent, unavailable, incapacitated or dead, or (b) there is an emergency making advance notice and the opportunity for the individual to restrict or object impractical, you may use the individual's protected health information with and disclose it to persons involved with the individual's health care (but not persons involved only with payment related to that health care) or disaster relief if you determine, in your professional judgment, that the use or disclosure will be in the individual's best interest. You may use or disclose only the minimum necessary protected health information directly relevant to the person's involvement with the individual's health care or disaster relief. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

You must document on FORM 1–Family or Notification Disclosure the reason that:

- Giving the individual advance notice was impractical; and
- The use or disclosure was in the individual's best interest; and
- The protected health information used or disclosed was the minimum necessary directly relevant to the person's involvement in the individual's health care or disaster relief.

Included the completed FORM 1 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Verification. You may rely on your professional judgment to verify the identity and authority of any person, not known to you, when disclosing protected health information to persons involved in an individual's health care or for disaster relief. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Prescriptions, Medical Supplies, and X–Rays. You may use professional judgment and your experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on the individual's behalf to pick up filled prescriptions, medical supplies, X–rays, or other similar forms of protected health information.

PROCEDURE—Verification. You may rely on your professional judgment to verify the identity and authority of any person, not known to you, in allowing a person to act on the individual's behalf to pick up filled prescriptions, medical supplies, X–rays, or other similar forms of protected health information. See **Section 25–Standard Procedure for Identity and Authority Verification** for our procedures for verifying identity and authority.

PROCEDURE—Minimum Necessary. You must limit to the minimum necessary the protected health information disclosed in delivering filled prescriptions, medical supplies, X–rays, or other similar items. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

b) **POLICY—Facility Directories.** We may use for our facility directories the minimum necessary components of an individual's name, condition (described to not communicate specific medical information), religious affiliation, and location in our facility. We may disclose this information to clergy and (except for religious affiliation) to persons who ask for the individual by name, if we follow all applicable procedures.

FORM—Facility Directory Disclosure. Use FORM 2–Facility Directory Disclosure to document an individual's informal permission to be listed in our facility directories.

PROCEDURE—Individual Present to Receive Advance Notice. If the individual is present or available, you must inform the individual in advance of our intent to include the permitted portion of the individual's protected health information in our facility directories, and explain that the information may be disclosed to clergy or (except for religious affiliation) to any person asking for the individual by name. You may include the permitted portion of the individual's protected health information in our facility directories and make the allowed disclosures if:

- The individual agrees; or
- The individual does not object after a reasonable opportunity to do so; or

- You infer from the situation that, in your professional judgment, the individual does not object.

You may inform the individual orally. The individual's responses may be oral. You do not need to have the individual sign an acknowledgment or other writing. You must complete FORM 2–Facility Directory Disclosure. Include it in the individual's records, and send a copy to our Privacy Official. You must comply with any restriction or prohibition the individual imposes.

PROCEDURE—Minimum Necessary. You must limit to the minimum necessary our uses and disclosures of protected health information in connection with our facility directories. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

PROCEDURE—Individual Incapacitated or Emergency. If the individual is incapacitated or in an emergency treatment circumstance, you may include the individual's minimum necessary protected health information in our facility directories and disclose that information to clergy and (except for religious affiliation) to persons asking for the individual by name if you determine, in your professional judgment, that such use and disclosure is in the individual's best interest and is consistent with any prior expressed preference by the individual known to us.

You must, as soon as practical after the incapacity or emergency ends, inform the individual of the use and disclosure of the individual's protected health information for our facility directories, and provide the individual the opportunity to restrict or prohibit its further use or disclosure for our facility directories.

You must document on FORM 2–Facility Directory Disclosure:

- The incapacity or emergency making advance notice to the individual impractical; and

- The reasons that the use and disclosure was in the individual's best interest; and

- The reasons that the protected health information used or disclosed was the minimum necessary for the purposes of our facility directories.

Include completed FORM 2–Facility Directory Disclosure in the individual's records, and send a copy to our Privacy Official.

PROCEDURE—Minimum Necessary. You must limit to the minimum necessary our uses and disclosures of protected health information in connection with our facility directories. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

c) **POLICY—Documentation.** We will document on paper or electronically our compliance with the Privacy Policies and Procedures of this **Section 2**.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official all documentation you create or receive with respect to our compliance with this **Section 2**. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

3. Authorization for Use or Disclosure.

a) **POLICY—Authorization.** We must have written authorization from the individual (or the individual's personal representative) before we may use or disclose an individual's protected health information for any purpose, except for the following:

- For treatment, payment or health care operations. See **Section 1(b)–Treatment, Payment, Health Care Operations**.
- To the individual, the individual's personal representative or HHS. See **Section 1(c)–Individual or Personal Representative** and **Section 5–Required Disclosures**.
- Pursuant to the individual's informal permission. See **Section 2–Informal Permission for Certain Uses and Disclosures**.
- As permitted for public interest or benefit activities. See **Section 4–Public Interest or Benefit Use and Disclosure**.
- As permitted with a business associate. See **Section 10–Business Associate**.
- Incidental to otherwise permitted or required uses and disclosures. See **Section 1(d)–Incidental Use or Disclosure**.

We are allowed, but not required, to make any use or disclosure of an individual's protected health information that the individual permits in a valid authorization. We must always act in strict accordance with an authorization that is the basis for a use or disclosure we make of protected health information. We may not rely on an authorization we know has been revoked or has expired.

FORMS—Authorization. Use the authorization form appropriate for the particular purpose for which permission to use or disclose protected health information is sought.

- **FORM–Authorization.** Use FORM 3-Authorization for any unconditioned authorization (including to use or disclose psychotherapy notes) that is not for marketing.

- **FORM–Marketing Authorization.** Use FORM 4-Marketing Authorization for an unconditioned authorization to use or disclose protected health information for marketing communications.

- **FORM-Conditioned Authorization for Research with Treatment.** Use FORM 5-Conditioned Authorization for Research with Treatment for an authorization that conditions provision of health care to an individual in connection with research on the individual's permission to use or disclose protected health information obtained for research.

- **FORM-Conditioned Authorization for Disclosure to Third Party.** Use FORM 6-Conditioned Authorization for Disclosure to Third Party for an authorization that conditions provision of health care to an individual solely for the purpose of creating protected health information for a third party (such as a life insurance company) on the individual's permission to disclose the protected health information to be generated by the health care to the third party.

- **[RESERVED—FORM 7–Conditioned Authorization for Enrollment or Eligibility]**

PROCEDURE—Obtaining Authorization. Our Privacy Official must approve your use or disclosure of an individual's protected health information pursuant to an authorization. Whenever you seek, or an individual directs, use or disclosure of the individual's protected health information for which authorization is required, you must:

- Select the appropriate authorization form for the purpose.

- Fill in, or have the individual (or the individual's personal representative) fill in, completely the authorization form. It is sufficient to check the statement, "At the request of the individual" (or the individual's personal representative), for the purpose when the authorization is initiated by the individual (or the individual's personal representative). It is sufficient to state, for the expiration date or event, "end of the research study" or "none" if appropriate for an authorization for use and disclosure of protected health information for research, including for the creation and maintenance of a research database or repository.

- Have the individual (or the individual's personal representative) read, sign, and date the completed authorization form. (An authorization that is incomplete, that you know contains false information, or that is not signed and dated is invalid.) If the authorization form is signed by the individual's personal representative, be sure that it shows the personal representative's name and the relationship that gives the personal representative authority to act on the individual's behalf.

- Give the individual (or the personal representative) a copy of the signed authorization form. Include the signed authorization in the individual's records. Send a copy to our Privacy Official.

FORM—Identity and Authority Verification. Use FORM 9-Identity and Authority Verification to document how you verify identity and authority of a person giving authorization.

PROCEDURE—Verification. You must verify the identity of the individual (and the identity and authority of a personal representative) who provides an authorization. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit the protected health information used or disclosed pursuant to an authorization to the minimum necessary, though you are confined to using and disclosing only the protected health information identified by the authorization.

b) **POLICY—Marketing.** We must obtain written authorization before we may use or disclose an individual's protected health information for any marketing communication, except:

- Marketing communications that we make face–to–face with the individual; and

- Marketing communications that involve promotional gifts of nominal value.

PROCEDURE—Obtaining Marketing Authorization. Our Privacy Official must approve a request for authorization to use or disclose protected health information for marketing before you may ask an individual for such authorization. Use FORM 4-Marketing Authorization and follow the procedures for obtaining authorization above.

c) **POLICY—Fundraising for Others.** We must obtain written authorization before we may use or disclose protected health information to raise funds for any organization, other than our own organization. Compare **Section 1(b)(vi)–Fundraising for Our Organization**.

PROCEDURE—Obtaining Fundraising Authorization. Our Privacy Official must approve a request for authorization to use or disclose protected health information for fundraising for others before you may ask an individual for such authorization. Use FORM 3-Authorization and follow the procedures for obtaining authorization above.

d) **POLICY—Psychotherapy Notes.** We must obtain written authorization before we may use or disclose psychotherapy notes, except:

- We may use psychotherapy notes for treatment if we originated them.

- We may use and disclose psychotherapy notes to defend ourselves in legal proceedings brought by the individual.
- We may use and disclose psychotherapy notes to avert a serious and imminent threat to public health or safety.
- We may use and disclose psychotherapy notes that we originated for our own training programs of mental health practitioners who learn under supervision to practice or improve their skills in group, joint, family or individual counseling.
- We may use and disclose psychotherapy notes for lawful oversight of their originator by a health oversight agency.
- We may use and disclose psychotherapy notes for the lawful activities of a coroner or medical examiner.
- We may use and disclose psychotherapy notes to the extent required by law.
- We may disclose psychotherapy notes to HHS as required for investigation, enforcement or review of our compliance with the HIPAA Administrative Simplification Rules.

NOTE: The MHIA is more restrictive with regard to psychotherapy notes, see Section 23A.

PROCEDURE—Obtaining Authorization for Psychotherapy Notes. Our Privacy Official must approve a request for authorization to use or disclose psychotherapy notes before you may ask an individual for such an authorization. Use FORM 3-Authorization and follow the procedures for obtaining authorization above. You may combine multiple authorizations for use and disclosure of psychotherapy notes in a single authorization form, but you must not combine an authorization for use and disclosure of psychotherapy notes with authorizations for any other purpose.

e) POLICY—Conditioned Authorization. We may not condition treatment on an individual providing an authorization or health plan enrollment or benefits eligibility, except in the following situations:

i) Research Including Treatment. We may condition treatment related to research on the individual providing an authorization to allow the use and disclosure of the individual's protected health information for the research. We may combine an authorization for use and disclosure of protected health information for research with informed consent or any other type of written permission pertaining to the same research.

ii) Protected Health Information for Third Party. We may condition the provision of health care solely for the purpose of creating protected health

information for a third party (for example, a life insurance physical examination) on the individual providing authorization to allow disclosure of that protected health information to the third party.

iii) **Enrollment and Eligibility.** We may condition an individual's enrollment in our health plans or eligibility for benefits on the individual providing authorization (other than for psychotherapy notes) before we enroll the individual to allow us to use or disclose protected health information to determine the individual's eligibility for enrollment or benefits or for our underwriting or risk rating of the individual.

PROCEDURE—Obtaining Conditioned Authorization. Our Privacy Official must approve a request for a conditioned authorization before you may ask an individual for such an authorization. Use FORM 5-Conditioned Authorization for Research with Treatment, FORM 6-Conditioned Authorization for Disclosure to Third Party, or FORM 7-Conditioned Authorization for Enrollment and Eligibility, as appropriate, and follow the procedures for obtaining authorization above. A conditioned authorization must not be combined with any other authorization.

f) **POLICY—Combined Authorizations.** We may combine multiple authorizations for an individual's protected health information on a single authorization form, except:

- We may not combine a conditioned authorization with any other authorization.
- We may not combine an authorization for psychotherapy notes with an authorization for any other purpose.

NOTE: The MHIA is more restrictive with regard to psychotherapy notes, see Section 23A.

PROCEDURE—Combining Authorizations. Using the procedure for obtaining authorization above, you may combine authorizations for a variety of purposes, other than marketing, on FORM 3-Authorization, and you may combine authorizations for different kinds of marketing communications on FORM 4-Marketing Authorization, as long as none of these combined authorizations is conditioned or is for psychotherapy notes.

You must not combine a conditioned authorization that uses FORM 5-Conditioned Authorization for Research with Treatment, FORM 6-Conditioned Authorization for Disclosure to Third Party, or FORM 7-Conditioned Authorization for Enrollment and Eligibility, with any other authorization. You must not combine an authorization for psychotherapy notes using FORM 3-Authorization with an authorization for any purpose other than additional psychotherapy notes.

g) **POLICY—Authorization Received from Another.** We are allowed, but not required, to make any use or disclosure of an individual's protected health information that the individual permits in a valid authorization that is presented to us.

PROCEDURE—Authorization Received from Another. Upon receipt of an authorization to use or disclose protected health information, forward a copy to our Privacy Official and include the original for the individual's records. Our Privacy Official will inform you whether the authorization is valid and may be complied with. If our Privacy Official approves compliance with the authorization, you must comply strictly with its terms, using or disclosing only the protected health information designated by the authorization, only with the persons or entities identified by the authorization, and only for the purposes stated in the authorization.

PROCEDURE—Verification. You must verify the identity of a person or entity as one that the authorization allows to receive and use the protected health information before you may disclose it to that person or entity. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit the protected health information used or disclosed pursuant to an authorization to the minimum necessary, though you are confined to using and disclosing only the protected health information identified by the authorization.

h) **POLICY—Authorization Revocation or Expiration.** We may not rely on an authorization we know has been revoked or has expired. An individual may revoke authorization at any time. Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation.

FORM—Authorization Revocation. Use FORM 8-Authorization Revocation to confirm an individual's revocation of a previously given authorization.

PROCEDURE—Authorization Revocation or Expiration. You must confirm that an authorization has not expired or been revoked before you may use or disclose protected health information pursuant to the authorization.

PROCEDURE—Revocation. If an individual (or the individual's personal representative) who has given authorization indicates a desire to revoke it, document the revocation as follows:

- Fill in, or have the individual (or the individual's personal representative) fill in, FORM 8–Authorization Revocation.
- Have the individual (or the individual's personal representative) sign and date the completed FORM 8. If the form is signed by the individual's personal representative, be sure that it shows the personal representative's

name and the relationship that gives the personal representative authority to act on the individual's behalf.

- Give the individual (or the personal representative) a copy of the completed and signed FORM 8.

- Attach the completed and signed FORM 8 on top of the authorization that it revokes, and include them in the individual's records. Send a copy of them to our Privacy Official.

PROCEDURE—Verification. You must verify the identity of the individual (and the identity and authority of a personal representative) revoking authorization. See **Section 25–Standard Procedure for Identity and Authority Verification**.

i) **POLICY—Pre–Compliance Authorizations.** We may continue to use and disclose protected health information we created or received before April 14, 2003 (our Privacy Rules compliance date), pursuant to express legal permission given to us before April 14, 2003 by the individual who is the subject of that protected health information. We do not need to obtain authorization or other new permission from the individual for those uses or disclosures of that protected health information.

PROCEDURE—Pre–Compliance Authorizations. Our Privacy Official must confirm that express legal permission given to us before April 14, 2003 is sufficient to permit you to continue to use or disclose protected health information we created or received before April 14, 2003 in ways that would otherwise require the individual's authorization. Do not use or disclose that protected health information until you receive our Privacy Official's direction either that you may rely on the pre-compliance express legal permission or that authorization is needed. Follow that direction.

If you have protected health information created or received before April 14, 2003 that you want to use or disclose in accordance with express legal permission obtained before April 14, 2003, gather all relevant information, including the documentation evidencing the express legal permission. Submit the information and documentation to our Privacy Official.

PROCEDURE—Verification. You must verify the identity of a person or entity as one that the pre-compliance express legal permission allows to receive and use the protected health information before you may disclose it to that person or entity. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You must limit use and disclosure after April 13, 2003 of protected health information made pursuant to a pre-compliance express legal permission to the minimum necessary for the purpose. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

PROCEDURE—Disclosure Log. You must log each disclosure of protected health information pursuant to pre-compliance express legal permission unless the disclosure is not subject to disclosure accounting. See **Section 16-Disclosure Accounting** for information regarding accountable disclosures, and **Section 27-Standard Procedures for Logging Disclosures for Accounting.**

j) **POLICY—Documentation.** We will retain, on paper or electronically, each signed authorization and each authorization revocation we create or receive until 6 years after the later of their creation or last effective date**.**

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official each authorization and each authorization revocation you create or receive. Our Privacy Official will retain each authorization and authorization revocation until 6 years after the later of their creation or last effective date.

4. Public Interest or Benefit Use and Disclosure.

a) **POLICY—Public Interest or Benefit Use and Disclosure.** We may use or disclose an individual's protected health information for the public health, public interest, public benefit, and law enforcement activities listed in this **Section 4**, without the individual's permission, as long as we follow all applicable procedural requirements.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Public Interest or Benefit Use and Disclosure. Immediately notify our Privacy Official upon receipt of any request, demand or legal process to use or disclose protected health information in connection with any of the activities listed in this **Section 4**. Unless you are confronted by an emergency situation or legal process where delay is impractical, do not use or disclose any protected health information until you get direction from our Privacy Official. Follow their directions fully and faithfully.

PROCEDURE—Emergency or Legal Process. If confronted by an emergency, legal process, or an insistent law enforcement official, and it is not practical to obtain the approval and direction of our Privacy Official before use or disclosure is required, you may use or disclose the minimum necessary protected health information that, in your professional judgment, is needed to ameliorate the emergency or to comply with the process or law enforcement official's demands.

FORM—Identity and Authority Verification. Use FORM 9-Identity and Authority Verification to document how you verify identity and authority of a government representative, law enforcement official or other person seeking use

or disclosure of protected health information for public health, public interest, public benefit or law enforcement activities.

PROCEDURE—Verification. You must verify the identity and authority of the person seeking use or disclosure of protected health information for the public interest or benefit use or disclosure. See **Section 25–Standard Procedure for Identity and Authority Verification**.

FORM—Minimum Necessary Determination. Use FORM 10-Disclosure Log/Minimum Necessary to assist with and document your determination of the minimum necessary use or disclosure.

PROCEDURE—Minimum Necessary. You must determine the minimum necessary protected health information to use or disclose for the particular public health or benefit activity involved. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

FORM—Disclosure Logging. Use FORM 10-Disclosure Log/Minimum Necessary to log each disclosure for accounting.

PROCEDURE—Disclosure Log. You must log each disclosure for a public health or benefit activity for accounting. See **Section 27–Standard Procedure for Logging Disclosures for Accounting**.

b) [RESERVED]

c) Public Health Activities. We may use and disclose the minimum necessary protected health information for public health activities as follows:

i) Public Health Authority. We may disclose the minimum necessary protected health information to a public health authority legally authorized to collect or receive protected health information to prevent or control disease, injury or disability (including disease, injury, birth, death, other vital event reporting, and public health surveillance, investigation or intervention).

ii) Foreign Government Officials. We may, at the direction of a public health authority, disclose the minimum necessary protected health information to a foreign government official acting in collaboration with a public health authority.

iii) Persons Subject to Food & Drug Administration. We may disclose the minimum necessary protected health information for activities related to the quality, safety or effectiveness of a FDA–regulated product or activity to persons subject to FDA jurisdiction with responsibility for that FDA–regulated product or service, including to:

- Collect or report adverse events (or similar activities regarding food or dietary supplements); product, product use or labeling defects or problems; or biological product deviations.

- Enable product recalls, repairs, replacements or lookbacks (including locating and notifying individuals who received the products).

- Track FDA–regulated products.

- Conduct post–marketing surveillance.

iv) **Persons Exposed to Communicable Disease.** We may disclose the minimum necessary protected health information to persons who may have been exposed to communicable disease, or are otherwise at risk of contracting or spreading disease, when we or a public health authority is legally authorized to give notification as needed in conducting public health intervention or investigation.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

d) **Public Health and Safety Threats.** We may, consistent with applicable law and ethical standards, use or disclose the minimum necessary protected health information that we believe, in good faith (based on actual knowledge or credible representation of persons with apparent knowledge or authority), is needed:

- To prevent or lessen a serious and imminent health or safety threat to a person or the public, provided we reasonably believe the use or disclosure involves a person (including the target) who is able to prevent or lessen the threat.

- For a law enforcement official to identify or apprehend an individual who appears from the circumstances to have escaped from a correctional institution or lawful custody, or we reasonably believe may have caused serious physical harm to a victim, based on the individual's statement admitting participation in a violent crime.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Minimum Necessary. The minimum necessary protected health information you may disclose to the law enforcement official for these purposes is not more than the individual's statement, name, address, Social Security Number, date and place of birth, blood type, type of injury, date and time of treatment, distinguishing characteristics (e.g., height, weight, gender, race, hair and eye color, facial hair, scars, tattoos) and, if applicable, death. You may not

disclose, unless required by law, DNA, DNA analysis, dental records, or body or tissue typing, samples or analyses (other than blood type). See **Section 26– Standard Procedure for Minimum Necessary Determination**.

e) **Provider's Treatment Activities for Workplace Health and Safety.** We may disclose to an employer the minimum necessary protected health information we obtain about an individual who is a member of the employer's workforce in connection with medical surveillance of the workplace or evaluation of the individual for work–related illness or injury.

We must be undertaking the evaluation or medical surveillance at the employer's request, and the protected health information we disclose must be no more than the minimum necessary to convey our findings concerning our evaluation or medical surveillance or as needed for the employer to comply with federal or state obligations to record workplace illness or injury or conduct workplace medical surveillance.

We must give individuals written notice that their protected health information we obtain by the evaluations or medical surveillance will be disclosed to the employer. We may give that notice either at the time we furnish health care to the individual or, if we are furnishing the health care at the employers' workplace, by prominently posting the notice at the location where we are furnishing the health care.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

f) **Workers' Compensation.** The HIPAA Privacy Regulation will not alter our ability to disseminate PHI with regards to workers compensation claims. As such, we should continue to follow the dissemination practices that are consistent with the District's "Workers Compensation Law". We must remember to disclose the minimum necessary protected health information authorized by and needed to comply with workers' compensation or similar programs established by law that provide benefits for work–related injury or illness without regard to fault.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

g) **Deaths.** We may disclose the minimum necessary protected health information to a coroner or medical examiner for identifying deceased persons, determining cause of death or their other legally authorized duties. We may disclose protected health information to funeral directors, consistent with applicable law, as necessary for them to carry out their duties.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

h) Organ Donation. We may use the minimum necessary protected health information, or disclose it to organ procurement organizations or other entities engaged in procuring, banking or transplanting cadaveric organs, eyes or tissue, to facilitate organ, eye or tissue donation or transplantation.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

i) Required by Law. We may use or disclose protected health information as required by law.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Minimum Necessary. There is no minimum necessary limitation for use or disclosure of protected health information required by law, but the use or disclosure must comply with and be limited to the relevant legal requirements, and you must follow all applicable legal procedural requirements.

j) Health Oversight Activities. We may disclose the minimum necessary protected health information to a health oversight agency as needed for legally authorized health oversight activities, such as audits, civil, criminal or administrative actions or proceedings, inspections, licensure, certification, disciplinary actions, and appropriate oversight of the health care system or government benefits programs (e.g., Medicare and Medicaid) for which health information is relevant to beneficiary eligibility or entities subject to government regulatory programs or civil rights laws.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

k) Judicial and Administrative Proceedings. We may disclose the minimum necessary protected health information in the course of a judicial or administrative proceeding:

i) Order. In response to a court or administrative tribunal order, provided we disclose only the expressly ordered protected health information.

ii) Process. In response to a subpoena, discovery request or other lawful process not accompanied by court or administrative tribunal order, if we:

- Make a reasonable effort to provide notice to the individual sufficient to permit the individual to object to, or seek a qualified protective order from, a court or administrative tribunal; or

- We receive "satisfactory assurance" that the information seeker has made reasonable efforts either (a) to ensure the individual has notice, or (b) to secure a qualified protective order from the court or administrative tribunal or by party stipulation that limits the parties' use or disclosure to the purpose of the proceeding, and requires return or destruction of the protected health information (including all copies) at end of the proceeding.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Approval of "Satisfactory Assurance." Our Privacy Official must determine that we have sufficient "satisfactory assurance" before you may disclose protected health information for these purposes.

l) Law Enforcement.

i) Required by Law. We may disclose protected health information to a law enforcement official as required by law, including to report wounds or physical injuries. (This provision does not apply to reporting adult or child abuse, neglect or domestic violence. See **Sections 4(m)–Adult Abuse, Neglect, Domestic Violence** for information about reporting adult abuse, neglect or domestic violence, and **4(n)–Child Abuse or Neglect** for information about reporting child abuse or neglect.)

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Minimum Necessary. There is no minimum necessary limitation for use or disclosure of protected health information required by law, but the use or disclosure must comply with and be limited to the relevant legal requirements, and you must follow all applicable legal procedural requirements.

ii) Process. We may disclose the minimum necessary protected health information to a law enforcement official in compliance with a judicial order, warrant, summons, regular or grand jury subpoena. We may disclose the minimum necessary protected health information to a law enforcement official in compliance with an administrative subpoena, summons, request, civil investigative demand or similar process that is specific and limited in scope, seeks protected health information that is relevant and material to a

legitimate law enforcement inquiry, and for which de–identified health information cannot reasonably be used.

iii) **Identification.** We may (and we must if required by law) disclose protected health information to a law enforcement official seeking information to identify or locate a suspect, fugitive, material witness, or missing person.

PROCEDURE—Minimum Necessary. The minimum necessary protected health information you may disclose to the law enforcement official for these purposes is not more than the individual's name, address, Social Security Number, date and place of birth, blood type, type of injury, date and time of treatment, distinguishing characteristics (e.g., height, weight, gender, race, hair and eye color, facial hair, scars, tattoos) and, if applicable, death. You may not disclose, unless required by law, DNA, DNA analysis, dental records, or body or tissue typing, samples or analyses (other than blood type). See **Section 26–Standard Procedure for Minimum Necessary Determination**.

iv) **Suspicious Death.** We may disclose the minimum necessary protected health information to alert a law enforcement official about an individual's death that we suspect may have resulted from criminal conduct.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

v) **Crime on Premises.** We may disclose to a law enforcement official the minimum necessary protected health information that we believe in good faith constitutes evidence of criminal conduct on our premises.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

vi) **Medical Emergency.** We may disclose to a law enforcement official the minimum necessary protected health information when furnishing health care in a medical emergency (other than an emergency on our premises) if the disclosure appears necessary to alert law enforcement officials of commission and nature of a crime, the location of the crime and its victims, and the identity, description, and location of suspected criminals. (This provision does not apply if the medical emergency results from adult abuse, neglect or domestic violence. See **Section 4(m)–Adult Abuse, Neglect, Domestic Violence** for reporting adult abuse, neglect or domestic violence.)

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

vii) **Crime Victim.** We may (and we must if required by law) disclose protected health information to a law enforcement official seeking information about an actual or suspected crime victim. (This provision does not apply to reporting for public health activities or adult abuse, neglect or domestic violence, unless reporting these to the law enforcement official is required by law. See **Sections 4(c)–Public Health Activities** for information about reporting public health activities, and **4(m)–Adult Abuse, Neglect, Domestic Violence** for information about reporting adult abuse, neglect or domestic violence.)

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

FORM—Crime Victim Reporting. Use FORM 11–Crime Victim/Abuse Report to document a crime victim report to law enforcement officials and any notification of the report to the crime victim.

PROCEDURE—Crime Victim Reporting. If you suspect that an individual may be a crime victim, use FORM 11-Crime Victim/Abuse Report to document the reasons for your suspicion. Submit a copy of the completed FORM 11 to our Privacy Official. Follow the instructions of our Privacy Official whether to notify and seek the permission of the suspected crime victim to, or to notify the suspected crime victim of our legal requirement to, report our suspicion to appropriate law enforcement officials. If the notification and report are made, add that information to FORM 11. Include the completed FORM 11 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Crime Victim Unavailable. If a crime victim is incapacitated or unavailable in an emergency situation and so cannot practically give permission for disclosure of protected health information, you may disclose the minimum necessary protected health information requested by a law enforcement official investigating the crime who represents:

- The information is needed to determine whether the law has been violated; and
- The information will not be used against the victim; and
- Immediate law enforcement activity that depends on the disclosure will be materially and adversely affected by waiting for the victim's agreement.

Complete FORM 11-Crime Victim/Abuse Report to document the law enforcement official's representations, why you could not obtain the victim's permission, and your report to the law enforcement official.

Include the completed FORM 11 in the crime victim's records. Send a copy to our Privacy Official.

PROCEDURE—Minimum Necessary. You must determine the minimum necessary protected health information to use or disclose for a crime victim report, unless the information to report is required by law. If required by law, there is no minimum necessary limitation, but the use or disclosure must comply with and be limited to the relevant legal requirements, and you must follow all applicable legal procedural requirements. See **Section 26– Standard Procedure for Minimum Necessary Determination**.

m) **Adult Abuse, Neglect, Domestic Violence.** We may disclose the minimum necessary protected health information about an individual, whom we reasonably believe is or has been the victim of adult abuse, neglect or domestic violence, to a government authority (including a social service or protective service agency) legally authorized to receive reports of adult abuse, neglect or domestic violence, if the disclosure is required by law or the individual agrees to the disclosure. We must notify the individual or the individual's personal representative that we will report or have reported adult abuse, neglect or domestic violence, unless we conclude, in our professional judgment, that telling the individual or the individual's personal representative will place the individual at risk of serious harm.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

FORM—Adult Abuse Reporting and Notification. Use FORM 11–Crime Victim/Abuse Report to document an adult abuse report to government agencies and any notification of the report to the individual.

PROCEDURE—Adult Abuse Reporting. If you suspect adult abuse, neglect or domestic violence, use FORM 11-Crime Victim/Abuse Report to document the reasons for your suspicion. Submit a copy of the completed FORM 11 to our Privacy Official. Follow the instructions of our Privacy Official whether to report the suspected abuse to appropriate government authorities and to notify and seek the agreement of the abused individual for the report. If report and/or notification is made, add that information to FORM 11. Include the completed FORM 11 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Permitted by Law. You may disclose the minimum necessary protected health information to report abuse, neglect or domestic violence, without the individual's agreement, if the disclosure is expressly authorized by statute or regulation, and you conclude, in your professional judgment, that the disclosure is needed to prevent serious harm to the individual or other potential victims. You must obtain the approval of our Privacy Official before you make the disclosure. Use FORM 11-Crime Victim/Abuse Report to document your

reasons for suspecting abuse and for recommending its report without the individual's agreement. Submit a copy of the completed FORM 11 to our Privacy Official. Follow the instructions of our Privacy Official whether to make the report. If a report is made, add that information to FORM 11. Include the completed FORM 11 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Individual Incapacitated. You may disclose the minimum necessary protected health information to report abuse of an individual who is unable to agree because of incapacity, if the disclosure is authorized by statute or regulation and a law enforcement official or other public official authorized to receive adult abuse, neglect or domestic violence reports seeks the information with the representation that:

- The protected health information is not intended to be used against the individual; and
- Immediate enforcement activity that depends on the disclosure will be materially and adversely affected by waiting for the individual to be able to agree.

Complete FORM 11-Crime Victim/Abuse Report to document the official's representations, why you could not obtain the individual's agreement, and your report to the law enforcement official. Include the completed FORM 11 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Minimum Necessary. You must determine the minimum necessary protected health information to use or disclose for an adult abuse report, unless the information to report is required by law. If required by law, there is no minimum necessary limitation, but the use or disclosure must comply with and be limited to the relevant legal requirements, and you must follow all applicable legal procedural requirements. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

n) **Child Abuse or Neglect.** We may disclose the minimum necessary protected health information to an appropriate government authority (such as a public health authority) legally authorized to collect or receive protected health information in connection with reports of child abuse or neglect.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

FORM—Child Abuse Reporting. Use FORM 11–Crime Victim/Abuse Report to document child abuse reports to government agencies.

PROCEDURE—Child Abuse Reporting. If you suspect child abuse or neglect, use FORM 11-Crime Victim/Abuse Report to document the reasons for your

suspicion. Submit a copy of the completed FORM 11 to our Privacy Official. Follow the instructions of our Privacy Official whether to report the suspected child abuse to appropriate government authorities. If a report is made, add that information to FORM 11. Include the completed FORM 11 in the individual's records. Send a copy to our Privacy Official.

PROCEDURE—Minimum Necessary. You must determine the minimum necessary protected health information to use or disclose for a child abuse report, unless the information to report is required by law. If required by law, there is no minimum necessary limitation, but the use or disclosure must comply with and be limited to the relevant legal requirements, and you must follow all applicable legal procedural requirements. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

o) Research. We may disclose the minimum necessary protected health information for research, regardless of funding source, if:

i) Institutional Review Board Approval. We receive proper documentation confirming that an Institutional Review Board or equivalent privacy board has approved alteration or waiver in whole or part of authorization to disclose or use the protected health information for the research.

ii) Preparatory Information. We receive proper representation from a researcher seeking protected health information to prepare for research that the protected health information is needed for the research, will be used and disclosed solely as needed to prepare the research protocol or for a similar preparatory purpose, and no protected health information will be removed from our premises during the review.

iii) Decedent Information. We receive proper representation from a researcher seeking decedents' protected health information that the use and disclosure is needed and is solely for research on decedents' protected health information. We may request documentation showing that the individuals whose protected health information is to be disclosed are dead.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

FORM—Research. Use FORM 12–Research Access Request to document the researcher's representations or documentation.

PROCEDURE—Research. You must have our Privacy Official's approval before you may use or disclose the minimum necessary protected health information for research. Complete FORM 12-Research Access Request to document the required researcher's representations or documentation. Send a copy of the completed FORM 12 to our Privacy Official, and retain the original for your agency file. Follow the instruction of our Privacy Official, including the

procedures for logging disclosures for research, if our Privacy Official approves the researcher's request for protected health information for research.

iv) **Pre–Compliance Permission for Research.** We may use and disclose for research protected health information that we created or received either before, on, or after April 14, 2003 if we obtained, prior to April 14, 2003, either (a) the individual's express legal permission to use and disclose the protected health information for the research, (b) the individual's informed consent to participate in the research, or (c) an Institutional Review Board waiver of informed consent. We must not have agreed, after April 13, 2003, to restrict our use or disclosure of that protected health information.

PROCEDURE—Pre–Compliance Permission for Research. Our Privacy Official must confirm that you may use or disclose the protected health information for research based on the express legal permission received before April 14, 2003. Do not use or disclose the protected health information for research until you receive our Privacy Official's determination. If authorization is needed to use or disclose the protected health information for research, see **Section 3–Authorization** for the procedures for obtaining a valid authorization.

If you have protected health information for which we have express legal permission received before April 14, 2003 that allows its use or disclosure for research, gather all relevant information, including the documentation evidencing the pre-compliance express legal permission, informed consent or Institutional Review Board waiver. Submit the information and documentation to our Privacy Official.

p) **Inmates and Others in Lawful Custody.** We may disclose the minimum necessary protected health information of an inmate or individual in lawful custody to a correctional institution or a law enforcement official, if the correctional institution or law enforcement official represents that the protected health information is needed for:

- The inmate's or individual's health care; or
- The health and safety of the inmate, individual, other inmates, officers, employees or others at the correctional institution or responsible for transporting or transferring inmates to other correctional institutions or facilities; or
- Law enforcement on the correctional institution's premises, or administration and maintenance of correctional institution's safety, security and good order.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

q) Government Personnel, Programs, and National Security.

i) National Security and Intelligence. We may disclose the minimum necessary protected health information to authorized federal officials for lawful intelligence, counterintelligence, and national security activities.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

ii) Government Officials. We may disclose the minimum necessary protected health information for protection of senior federal and foreign officials, and for medical suitability and similar investigations and determinations for appropriate protective personnel and Department of State and Foreign Service personnel and dependants.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

iii) Military Personnel. We may use and disclose the minimum necessary protected health information about military personnel (domestic or foreign) for activities deemed necessary for military purposes by their appropriate military command authority.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

r) POLICY—Documentation. We will retain, on paper or electronically, the documentation we obtain or receive in connection with uses or disclosures for public interest or benefit activities until 6 years after the later of its creation or last effective date.

NOTE: Use and disclosure of mental health information for public interest or benefit is more restrictive under the MHIA, see subsection 4 of Section 23A of the Policy.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official all documentation you create or receive in connection with uses or disclosures for public interest or benefit activities**.** Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

5. Required Disclosures.

a) **POLICY—Required Disclosures to Individual or Personal Representative.** We must disclose all protected health information subject to the right of access or disclosure accounting to an individual (or the individual's personal representative) requesting access or disclosure accounting. See **Section 14–Access** for information about an individual's rights to access protected health information, and **Section 16–Disclosure Accounting** for information about an individual's rights to disclosure accounting.

FORM—Identity and Authority Verification. Use FORM 9-Identity and Authority Verification to document how you verify identity and authority of an individual or personal representative.

PROCEDURE—Verification. You must verify the identity of an individual, and the identity and authority of a personal representative, seeking protected health information before you may disclose the protected health information to that individual or personal representative. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE--Minimum Necessary. You are not required to limit to the minimum necessary the protected health information you disclose to an individual who is its subject or to the individual's personal representative.

b) **POLICY—Required Disclosures to HHS.** We must disclose protected health information to HHS as required for complaint investigation or compliance enforcement or review.

PROCEDURE—Required Disclosures to HHS. Promptly notify our Privacy Official upon receipt of a request for protected health information from HHS. Do not disclose any protected health information in response to an HHS request unless and until you receive instruction from our Privacy Official. Our Privacy Official will coordinate our responses to HHS requests.

FORM—Identity and Authority Verification. Use FORM 9-Identity and Authority Verification to document how you verify identity and authority of HHS representatives.

PROCEDURE—Verification. You must verify the identity and authority of an HHS representative seeking protected health information before you may disclose the protected health information to the HHS representative. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary disclosures of protected health information to HHS for complaint investigation or compliance enforcement or review.

FORM—Disclosure Logging. Use FORM 10-Disclosure Log/Minimum Necessary to log each disclosure to HHS.

PROCEDURE—Disclosure Log. You must log each disclosure to HHS for accounting. See **Section 27–Standard Procedure for Logging Disclosures for Accounting**.

c) **POLICY—Documentation.** We will retain, on paper or electronically, the documentation we create or receive in connection with required disclosures until 6 years after the later of its creation or last effective date.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official with all documentation you create or receive in connection with required disclosures. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

6. Minimum Necessary.

a) **POLICY—Minimum Necessary.** We must make reasonable efforts to use, to disclose, or to request of another covered entity, only the minimum necessary protected health information to accomplish the intended purpose. There is no minimum necessary limitation for:

- Disclosure to or a request by a health care provider for treatment.
- Use with and disclosure to an individual (or the individual's personal representative).
- Use and disclosure pursuant to an authorization by an individual (or the individual's personal representative).
- Disclosure to HHS for complaint investigation or compliance enforcement or review.
- Use and disclosure required by law.
- Use and disclosure required for compliance with the HIPAA Administrative Simplification Rules.

FORM—Minimum Necessary Determination. Use FORM 10-Disclosure Log/Minimum Necessary to document your minimum necessary determinations.

PROCEDURE—Minimum Necessary Determination. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

b) **POLICY—Workforce Use.** We must make reasonable efforts to limit access to and use of protected health information by our workforce members to the minimum necessary to perform their duties.

PROCEDURE—Implementation. Our Privacy Official, working with the heads of each agency, will identify, and document on **Table 1—Minimum Necessary Use of Protected Health Information by Workforce Members** of **Section 26–Standard Procedure for Minimum Necessary Determination**:

- Those workforce members (or classes of workforce members) who need access to protected health information to perform their duties; and
- The categories of protected health information needed by each of those workforce members (or those classes of workforce members) to perform those duties; and
- Any conditions appropriate to each workforce member's access to those categories of protected health information.

Our Privacy Official will then issue additional written procedures regarding access to and use of protected health information by our workforce members. Each agency head, or designee, will implement those additional written procedures to ensure that each workforce member (or class of workforce members) within the agency has access to and uses only that protected health information consistent with the identified and documented needs.

PROCEDURE—Workforce Use. As a member of our workforce, you may access and use only the minimum necessary protected health information reasonably needed to perform your duties for our organization. You must not attempt to access or use more than the minimum necessary protected health information needed to perform your duties. If you have questions regarding the protected health information you may access or use to perform your job, consult your agency head, or designee, or our Privacy Official.

c) **POLICY—Routine or Recurring Disclosures and Requests.** We will follow our standard protocols for determining the minimum necessary protected health information for routine or recurring disclosures of and requests for protected health information to which the minimum necessary limitation applies.

PROCEDURE—Standard Protocols Development. Our Privacy Official, working with the heads of each agency, will identify and document on **Table 2—Minimum Necessary Determination for Protected Health Information Disclosures and Requests** of **Section 26–Standard Procedure for Minimum Necessary Determination**:

- Our routine or recurring disclosures and requests for protected health information; and

- The categories of protected health information needed to accomplish the purpose of each of these routine or recurring disclosures and requests; and

- Any conditions appropriate to each routine or recurring disclosure and request for those categories of protected health information.

Our Privacy Official will issue standard protocols for the minimum necessary protected health information for specified routine or recurring disclosures and requests. Each agency head, or designee, will implement these standard protocols with respect to any of the specified routine or recurring disclosures or requests that affect the agency to ensure that each workforce member within the agency follows the standard protocols when making such routine or recurring disclosures or requests.

d) **POLICY—Non–Routine and Non–Recurring Disclosures or Requests.** For any disclosure of, or request of a covered entity for, protected health information (a) to which the minimum necessary limitation applies and (b) that our Privacy Official has not identified and documented as routine or recurring, we will apply our criteria to the particular situation to limit the protected health information we disclose or request to the minimum reasonably necessary to accomplish the purpose of the disclosure or request.

PROCEDURE—Criteria Development. Our Privacy Official, working with the heads of each agency, will develop criteria to apply to determine, on an individual basis, the minimum necessary protected health information for non-routine and non-recurring disclosures and request, and reflect those criteria in **Section 26–Standard Procedure for Minimum Necessary Determination**. Each agency head, or designee, will ensure that each workforce member within the agency applies these criteria on an individual basis when needed to determine the minimum necessary protected health information to disclose or to request of a covered entity on a non-routine and non-recurring basis.

e) **POLICY—Entire Medical Record.** We will not use, disclose or request of a covered entity an entire medical record, except as permitted in procedures that our Privacy Official adopts reflecting those situations where the entire medical record is the amount reasonably necessary for the purpose, or as approved by our Privacy Official as specifically justified in a particular circumstance. We will provide access to an entire medical record only to those workforce members or classes of workforce members that our procedures identify as needing the entire medical record and only in accordance with conditions established by our procedures.

PROCEDURE—Entire Medical Record. Our Privacy Official, working with the heads of each agency, will identify those situations for which an entire medical record is the minimum amount of protected health information reasonably needed, and reflect those situations in **Section 26–Standard Procedure for Minimum Necessary Determination**. Each agency head, or designee, will ensure that each workforce member within the agency uses,

discloses or requests of a covered entity an entire medical record only in these identified situations, or as approved by our Privacy Official as specifically justified in a particular circumstance.

f) **POLICY—Requests from Others.** We may rely, if reasonable under the circumstances, on a request for protected health information to be for the minimum necessary, if the requester is:

- A covered entity (such as a health plan or another health care provider who is subject to the Privacy Rules).
- A professional (such as an attorney or accountant) who is a member of our workforce or our business associate, and who represents that the minimum necessary is being requested.
- A government agent or law enforcement official who represents that the minimum necessary is being requested.
- A researcher who represents or provides appropriate documentation that the minimum necessary is being requested. See **Section 4(o)-Research.**

PROCEDURE—Request from Covered Entity. You may rely on a request for protected health information to be for the minimum necessary if from a covered entity, or from a professional, a government official or a researcher who so represents, as long as your reliance is reasonable under the circumstance. Use FORM 10-Disclosure Log/Minimum Necessary to document your reliance. See **Section 26–Standard Procedure for Minimum Necessary Determination**. If you have any doubts about the request, consult your agency head, our Privacy Official before you make the disclosure.

PROCEDURE—Verification. You must verify that the requester is a covered entity, professional, government agent or researcher before you may rely on the request to be for the minimum necessary. See **Section 25–Standard Procedure for Identity and Authority Verification**.

g) **POLICY—Documentation.** We will retain, on paper or electronically, the documentation we create or receive in connection with minimum necessary determinations until 6 years after the later of its creation or last effective date.

PROCEDURE—Documentation. You must furnish our Privacy Official with a copy of all documentation you create or receive in connection with minimum necessary determinations. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

II. DATA POLICIES AND PROCEDURES

7. Limited Data Set.

a) **POLICY—Limited Data Set Use and Disclosure.** We may use a limited data set, and disclose it to a recipient with which we have a data use agreement, for research, public health or health care operations.

FORM—Data Use Agreement. FORM 21–Data Use Agreement contains the mandatory terms that the Privacy Rules require to be in a data use agreement.

PROCEDURE—Obtaining the Data Use Agreement. You must obtain a data use agreement signed by the intended recipient of a limited data set before you may disclose a limited data set to that recipient. Use FORM 21–Data Use Agreement as a template for preparing and negotiating the data use agreement. Be sure to indicate in the data use agreement whether the limited data set is for research, public health, or specific health care operations, and to specify the uses and disclosures that the recipient may make of the protected health information in the limited data set to be disclosed.

PROCEDURE—Contract Approval. Submit the proposed data use agreement to our Privacy Official for approval. If approved, obtain the signature of the intended recipient on the data use agreement before disclosing the limited data set. Send the original, signed data use agreement to our Privacy Official. Retain a copy for your agency's file.

b) **POLICY—Limited Data Set Creation.** We may use protected health information, and disclose it to a business associate, to create a limited data set for our use or for disclosure to another (including the business associate that created the limited data set). See **Section 10–Business Associates** for information about our relationship with business associates.

PROCEDURE—Limited Data Set Creation. A limited data set must exclude all direct identifiers of each individual whose protected health information is included and of each of those individuals' relatives, household members, and employers. It may contain any other data, including age, any element of dates (e.g., birth dates, admission dates, discharge dates, death dates), any geographic information broader than postal addresses (e.g., municipalities, States, zip codes), and any unique identifying number, characteristic or code.

PROCEDURE—Minimum Necessary. A limited data set may contain only the minimum necessary protected health information for the purpose for which the limited data set is to be used or disclosed. See **Section 26–Standard Procedures for Minimum Necessary Determination**.

PROCEDURE—Limited Data Set Verification. Our Privacy Official must verify that data qualify as a limited data set, and that the limited data set satisfies the minimum necessary limitation, before the data may be used or disclosed for one of the permitted purposes of research, public health or health care operations.

c) **POLICY—Data Use Agreement Recipient's Compliance.** If we learn that a recipient of a limited data set from us has materially breached the data use agreement, we will require the recipient to promptly cure the breach. If the recipient fails to cure the breach to our satisfaction, we will discontinue disclosing protected health information through the limited data set or otherwise, terminate the data use agreement, and report the recipient's breach to HHS.

PROCEDURE—Recipient's Suspected Breach. You must immediately notify and cooperate with our Privacy Official if you learn that a recipient of a limited data set from us has breached the data use agreement. Follow any direction you receive from our Privacy Official with respect to the breach.

d) **POLICY—Our Data Use Agreement Compliance.** We will fully comply with the terms of any data use agreement we enter into as the recipient of a limited data set from a covered entity. Our failure to comply with a data use agreement can expose our organization to sanctions under the Privacy Rules.

PROCEDURE—Our Suspected Breach. You must immediately notify and cooperate with our Privacy Official if you learn that we may have breached or violated a data use agreement we entered into as recipient of a limited data set. You must follow the instructions of our Privacy Official regarding investigation and resolution of the suspected breach or violation.

e) **POLICY—Documentation.** We will retain, on paper or electronically, each data use agreement and any other documentation we obtain or receive in connection with limited data sets until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with each data use agreement and a copy of any other documentation obtained or received in connection with limited data sets. Our Privacy Official will retain the data use agreements and the other documentation until 6 years after the later of their creation or last effective date.

8. De–Identified Health Information.

a) **POLICY—De–Identified Health Information.** We may use and disclose de–identified health information without restriction. We will treat as protected health information any key or other means to re–identify health information that has been de-identified.

PROCEDURE—De–Identified Health Information. Our Privacy Official must verify that health information is de–identified before you may use or disclose it without regard for the privacy protections of these Privacy Policies and Procedures and the Privacy Rules.

b) **POLICY—De–Identified Health Information Creation.** We may use protected health information, and disclose it to a business associate, to create de–identified health information. See **Section 10–Business Associate** for information about our relationship with business associates.

PROCEDURE—De–Identified Health Information Creation. Health information may be de–identified under the supervision and subject to the documented approval of our Privacy Official as follows:

i) Statistical Expert. A statistical expert, with knowledge and experience in generally accepted statistical and scientific principles and methods for rendering information not personally identifiable, may determine and document that the risk is very small that health information we had de–identified could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is its subject.

ii) Identifier Removal. All identifiers of the individual and the individual's relatives, household members, and employers, associated with the health information must be removed. We must have no actual knowledge that the information remaining after stripping these identifiers could be used, alone or in combination with other information, to identify the individual.

c) **POLICY—Re–Identification Codes.** Any code or means employed to permit re–identification of de–identified health information will not be derived from or relate to any individual whose information has been de–identified, be capable of translation to identify an individual, or be used or disclosed for any purpose other than re–identification of de–identified health information.

PROCEDURE—Re-Identification Codes. Our Privacy Official must approve the selection of re-identification codes for de-identified health information. You will consider re-identification codes to be protected health information and apply the privacy protections of these Privacy Policies and Procedures to them.

d) **POLICY—Documentation.** We will retain, on paper or electronically, the documentation we create or receive in connection with the de–identification of protected health information until 6 years after the later of its creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with all documentation created or received in connection with the de–identification of protected health information. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

III. RELATIONSHIP RULES

9. Personal Representatives.

a) **POLICY—Personal Representative.** We must consider a personal representative to be the individual for all purposes under these Privacy Policies and Procedures and the Privacy Rules, unless we conclude that the personal representative may be abusive.

FORM—Identity and Authority Verification. Use FORM 9-Identity and Authority Verification to document how you verify identity and authority of personal representatives.

PROCEDURE—Verification. You must verify the identity and authority of a personal representative before you may disclose protected health information to the personal representative. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary the protected health information disclosed to a personal representative.

b) **POLICY—Abusive Personal Representative.** We will not consider a person to be a personal representative, and will not disclose any protected health information to that person, if we:

- Reasonably believe that the person has subjected or may subject the individual to abuse, neglect or domestic violence, and that acknowledging a representation could endanger the individual; and
- Conclude, in our professional judgment, that recognizing the person to be a personal representative is not in the individual's best interest.

FORM—Adult Abuse Reporting and Notification. Use FORM 11–Crime Victim/Abuse Report to document the reasons for suspecting an abusive personal representative, including any report of abuse to government agencies and notification of the report to the individual.

PROCEDURE—Abusive Personal Representative. Consult our Privacy Official before you disclose an individual's protected health information to a personal representative you suspect may be abusive. Complete FORM 11–Crime Victim/Abuse Report to document the reasons for your belief and submit a copy to our Privacy Official. Follow the instructions of our Privacy Official regarding the personal representative. See **Section 4(m)–Adult Abuse, Neglect, Domestic Violence** and **Section 4(n)–Child Abuse or Neglect** for information about reporting abusive relationships to appropriate government authority.

c) Personal Representatives of Adults and Emancipated Minors.

i) POLICY—Permitted Uses and Disclosures. We may use with and disclose to a personal representative of an adult or emancipated minor that protected health information relevant to the scope of the representation.

PROCEDURE—Permitted Uses and Disclosures. Consult our Privacy Official if there is any question regarding use with or disclosure to a personal representative of an adult or emancipated minor.

ii) POLICY—Required Disclosures. We will furnish a personal representative the same access to and disclosure accounting for an individual's protected health information that must be accorded the individual, provided the access or disclosure accounting involves protected health information relevant to the scope of the representation.

PROCEDURE—Required Disclosures. Consult our Privacy Official if there is any question regarding required disclosure to a personal representative of an adult or emancipated minor. See **Section 14-Access** and **Section 16-Disclosure Accounting** for information about individual's rights to access and have disclosure accounting for protected health information.

d) Personal Representatives of Unemancipated Minors.

i) POLICY—Access Permitted. We will grant a parent, guardian or person acting in loco parentis access to and control over an unemancipated minor's protected health information if, and to the extent, applicable State or other law (including case law) permits or requires us to give the parent, guardian, or person acting in loco parentis access or control.

PROCEDURE—Access Permitted. Consult our Privacy Official if there is any question regarding access to and control over an unemancipated minor's protected health information by a parent, guardian or person acting in loco parentis. See **Section 14-Access** and **Section 16-Disclosure Accounting** for information about individual's rights to access and have disclosure accounting for protected health information.

ii) **POLICY—Access Prohibited.** We will not recognize a parent, guardian or person acting in loco parentis as a personal representative of an unemancipated minor if, and to the extent, applicable State or other law (including case law) prohibits us from giving the parent, guardian or person acting in loco parentis access or control.

PROCEDURE—Access Prohibited. Consult our Privacy Official if there is any question regarding access to and control over an unemancipated minor's protected health information by a parent, guardian or person acting in loco parentis. See **Section 14-Access** and **Section 16-Disclosure Accounting** for information about individual's rights to access and have disclosure accounting for protected health information.

iii) **POLICY—Professional Judgment.** Where no applicable State or other law (including case law) addresses whether a parent, guardian or person acting in loco parentis may have access to and control over an unemancipated minor's protected health information, we will grant or deny the parent, guardian or person acting in loco parentis access and control consistent with any applicable State or other law (including case law) based on the professional judgment of a licensed health care professional.

PROCEDURE—Professional Judgment. Consult our Privacy Official if there is any question regarding access to and control over an unemancipated minor's protected health information by a parent, guardian or person acting in loco parentis. See **Section 14-Access** and **Section 16-Disclosure Accounting** for information about individual's rights to access and have disclosure accounting for protected health information.

iv) **POLICY—Minor's Control.** Unless State or other law (including case law) permits or requires parental control of an unemancipated minor's protected health information, the unemancipated minor has, to the extent consistent with applicable State or other law (including case law), the authority to control and have access to his or her own protected health information pertaining to a health care service as follows:

(1) **Minor's Assent to Health Care.** The unemancipated minor agrees to the health care, no other agreements are required by law (even if the agreement of others has been obtained), and the unemancipated minor has not requested a parent, guardian, person acting in loco parentis, or another person to be regarded as a personal representative.

PROCEDURE—Minor's Assent to Health Care. Consult our Privacy Official if there is any question regarding an unemancipated minor's capacity to assent to health care.

(2) **Minor's Lawful Receipt of Health Care.** The unemancipated minor, a court, or a legally authorized person agrees to the health care, and

applicable State or other law allows the unemancipated minor to obtain the health care without assent of a parent, guardian, or person acting in loco parentis.

PROCEDURE—Minor's Lawful Receipt of Health Care. Consult our Privacy Official if there is any question regarding an unemancipated minor's lawful receipt of health care.

(3) Parental Assent to Confidentiality. The parent, guardian, or person acting in loco parentis assents to a confidentiality agreement between the unemancipated minor and the health care provider regarding the health care.

PROCEDURE—Parental Assent to Confidentiality. Consult our Privacy Official if there is any question regarding the assent of a parent, guardian, or person acting in loco parentis to a confidentiality agreement between an unemancipated minor and a health care provider regarding health care.

e) Personal Representatives of Deceased Individuals.

i) POLICY—Information Protected. We will accord the protected health information of a deceased individual all of the privacy protections of these Privacy Policies and Procedures and the Privacy Rules.

PROCEDURE—Information Protected. You will apply the privacy protections of these Privacy Policies and Procedures and the Privacy Rules to the protected health information of deceased individuals.

ii) POLICY—Rights of Executors. We will furnish an executor, administrator or other person authorized by applicable law to act for a deceased individual or the deceased individual's estate, the same rights with respect to a deceased individual's protected health information that must be accorded the individual, provided the protected health information is relevant to the scope of the representation.

PROCEDURE—Rights of Executors. Consult our Privacy Official if there is any question regarding the right of an executor, administrator or other person authorized by applicable law to act for a deceased individual or the estate.

f) POLICY—Documentation. We will retain, on paper or electronically, the documentation we create or receive in connection with uses or disclosures involving personal representatives until 6 years after the later of its creation or last effective date.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official all documentation created or received in

connection with uses or disclosures involving personal representatives. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

10. Business Associates.

a) POLICY—Uses and Disclosures with Business Associates. We will not disclose protected health information to a business associate, or allow a business associate to create or receive protected health information on our behalf, unless our Privacy Official confirms that the business associate has entered into a compliant written contract with us.

NOTE: If the health care component's role is that of a **provider**, then the business associate contract requirement does not apply to our permitted disclosures to a health care provider concerning treatment.

If the health care component's role is that of a **health plan**, then the business associate contract requirement does not apply to our permitted disclosures to:

- A health care provider concerning treatment.
- A plan sponsor of a group health plan which we service. See **Section 11-Group Health Plans and Plan Sponsors**.

FORMS–Business Associate Contract.

- **FORM–Business Associate Contract Terms.** FORM 22-Business Associate Contract Terms contains the mandatory terms that the Privacy Rules require to be in a business associate contract.
- **FORM–Crosswalk Business Associate Terms to Privacy Rules Mandates.** FORM 23–Crosswalk Business Associate Terms to Privacy Rules Mandates is a tool that shows the relationship between the contract terms of FORM 22–Business Associate Contract Terms and the business associate contract terms mandated by the Privacy Rules.
- **FORM–HHS Sample Business Associate Provisions.** FORM 24–HHS Sample Business Associate Provisions contains the sample business associate provisions published by HHS to guide development and negotiation of compliant business associate contracts.

PROCEDURE–Obtaining the Business Associate Contract. You must obtain a signed, compliant business associate contract before you may disclose protected health information to a business associate, or allow a business associate to create or receive protected health information on our organization's behalf. Use FORM 22–Business Associate Contract Terms as a template for preparing and negotiating a business associate contract. Use FORM 23–Crosswalk Business

Associate Terms to Privacy Rules Mandates as an aid during negotiations to show which terms are mandated by the Privacy Rules. Be sure to specify the uses and disclosures that the business associate may make of protected health information.

PROCEDURE–Contract Approval. Submit the proposed business associate contract to our Privacy Official for approval. If approved, sign and obtain the business associate's signature on the contract. Send the signed, original business associate contract to our Privacy Official. Retain a copy for your agency's file.

PROCEDURE—Minimum Necessary. Uses with and disclosures to our business associates of protected health information are subject to the minimum necessary limitation. See **Section 6–Minimum Necessary** for information about the minimum necessary limitation, and **Section 26–Standard Procedures for Minimum Necessary Determination** for our procedures to determine minimum necessary.

PROCEDURE—Disclosure Log. Disclosures to our business associates are accountable, unless exempted from disclosure accounting. See **Section 16–Disclosure Accounting** for information about accountable disclosures, and **Section 27–Standard Procedures for Logging Disclosures for Accounting** for our disclosure logging procedures.

b) **POLICY—Business Associate Compliance.** If we learn that a business associate has materially breached the business associate contract, we will require the business associate to promptly cure the breach. If the business associate fails to cure the breach to our satisfaction, we will terminate the business associate contract and our business associate relationship with that business associate. If termination of the contract is not feasible, we will report the business associate's breach to HHS.

PROCEDURE—Suspected Breach. You must immediately notify and cooperate with our Privacy Official if you learn that a business associate may have breached or violated the business associate contract. You must follow the instructions of our Privacy Official regarding investigation and resolution of the suspected breach or violation.

c) **POLICY—Our Organization as Business Associate.** We may serve as the business associate of a covered entity (for example, we may provide billing services, practice management, provide administrative services only or third party administration for a group health plan, or electronic transaction translation and transmission as a health care clearinghouse for other health care providers). When we serve as a business associate of a covered entity, we will enter into a business associate contract with that covered entity.

PROCEDURE—Our Organization as Business Associate. You must obtain the approval of our Privacy Official for any business associate contract you may be asked to accept on behalf of our organization before you may undertake any

business associate function or activity involving protected health information. Offer FORM 22-Business Associate Contract Terms as our preferred template for developing and negotiating business associate contracts.

d) **POLICY—Our Business Associate Contract Compliance.** We will fully comply with the terms of each business associate contract we enter into as a business associate of a covered entity.

PROCEDURE—Our Suspected Breach. You must immediately notify and cooperate with our Privacy Official if you learn that we may have breached or violated our business associate contract with a covered entity. You must follow the instructions of our Privacy Official regarding investigation and resolution of the suspected breach or violation. Our failure to comply with our business associate contract obligations can expose our organization to sanctions under the Privacy Rules.

e) **POLICY—Documentation.** We will retain, on paper or electronically, each business associate contract the involves our organization, and all documentation we create or receive regarding compliance of our business associates or our compliance as a business associate of covered entities, until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with each business associate contract that involves our organization, and all documentation created or received regarding compliance of our business associates or our compliance as a business associate of covered entities. You may retain a copy for your agency's file. Our Privacy Official will retain the business associate contracts and the other documentation of our compliance with this **Section 10** until 6 years after the later of their creation or last effective date.

11. Group Health Plans and Plan Sponsors.

a) **POLICY—Organized Health Care Arrangements with Insured Group Health Plans.** We are part of an organized health care arrangement with each group health plan the benefits of which we insure. We are allowed to disclose to a group health plan we insure, for the health care operations of our organized health care arrangement, the protected health information we create or receive that relates to current or former participants or beneficiaries of that group health plan, without the permission of those participants or beneficiaries. See **Section 1(b)(v)-POLICY—Organized Health Care Arrangement's Health Care Operations.**

PROCEDURE—Verification of Organized Health Care Arrangements with Insured Group Health Plans. Our Privacy Official must confirm that we are part of an organized health care arrangement before you may disclose to a group health plan the protected health information of current or former participants or

beneficiaries for the health care operations of the organized health care arrangement. See **Section 12(b)-Organized Health Care Arrangement** for information about organized health care arrangements.

b) **POLICY—Business Associate Relationships with Self-Funded Group Health Plans.** We act as the business associate of a self-funded group health plan for which we provide administrative services only or third party administration. Our use and disclosure of the protected health information of the participants and beneficiaries of that group health plan will be controlled by the terms of our business associate contract with the group health plan. See **Section 10-Business Associate** for information about business associate relationships.

FORM—ASO Business Associate Terms. FORM 25-ASO Business Associate Terms contains the terms that the Privacy Rules mandate for a business associate contract, and a variety of optional terms (marked by asterisks) pertinent to an administrative services only relationship with a group health plan and the group health plan's sponsor.

PROCEDURE—Business Associate Relationships with Self-Funded Group Health Plans. Use FORM 25-ASO Business Associate Terms as a template for negotiating administrative services only ("ASO") arrangements with self-funded group health plans and their plan sponsors. Terms in FORM 25 not marked by asterisks are mandated by the Privacy Rules and cannot be modified without the prior approval of our Privacy Official.

Each ASO business associate agreement must be signed by an authorized representative of the group health plan, such as the plan fiduciary. That signature is required because the group health plan is the covered entity in the relationship. The plan sponsor may also sign, but that signature is ineffective to create the business associate relationship that must exist between the group health plan and us as its business associate when we provide administrative services only for the self-funded group health plan.

Submit the proposed ASO business associate agreement to our Privacy Official for approval. If approved, sign and have the authorized representative of the group health plan, such as the plan fiduciary, sign the agreement. Send the original, signed agreement to our Privacy Official. Retain a copy for your agency's file.

PROCEDURE—Compliance with ASO Business Associate Contract. See **Section 10(c)-POLICY—Our Organization as Business Associate** for our compliance policies and procedures when we serve as a covered entity's business associate.

c) **POLICY—Disclosure of Protected Health Information to Plan Sponsors.** Neither we nor a group health plan may, without enrollees' authorization, disclose enrollees' protected health information to the plan sponsor—the employer, union

or other entity that established and maintains the group health plan. There are three exceptions:

i) **Enrollment Data to Plan Sponsor.** A plan sponsor may receive from its group health plan and from us the minimum necessary information to determine whether an individual is or is not participating in the group health plan or is enrolled in or has disenrolled from our insured coverage.

PROCEDURE—Enrollment Data to Plan Sponsor. You must not disclose enrollment information to a plan sponsor unless our Privacy Official confirms that the information to be disclosed is the minimum necessary to determine if an individual is or is not participating in the group health plan or is enrolled in or has disenrolled from our insured coverage. See **Section 26–Standard Procedure for Minimum Necessary Determination**.

ii) **Summary Health Information to Plan Sponsor.** A plan sponsor may receive from its group health plan and from us the minimum necessary summary health information to enable the plan sponsor to either (a) obtain premium bids for providing coverage under the group health plan, or (b) modify, amend or terminate the group health plan.

FORM—Plan Sponsor's Summary Health Information Request. FORM 26-Plan Sponsor's Summary Health Information Request is a template for the required plan sponsor representation that a request for summary health information is for one of the two permitted purposes.

PROCEDURE—Summary Health Information to Plan Sponsors. You must not disclose summary health information to a plan sponsor unless our Privacy Official confirms that the information to be disclosed is the minimum necessary summary health information, and that its disclosure to the plan sponsor is for a permitted purpose. Use FORM 26-Plan Sponsor's Summary Health Information Request as the template for a plan sponsor to confirm that it requests summary health information for a permitted purpose. Send the plan sponsor's confirmation to our Privacy Official. Retain a copy for your agency's file.

iii) **Plan Administration Functions by Plan Sponsor.** A plan sponsor may receive from its group health plan and from us the minimum necessary enrollees' protected health information to enable the plan sponsor to perform plan administration functions for the group health plan, provided that the plan sponsor furnishes written certification that the group health plan's document has been amended to include "satisfactory assurance" that the plan sponsor will appropriately safeguard and limit use and disclosure of the protected health information, including not using or disclosing the protected health information for any employment-related action or decision or in connection with any other benefit or benefit plan.

FORM—Plan Sponsor's "Satisfactory Assurance." FORM 27–Plan Document Amendment contains the mandatory terms for the plan document of a group health plan that the Privacy Rules require to evidence the plan sponsor's "satisfactory assurance." You may use FORM 27 to show a group health plan and its plan sponsor the "satisfactory assurance" that must appear in the plan document for the plan sponsor to qualify under the Privacy Rules to receive protected health information to perform plan administrative functions.

FORM—Plan Sponsor's Certification. FORM 28–Plan Sponsor's Certification is an example of the certification of "satisfactory assurance" a plan sponsor must make before we will disclose a group health plan enrollees' protected health information to the plan sponsor for plan administration functions. You may use FORM 28 to show a group health plan and its plan sponsor a sufficient "satisfactory assurance" certification.

PROCEDURE—Plan Sponsor's Certification. You must not disclose protected health information to a plan sponsor unless our Privacy Official receives sufficient evidence of the plan sponsor's certification of "satisfactory assurance" that the requisite plan document amendment has been made. You are under no obligation to inspect or obtain the plan document to determine if it has actually been amended. Rather, you may rely on the plan sponsor's certification (unless you know it to be false).

PROCEDURE—Minimum Necessary. Our Privacy Official will consult with you to determine whether permitted disclosures of enrollment data, summary health information or protected health information for plan administration functions to the plan sponsor will be routine or recurring or must be addressed on an individual basis. See **Section 6-Minimum Necessary** for information about the minimum necessary limitation, and **Section 26–Standard Procedure for Minimum Necessary Determination** for our procedures for determination of minimum necessary.

PROCEDURE—Disclosure Log. Disclosures to plan sponsors are accountable, unless exempted from disclosure accounting. See **Section 16–Disclosure Accounting** for information about accountable disclosures, and **Section 27–Standard Procedures for Logging Disclosures for Accounting** for our disclosure logging procedures.

PROCEDURE—Suspected Breach. You must immediately notify and cooperate with our Privacy Official, if you learn that a plan sponsor may have breached or violated its "satisfactory assurance." You must follow the instructions of our Privacy Official regarding investigation of the suspected breach or violation, and our continued disclosure of protected health information to that plan sponsor.

d) **Group Health Plan Privacy Practices Notice.** A group health plan's obligations regarding the Privacy Practices Notice vary depending on whether it is self-funded or fully insured and, if fully insured, whether it creates or receives protected health information. We will address the obligations regarding Privacy Practices Notices based on the status of and our relationship with a group health plan. See **Section 13-Privacy Practices Notice**.

i) **Self-Funded Group Health Plan.** A group health plan, self-funded in whole or part, must provide each enrollee a Privacy Practices Notice. The self-funded group health plan's Notice must state that it intends to disclose protected health information (including enrollment data or summary health information) to its plan sponsor, if that is the case.

POLICY—Privacy Practices Notice for Self-Funded Group Health Plan. If we provide administrative services only to a self-funded group health plan (making us the group health plan's business associate), we will not be obligated to provide a separate Privacy Practices Notice. That is the obligation of the self-funded group health plan.

If we underwrite an insured part of the coverage of a partially self-funded group health plan, we must issue a Privacy Practices Notice to the enrollees we insure. We may issue the enrollees a joint Notice with the group health plan. Our Notice or the joint Notice must state that we intend to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, if that is the case. See **Section 13-Privacy Practices Notice**.

ii) **Insured Group Health Plan with Protected Health Information.** A group health plan that furnishes health benefits solely through insurance contracts and that creates or receives protected health information (other than enrollment data and summary health information) must maintain a Privacy Practices Notice, but need distribute it only on request. See **Section 13-Privacy Practices Notice**.

POLICY—Privacy Practices Notice for Insured Group Health Plan with Protected Health Information. If we underwrite an insured group health plan that creates or receives protected health information (other than enrollment data and summary health information), we must issue a Privacy Practices Notice to the enrollees we insure. We may issue the enrollees a joint Notice with the group health plan, as we are in an organized health care arrangement with a group health plan that we insure. Our Notice or the joint Notice must state that we intend to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, if that is the case. The group health plan must maintain a Privacy Practices Notice (which may be a joint Notice with us as its insurer), but need distribute that Notice only upon request. See **Section 13-Privacy Practices Notice**.

iii) **Insured Group Health Plan without Protected Health Information.** A group health plan, that furnishes health benefits solely through insurance contracts and that neither creates nor receives protected health information (other than enrollment data and summary health information), is not required to maintain or distribute a Privacy Practices Notice. It only needs to have its plan document reflect the privacy practices of its plan sponsor.

PROCEDURE—Insured Group Health Plan Privacy Practices Notice. If we underwrite an insured a group health plan that neither creates nor receives protected health information (other than enrollment data and summary health information), we must distribute a Privacy Practices Notice to the enrollees that we insure. Our Notice must state that we intend to disclose protected health information to the plan sponsor, if that is the case. See **Section 13-Privacy Practices Notice**.

PROCEDURE— Agencies. The agency head, or designee, of each agency that services group health plans will report to our Privacy Official those group health plans for which we provide administrative services only (thereby making us those group health plans' business associate) and those group health plans for which we underwrite an insurance contract. Our Privacy Official will coordinate with the agency head, or designee, and the group health plans to determine the Privacy Practices Notice that should be prepared and who will prepare and distribute the Notice.

e) **POLICY—Documentation.** We will retain, on paper or electronically, each plan sponsor's certification of "satisfactory assurance," each request for summary health information, and all other documentation we create or receive regarding compliance with this **Section 11**, until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with each plan sponsor's certification of "satisfactory assurance," request for summary health information, and all other documentation created or received regarding compliance with this **Section 11**. You may retain a copy for your agency's file. Our Privacy Official will retain each plan sponsor's certification of "satisfactory assurance," request for summary health information, and all other documentation regarding compliance with this **Section 11** until 6 years after the later of their creation or last effective date.

12. Covered Entity Structures.

a) **Covered Entity Structures.** Special rules apply to the privacy obligations of certain kinds of business organizations, affiliations, joint ventures, and operations. This section identifies these special rules.

POLICY—Determining Covered Entity Structures. Only our Privacy Official may determine that a certain kind of business organization, affiliation, joint venture, or operation involving our organization qualifies for these special rules regarding the privacy of protected health information.

PROCEDURE—Verifying Covered Entity Structures. You must obtain verification and procedural instructions from our Privacy Official that a particular business organization, affiliation, joint venture, or operation involving our organization qualifies for special rules regarding the privacy of protected health information. You must strictly follow those procedural instructions.

If you question whether a business organization, affiliation, joint venture, or operation involving our organization qualifies for these special rules or how the special rules apply, consult your agency head, or our Privacy Official before you act.

b) Organized Health Care Arrangement. An organized health care arrangement in which we may participate as a health care provider or as a health plan is any of the following relationships of covered entities:

- A clinically–integrated care setting where individuals typically receive health care from more than one health care provider (e.g., a hospital and its medical staff); or

- An organized system of health care in which the covered entity participants hold themselves out to the public as part of a joint arrangement and participate in joint activities that include at least (a) utilization review, (b) quality assessment and improvement activities, or (c) payment activities that involve sharing the financial risk of the health care delivered by the participants.

- A group health plan and the health insurance issuer or HMO that insures its benefits, with respect to the protected health information that the health insurance issuer or HMO creates or receives that relates to current and former enrollees of the group health plan.

- All group health plans maintained by the same plan sponsor.

- All group health plans maintained by the same plan sponsor and all health insurance issuers or HMOs that insure the benefits of those group health plans, with respect to the protected health information that the health insurance issuers or HMOs create or receive that relates to current and former enrollees of those group health plans.

- Certain managed care arrangements in which the covered entity participants hold themselves out to the public as part of a joint arrangement and participate in joint activities that include at least (a) utilization review, (b) quality assessment and improvement activities, or (c) payment activities that

involve sharing the financial risk of the health care delivered by the participants.

POLICY—Organized Health Care Arrangement Status. If we are a participant in an organized health care arrangement, we may disclose the minimum necessary protected health information to the other covered entity participants in the organized health care arrangement for the health care operations of the organized health care arrangement. See **Section 1(b)(v)-Organized Health Care Arrangement's Health Care Operations**.

PROCEDURE—Organized Health Care Arrangement Compliance. Before making any disclosure of protected health information with respect to an organized health care arrangement, you must confirm with our Privacy Official that:

- We participate in the organized health care arrangement; and
- The intended recipient of the protected health information is a covered entity participant in that organized health care arrangement; and
- The protected health information to be disclosed is the minimum necessary for a health care operation of the organized health care arrangement.

c) Hybrid Entity. A hybrid entity is a covered entity that has business activities that include both covered functions and other functions. A hybrid entity must treat all of its business activities, including its non–health care functions, as subject to the Privacy Rules, unless it designates in writing all of its operations that performs covered functions as its health care components. After making such designation, only its health care components will be subject to the Privacy Rules. A hybrid entity may include in its health care components any operation that performs business associate functions or activities for a health care component.

POLICY—Hybrid Entity Status. The District of Columbia has determined that it is a hybrid entity, thus, we will be responsible for the compliance of our health care components with the Privacy Rules. Our health care components will adhere to these Privacy Policies and Procedures to ensure their compliance with the Privacy Rules. Our health care components will not disclose protected health information to, or permit use of protected health information by, another component of our organization that is not a health care component in ways that the Privacy Rules prohibit for legally independent entities. A workforce member who performs duties for our health care components and for our other components must not use or disclose protected health information created or received in the course of or incident to the duties for the health care components in ways that the Privacy Rules prohibit.

FORM—Hybrid Entity Designation. FORM 29–Hybrid Entity Health Care Component Designation is used to make the written designation of our health care components, and any component performing business associate functions or

activities that we elect to include as a health care component, in order for our organization to become a hybrid entity.

PROCEDURE—Hybrid Entity Designation and Compliance. Senior officials of the District, in consultation with our Privacy Official, will determine the manner in which we will become a hybrid entity by making the required written designation. As a hybrid entity, our Privacy Official will ensure proper documentation of our health care components, and of any components performing business associate functions or activities that senior officials of the District determine to include as a health care component, by having FORM 29 completed. The Privacy Official will coordinate notifying the heads of each agency of our hybrid entity status and ensure that those agencies performing covered functions understand and comply with these Privacy Policies and Procedures and the Privacy Rules regarding use and disclosure of protected health information by a hybrid entity.

If you are a workforce member who performs duties for health care components as well as other non-health care components of a hybrid entity, you must not use or disclose protected health information created or received in the course of, or incident to, duties you perform for the health care components in any way that is prohibited by the Privacy Rules.

d) Single Affiliated Covered Entity. Covered entities that are legally separate, but affiliated by common ownership or common control, may designate themselves or their health care components as a single affiliated covered entity for Privacy Rules compliance. The designation must be in writing.

POLICY—Single Affiliated Covered Entity Status. If our organization determines that it should become part of an affiliated covered entity, we will comply with the Privacy Rules applicable to the covered functions that we perform. We will not allow use or disclosure of protected health information received only with respect to one covered function to be used or disclosed for other covered functions of the single affiliated covered entity of which we are a part, except as the Privacy Rules allow of non–affiliated covered entities.

FORM—Single Affiliated Covered Entity Designation. FORM 30–Single Affiliated Covered Entity Designation is used to make the written designation of the members of an affiliated covered entity.

PROCEDURE—Single Affiliated Covered Entity Designation and Compliance. Senior officials of the District, in consultation with our Privacy Official, will determine whether and which affiliates of our organization should be designated as a single affiliated covered entity. If we become a single affiliated covered entity, our Privacy Official will ensure proper documentation of the members of the single affiliated covered entity by having FORM 30 completed. The Privacy Official will coordinate notifying the management of each member of the single affiliated covered entity status and ensure that

management of each member complies with these Privacy Policies and Procedures and the Privacy Rules regarding use and disclosure of protected health information by a single affiliated covered entity. If we become a single affiliated covered entity, you must not use or disclosure protected health information created or received only with respect to one covered function for other covered functions of the single affiliated covered entity, except as the Privacy Rules allow of non–affiliated covered entities.

e) **Multiple–Function Covered Entity.** A covered entity that performs multiple covered functions (e.g., furnishes health care as a provider health plan, pays for the cost of health care as a health plan, and/or translates electronic transactions into and out of standard formats as a health care clearinghouse) is a multiple–function covered entity. A multiple–function covered entity must comply with the provisions of the Privacy Rules applicable to its various covered functions and may not allow protected health information received only with respect to one covered function to be used or disclosed for other covered functions, except as the Privacy Rules allow for covered functions performed by independent covered entities.

POLICY—Multiple-Function Covered Entity Status. To the extent that our organization performs multiple covered functions, we will comply with the provisions of the Privacy Rules applicable to our various covered functions. We will not allow protected health information received only with respect to one of our covered functions to be used or disclosed for any other of our covered functions, except as the Privacy Rules allow for covered functions performed by independent covered entities.

PROCEDURE—Multiple–Function Covered Entity Compliance. If we perform multiple covered functions, you must not allow protected health information created or received only with respect to one covered function to be used or disclosed for other covered functions, unless our Privacy Official approves the use or disclosure.

f) **Health Care Clearinghouse.** A health care clearinghouse is a covered entity that processes or facilitates the processing of health information received from one entity into or out of standard transactions for transmission to another entity.

i) **Operated as Business Associate.** A health care clearinghouse that creates or receives protected health information as a business associate may use and disclose the protected health information it creates or receives for or from a covered entity only as permitted by its business associate contract with that covered entity. See **Section 10–Business Associates** for information about business associate relationships. In this business associate capacity, a health care clearinghouse is relieved from compliance with most of the administrative obligations of the Privacy Rules.

ii) **Operated as Covered Entity.** A health care clearinghouse that creates or receives protected health information for any purpose, other than as a business associate of another covered entity, must comply fully with the Privacy Rules.

g) **POLICY—Documentation.** We will retain, on paper or electronically, the documentation we create or receive in connection with designations of and activities involving covered entity structures, until 6 years after the later of its creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with any documentation created or received in connection with designations of or activities involving covered entity structures. Our Privacy Official will retain the documentation until 6 years after the later of its creation or last effective date.

IV. INDIVIDUAL'S INFORMATION RIGHTS

13. Privacy Practices Notice.

a) Privacy Practices Notice

i) **PROVIDER POLICY—Privacy Practices Notice.** As a health care provider, we will maintain a Privacy Practices Notice to give individuals written notice of the uses and disclosures of protected health information that we may make, and of the individuals' rights and our legal duties with respect to protected health information. The Notice will be written in plain language. We will always use and disclose protected health information consistently with our Notice. We will furnish our Notice to any person who requests one.

We may have different Notices for different relationships we have with other health care provider, including joint Notices with health care providers which are in an organized health care arrangement with us. We must be sure that we provide an individual requesting or entitled to a Notice from us with the Notice or joint Notice applicable to that individual's relationship to us. See **Section 12(b)—Organized Health Care Arrangement** for information about organized health care arrangements.

FORM—Privacy Practices Notice. FORM 36A–Privacy Practices Notice contains the mandatory terms for a health care provider's Privacy Practices Notice.

PROCEDURE—Privacy Practices Notice Adoption. Our Privacy Official must approve each Privacy Practice Notice, including any joint Notice, before it may be made effective. Each Notice must bear its effective date (which may not be earlier than the date the Notice is printed or otherwise published).

ii) **HEALTH PLAN POLICY—Privacy Practices Notice.** As a health plan, we will maintain a Privacy Practices Notice to give individuals written notice of the uses and disclosures of protected health information that we may make, and of the individuals' rights and our legal duties with respect to protected health information. The Notice will be written in plain language. We will always use and disclose protected health information consistently with our Notice.

We may have different Notices for different relationships we have with our members and with group health plans, including joint Notices with group health plans and health insurance issuers or HMOs which are in an organized health care arrangement with us. We must be sure that we provide an individual entitled to a Notice from us with the Notice or joint Notice applicable to that individual's relationship to us. See **Section 11(d)-Group Health Plan Privacy Practices Notice** for information about Privacy Practices Notices for group health plans, and **Section 12(b)—Organized Health Care Arrangement** for information about organized health care arrangements.

FORM—Privacy Practices Notice. FORM 36B–Privacy Practices Notice contains the mandatory terms for a health plan's Privacy Practices Notice.

PROCEDURE—Privacy Practices Notice Adoption. Our Privacy Official must approve each Privacy Practice Notice, including any joint Notice, before it may be made effective. Each Notice must bear its effective date (which may not be earlier than the date the Notice is printed or otherwise published).

b) **POLICY—Revision to Privacy Practices Notice.** We will promptly revise our Privacy Practices Notice whenever there is a material change to our uses or disclosures of protected health information, to our legal duties, to the individuals' rights or to other privacy practices that render the statements in our Notice no longer accurate. All of our Notices will state that we reserve the right to change them and to make the changes applicable to all protected health information we maintain. That statement is needed to ensure that a change in our privacy practices can apply to all of the protected health information that we maintain, including protected health information that we created or received before the effective date of the change. Each of our Notices will also explain how we will disseminate a revised Notice.

PROCEDURE—Revision to Privacy Practices Notice. We will not implement a material change in our privacy practices before the effective date of the revised Notice reflecting the change, unless the change is required by law. If the change is required by law, we will implement the change immediately, and revise our Notice promptly to reflect the change required by law.

{Sections 13(c) and (d) apply only to a health care provider with a direct treatment relationships with an individual. A direct treatment relationship is any treatment relationship that is not an indirect treatment relationship. A health care provider has an indirect treatment relationships when the health care provider delivers

health care to an individual based on the orders of another health care provider and typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider who provides those services, products or reports to the individual.}

c) Privacy Practices Notice Distribution.

i) PROVIDER DISTRIUTION POLICY— Only a Privacy Practices Notice, including any joint Notice, that has been approved by our Privacy Official may be distributed to fulfill our obligation to give Notice.

PROCEDURE—Privacy Practices Notice Distribution. Our Privacy Official will coordinate with the heads of each affected agency to ensure proper distribution of our Notice. If your agency has responsibility for Notice distribution, you will distribute the Privacy Practice Notice appropriate to the relationship we have with the patient as follows:

- You will disseminate the appropriate Privacy Practices Notice to each individual no later than the date of our first service delivery to the individual after April 13, 2003.
- You will furnish the Notice by personal delivery if our first service delivery is a patient visit.
- You will deliver the Notice by automatic and contemporaneous electronic response if our first delivery is by electronic mail or the Internet.
- You will promptly mail the Notice if our first service delivery is by telephone.
- You will post our Notice in a clear and prominent place at each of our service delivery sites so that individuals seeking service from us may reasonably be expected to be able to read the Notice.
- In an emergency treatment situation, you will furnish our Notice as soon as reasonably practicable after the emergency has abated.
- You will ensure that our Notice is prominently posted and electronically available on each web site we maintain that provides information about our services.
- You will have our Notice available at each of our service delivery sites to give individuals who request it. You will furnish our Notice to any person on request.
- You may email our Notice to any individual who has agreed to electronic notification and not withdrawn that agreement. You must provide a paper copy of our Notice to the individual, if you know the individual failed to get

the email transmission of our Notice or if the individual requests a paper copy.

ii) **HEALTH PLAN DISTRIUTION POLICY—** Our Privacy Official will coordinate with the agency head, or designee, of each affected agency to ensure proper distribution of our Notice. If your agency has responsibility for Notice distribution, you will distribute the Privacy Practice Notice appropriate to the relationship we have with the subscriber as follows:

- You will disseminate the appropriate Privacy Practices Notice to each individual who is our subscriber no later than April 14, 2003 (our Privacy Rules compliance date).
- You will disseminate our Notice to each new subscriber at enrollment.
- You will notify our then current subscribers, at least once every 3 years, that our Notice is available on request, explaining how the subscribers may obtain it.
- You will ensure that our Notice is prominently posted and electronically available on each web site we maintain that provides information about our customer services or benefits.
- You will disseminate our revised Notice, resulting from any material change we adopt in our privacy practices, to our then current subscribers within 60 days of the material change. You must not implement the material change in our privacy practices before the effective date of our revised Notice (unless earlier implementation is required by law).
- You will furnish our Notice to any person on request.
- You may email our Notice to any individual who has agreed to electronic notification and not withdrawn that agreement. You must provide a paper copy of our Notice to the individual, if you know the individual failed to get the email transmission of our Notice or if the individual requests a paper copy.

d) **POLICY—Notice Acknowledgment for PROVIDER NOTICES.** We will make a good faith effort to obtain an individual's written acknowledgement of receipt of our Notice at the first service encounter. If the individual fails or refuses to give the acknowledgement, we will document our effort to obtain it.

If our first service encounter is an emergency treatment situation, we do not need to seek written acknowledgement of receipt of our Notice from the individual who received the emergency health care.

NOTE: Obtaining an individual's written acknowledgement of receipt of our Notice applies only to those Notices provided to the individual by District health

care components who perform a provider health care function and have a direct treatment relationship with the individual.

FORM—Notice Acknowledgement. Use FORM 37–Notice Acknowledgement to record the individual's acknowledgement of receipt of our Notice or our good faith effort to obtain such acknowledgement.

PROCEDURE—Notice Acknowledgement. If you are responsible for furnishing our Notice at service encounters, you must request the individual to sign an acknowledgement of receipt of our Notice.

- If the Notice is furnished in person, ask the individual to sign FORM 37–Notice Acknowledgement.
- If the Notice is mailed after a telephone service delivery, include FORM 37–Notice Acknowledgement and a stamped, self–addressed envelope with the mailing and request that the individual sign and return FORM 37 in the included envelope.
- If the Notice is furnished electronically, ask the individual to acknowledge its receipt by return email.
- If the individual fails or refuses to provide a signed FORM 37 or give other written or electronic acknowledgement of receipt of the Notice, document your good faith effort to obtain acknowledgement on FORM 37.

Attach the completed FORM 37–Notice Acknowledgement or any email or other tangible acknowledgement to the Notice furnished to the individual and include them in the individual's records. Send a copy to our Privacy Official.

Although it is not necessary to furnish an individual more than one copy of our Notice, if you are unsure whether an individual has received our Notice, furnish it to the individual and attempt to obtain the individual's acknowledgement on FORM 37–Notice Acknowledgement.

e) **POLICY—Organized Health Care Arrangement Joint Notice.** We may use a joint Privacy Practices Notice with the covered entities with which we participate in an organized health care arrangement. See **Section 12(b)—Organized Health Care Arrangement** for information about organized health care arrangements. These participants may use a joint Notice as long as each agrees to be bound by the joint Notice's terms with respect to all protected health information created or received pursuant to participation in the organized health care arrangement.

PROCEDURE—Organized Health Care Arrangement Joint Notice. Only our Privacy Official may approve our use of a joint Notice. You must have our Privacy Official's confirmation that we are part of an organized health care arrangement and approval of a joint Notice for that organized health care arrangement before you may disseminate a joint Notice in connection with that

organized health care arrangement. Distribution of a joint Notice will be in accordance with **Sections 13 (b), 13(c)(i) or 13(c)(ii),** and **13(d)** above, except distribution of a joint Notice to an individual by another covered entity participating in the organized health care arrangement satisfies our distribution obligation to that individual. You must document each distribution of the Notice you make. Send the documentation to our Privacy Official. You may maintain a copy for your agency's file.

PROCEDURE—Acknowledgement of Receipt of Organized Health Care Arrangement Joint Notice. You must obtain a copy of the written acknowledgement of receipt of notice from the covered entity that provided the joint Notice, or complete FORM 37–Notice Acknowledgement to document that another covered entity distributed the joint Notice to an individual and we were not obligated to distribute the joint Notice to that individual. Attach the completed FORM 37 to the joint Notice and include them in the individual's records. Send a copy to our Privacy Official.

NOTE: Obtaining an individual's written acknowledgement of receipt of our Notice applies only to those Notices provided to the individual by District health care components who perform a provider health care function and have a direct treatment relationship with the individual.

f) **POLICY—Notice for Insured Group Health Plans.** We will distribute either our Privacy Practices Notice or a joint Privacy Practices Notice for each group health plan for which we underwrite an insurance contract, as we are participants in an organized health care arrangement.

PROCEDURE—Notice for Insured Group Health Plans. Only our Privacy Official may approve our Notice or the use and content of a joint Notice. The agency head, or designee, of each agency that services group health plans will report to our Privacy Official those group health plans for which we underwrite an insurance contract. Our Privacy Official will coordinate with the agency head, or designee, and the group health plans that we insure to determine whether our Notice or a joint Notice should be prepared, and who will prepare and distribute the Notice.

If your agency has responsibility for Privacy Practices Notices for group health plans that we insure, you will use the Notice or a joint Notice, as approved by our Privacy Official, that is appropriate to the relationship we have with the subscribers enrolled under our coverage. Distribution of the Notice will be in accordance with **Section 13(b)** above. You must document each distribution of the Notice you make. Send the documentation to our Privacy Official. You may maintain a copy for your agency's file.

g) **POLICY—Notice for Self-Funded Group Health Plans.** We will provide and/or distribute the Privacy Practices Notice for a group health plan, self-funded in whole or part, that we administer only if we agree to undertake that task in our

ASO Business Associate Terms with the self-funded group health plan. See **Section 11(d)(i)-Self-Funded Group Health Plan**.

PROCEDURE—Notice for Self-Funded Group Health Plans. The agency head, or designee, of each agency that services group health plans will report to our Privacy Official those group health plans, self-funded in part or in whole, for which we provide administrative services only or third party administration (thereby making us those group health plans' business associate). You will not agree to prepare and/or distribute a Privacy Practices Notice for a self-funded group health plan unless our Privacy Official approve the arrangement and the arrangement is documented in our ASO Business Associate Terms with the self-funded group health plan.

If we agree to prepare and/or distribute the self-funded group health plan's Notice and your agency services that group health plan, you will act in accordance with our Notice obligations under our ASO Business Associate Terms with the group health plan. You must document each distribution of the Notice you make for the self-funded group health plan. Send the documentation to our Privacy Official. You may maintain a copy for your agency's file.

h) **POLICY—Documentation.** We will retain, on paper or electronically, a copy of each Privacy Practices Notice we issue, the documentation of our distribution and acknowledgement of receipt of Privacy Practices Notices, and all other documentation of our compliance with our Notice obligations, until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must provide our Privacy Official with a copy of each Privacy Practices Notice issued, the documentation of our distribution and acknowledgement of receipt of Privacy Practices Notices, and all other documentation of our compliance with our Notice obligations. You may retain a copy for your agency's file. Our Privacy Official will retain a copy of each Privacy Practices Notice we issue, each Notice acknowledgement we receive, and all other documentation of our compliance with our Notice obligations until 6 years after the later of their creation or last effective date.

14. Access.

a) **POLICY—Right to Inspect and Copy.** We will allow an individual to inspect and to obtain a copy of his or her protected health information for as long as we or our business associates maintain that protected health information in designated record sets. We may withhold from an individual only that protected health information specified in **Section 14(b)** below.

NOTE: The MHIA is more restrictive with regard to an individual's right to inspect and copy PHI, see Section 23A.

FORM—Access Request. Use FORM 38–Access Request to document an individual's request to inspect and to obtain a copy of his or her protected health information.

PROCEDURE—Access Request. We are obligated to respond to the individual's request for access within 30 days of its receipt. Consequently, do not delay transmitting an access request to our Privacy Official. Complete, or have the individual complete, the first page of FORM 38–Access Request, then promptly transmit the entire FORM 38 to our Privacy Official. You must not tell an individual that the protected health information requested will or will not be made available.

PROCEDURE—Access Fees. We may charge a reasonable, cost–based fee for providing access, including copying and mailing of the requested protected health information, and for preparing a summary or explanation of the requested protected health information. We may not charge for retrieving the requested protected health information. Our Privacy Official will determine any charges and inform the individual in advance so that the individual may elect to withdraw or modify the request to reduce or avoid the fee.

FORM—Access Response. The Access Request Processing page of FORM 38–Access Request is designed to coordinate the response to an individual's access request.

PROCEDURE—Access Response. Only our Privacy Official may determine whether to grant or deny an individual access to protected health information. Our Privacy Official will process each access request as follows:

- Track the processing of the access request on the Access Request Processing page of FORM 38-Access Request, and use the Direction to Retrieve Records page of FORM 38 to direct our agencies and business associates to furnish the protected health information needed to comply with the access request.

- Respond in writing to the individual's request for access within 30 days. (The initial response may be written notice that a 30 day extension will be taken for reasons stated in the notice.) Use the Grant of Access to Records page or the Denial of Access to Records page of FORM 38, as appropriate, to inform the individual whether access is granted or denied (with a statement of the reasons for denial, and the procedures for complaining to us and to HHS about a denial)

- If access is granted, use the Grant of Access to Records page to inform the individual of any applicable fees to ensure that the individual still wants access, copies, a summary or explanation, or mailing.

- Have the completed FORM 38 included in the individual's records, and retain a copy for the Privacy Official file.

b) POLICY—Protected Health Information We May Withhold.

i) Denial of Access without Right of Review. We may deny access to, and a copy of, the following information, without providing an individual the opportunity for review of the denial:

- Information compiled in reasonable anticipation of or for use in civil, criminal or administrative action or proceeding.
- Protected health information obtained in confidence from a source, other than a health care provider, if access is reasonably likely to reveal the source.
- Protected health information that may be withheld from the individual under the Clinical Laboratory Improvements Amendments of 1988 (42 U.S.C. § 263a).
- Psychotherapy notes.
- Protected health information compiled by a health care provider in the course of continuing research including treatment, provided the individual agreed to waive access when consenting to participate in the research and access will be reinstated when the research is completed.
- Protected health information contained in records that may be withheld from the individual under the Federal Privacy Act (5 U.S.C. § 552a).

NOTE: The MHIA is more restrictive with regard to an individual's right to inspect and copy PHI, see Section 23A.

ii) Denial of Copies to Inmates. When acting under a correctional institution's direction, we may, without providing opportunity for review, deny an inmate copies, but not inspection, of the inmate's protected health information when furnishing copies would jeopardize health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for transporting the inmate.

iii) Denial of Access to Dangerous Information. We may deny access, subject to providing the individual an opportunity for independent review, to protected health information that a licensed health care professional, in exercise of professional judgment, determines is reasonably likely to:

- Endanger the life or physical safety of the individual or another person; or
- Cause substantial harm to a person, not a health care provider, who is referenced in the protected health information; or

- Cause substantial harm to an individual or another person, if a personal representative's access request were granted.

PROCEDURE—Review of Access Denial for Endangerment. An individual has the right, on request, to have another licensed health care professional promptly review our denial of access on grounds of endangerment. When our Privacy Official denies access to protected health information, our Privacy Official will:

- Inform the individual in writing, using the Denial of Access to Records page of FORM 38, of the right of independent review and the procedures for exercising that right; and

- If the individual requests review, designate a licensed health care professional who did not participate in the denial decision to review the decision and, within a reasonable time, report to our Privacy Official whether the denial is justified; and

- Promptly report the reviewer's determination in writing to the individual, and act in accordance with the reviewer's determination.

c) **POLICY—Access Granted.** We will timely permit an individual who has been granted access the opportunity to inspect and obtain a copy of his or her protected health information at a time and place, or by mail, as may be mutually agreed by the individual and our Privacy Official. We will provide the individual a summary or explanation of the requested protected health information, if the individual requests and agrees to pay any fee we may charge for preparing the summary or explanation.

NOTE: The MHIA is more restrictive with regard to an individual's right to inspect and copy PHI, see Section 23A.

PROCEDURE—Access Granted. If instructed by our Privacy Official to supervise a grant of access, you will furnish the requested protected health information in the form or format that the individual requests, unless that is not feasible. Consult with the Privacy Official if it appears that the form or format the individual requests is not feasible. If our Privacy Official informs you that there is a fee, you must collect the fee before providing the access service to which the fee applies.

d) **POLICY—Designations.** We must identify in writing each designated record set we maintain or that is maintained on our behalf by our business associates, and the titles of persons or offices responsible for receiving and processing access requests.

FORM—Designations. FORM 51–Designated Personnel and Record Sets is used to identify our designated record sets, including any designated record set

maintained on our behalf by our business associates, and the personnel responsible for receiving and processing access requests.

PROCEDURE—Designations. The agency head, or designee, of each affected agency must document on FORM 51-Designated Personnel and Record Sets the persons or job categories responsible for receiving and processing access requests in the agency, and the designated record set maintained by the agency or for the agencies by business associates. Send the completed FORM 51 to our Privacy Official and maintain a copy in the agency file. Promptly update FORM 51 upon any change in designated personnel or record sets.

e) **POLICY—Documentation.** We must document, on paper or electronically, each designated record set we maintain or that is maintained on our behalf by our business associates, the titles of persons or offices responsible for receiving and processing access requests, each access request we receive, our response, and any other documentation regarding our compliance with our obligations to provide access.

PROCEDURE—Documentation. You must include in the individual's records and furnish to our Privacy Official each access request received and our response. You must also furnish our Privacy Official the designation of personnel and record sets and any other documentation regarding our compliance with respect to amendment requests. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

15. Amendment.

a) **POLICY—Right to Amend.** We will allow an individual to request to amend his or her protected health information for as long as we or our business associates maintain the protected health information in designated record sets. We may deny an amendment request only as specified in **Section 15(b)** below.

NOTE: The MHIA is more restrictive with regard to an individual's right to inspect and copy PHI, see Section 23A.

FORM—Amendment Requests. Use FORM 39–Amendment Request to document an individual's request to amend his or her protected health information.

PROCEDURE—Amendment Requests. We are obligated to respond to the individual's request to amend within 60 days of its receipt. Consequently, do not delay transmitting an amendment request to our Privacy Official. Complete, or have the individual complete, the first page of FORM 39–Amendment Request, then promptly transmit the entire FORM 39 to our Privacy Official. You must not tell an individual that the protected health information will or will not be amended.

FORM—Amendment Response. The Amendment Request Processing page of FORM 39-Amendment Request is designed to coordinate the response to an individual's amendment request.

PROCEDURE—Amendment Response. Only our Privacy Official may determine whether to grant or deny an individual's amendment request. Our Privacy Official will process each amendment request as follows:

- Track the processing of the amendment request on the Amendment Request Processing page of FORM 39-Amendment Request.

- Respond in writing to an individual's request to amend within 60 days. (The initial response may be written notice that a 30 day extension will be taken for reasons stated in the notice.) Use the Grant of Amendment to Records page or the Denial of Amendment to Records page of FORM 39, as appropriate, to inform the individual whether the amendment will be granted or denied (with a statement of the reasons for denial, an explanation for submitting written disagreement and other options for tagging protected health information as disputed, and the procedures for complaining to us and to HHS about a denial).

- If amendment is granted, use the Notification to Amend Records page of FORM 39 to inform agency head, or designee, and business associates with affected designated record sets that they are required to amend the record, and furnish the amendatory material to append or link to the affected records. Obtain from heads of affected agencies lists of contact information for those entities, including our business associates, that may have and rely on the unamended records to the detriment of the individual so that Privacy Official may notify them of the amendment.

- If amendment is denied, use the Notification of Record Amendment Denial page of FORM 39 to inform heads of agencies and business associates with affected designated record sets, and furnish the required materials to append or link to the affected records.

- Have the completed FORM 39 included in the individual's records, and retain a copy for the Privacy Official file.

PROCEDURE— Agencies. The head of each agency with an affected designated record set will amend the affected records as specified in a Notification to Amend Records from our Privacy Official, or append or link to affected records the materials furnished with the Notification of Record Amendment Denial from our Privacy Official and include the appended or linked materials in each disclosure of those records. If the agency is involved with standard transactions that do not permit inclusion of these materials with transmission of the affected records, the agency must separately supply the materials to the recipient of the standard transactions.

For a granted amendment, the agency head, or designee, will promptly submit a list of contact information for those entities, including our business associates, that may have and rely on the unamended records to the detriment of the individual so that our Privacy Official may notify them of the amendment.

b) **POLICY—Bases for Denying Amendment Request.** We may decline to amend protected health information if:

- We did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available to act on the request).
- The information to be amended is not part of a designated record set maintained by us or by a business associate on our behalf.
- The information is accurate and complete.
- The information to be amended may be withheld from the right of access. See **Section 14(b)—Protected Health Information We May Withhold**.

NOTE: The MHIA is more restrictive with regard to an individual's right to inspect and copy PHI, see Section 23A.

c) **POLICY—Amending on Another Covered Entity's Notice.** We will amend protected health information in our designated record sets upon receipt of notice from a covered entity that the protected health information has been amended.

PROCEDURE—Amending on Another Covered Entity's Notice. Promptly inform our Privacy Official upon receipt of a notice from a covered entity that protected health information has been amended, and send the notice to our Privacy Official. Our Privacy Official will:

- Determine if we hold the affected protected health information in our designated record sets or in designated record sets held on our behalf by business associates, and
- Use the Notification to Amend Records page of FORM 39-Amendment Request to notify and instruct the heads of agencies and our business associates with affected designated record sets to amend the affected records.

PROCEDURE—Agencies. The agency head, or designee, of each affected agency must ensure that the affected records in the agency's designated record set are properly amended as specified in the Notification to Amend Records from our Privacy Official, and that thereafter each disclosure is only of the properly amended records.

d) **POLICY—Designations.** We must identify in writing each designated record set we maintain or that is maintained on our behalf by our business associates, and the titles of persons or offices responsible for receiving and processing amendment requests.

FORM—Designations. FORM 51–Designated Personnel and Record Sets is used to identify our designated record sets, including any designated record set maintained on our behalf by our business associates, and the personnel responsible for receiving and processing amendment requests.

PROCEDURE—Designations. The agency head, or designee, of each affected agency must document on FORM 51–Designated Personnel and Record Sets the persons or job categories responsible for receiving and processing amendment requests in the agency, and the designated record sets maintained in the agencies or for the agencies by business associates. Send the completed FORM 51 to our Privacy Official and maintain a copy in the agency's file. Promptly update FORM 51 upon any change in designated personnel or record sets.

e) **POLICY—Documentation.** We must document, on paper or electronically, each designated record set we maintain or that is maintained on our behalf by our business associates, the titles of persons or offices responsible for receiving and processing amendment requests, each amendment request we receive, our response, and any other documentation regarding our compliance with respect to amendment requests.

PROCEDURE—Documentation. You must include in the individual's records and furnish to our Privacy Official each amendment request received and our response. You must also furnish our Privacy Official the designation of personnel and record sets and any other documentation regarding our compliance with respect to amendment requests. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

16. Disclosure Accounting.

a) **POLICY—Right to Disclosure Accounting.** We will provide to an individual upon request an accounting of each disclosure that we make of the individual's protected health information for up to 6 years prior to the request. Essentially, we are obligated to account for disclosures we make without the individual's authorization for research, for public interest or benefit activities, and to HHS for compliance review or enforcement. See **Section 4-Public Interest or Benefit Use and Disclosure** and **Section 5-Required Disclosures.** We are also obligated to account for any disclosures we make that violate the Privacy Rules. We do not have to account for disclosures that are exempt from accounting as specified in **Section 16(b)** below.

FORM—Disclosure Accounting Request. Use FORM 40–Disclosure Accounting Request to document an individual's request for disclosure accounting.

PROCEDURE—Disclosure Accounting Request. We are obligated to respond to the individual's request for a disclosure accounting within 60 days of its receipt. Consequently, do not delay transmitting a disclosure accounting request to our Privacy Official. Complete, or have the individual complete, the first page of FORM 40–Disclosure Accounting Request, then promptly transmit the entire FORM 40 to our Privacy Official.

PROCEDURE—Accounting Fees. We may not charge for an individual's first accounting in any 12 month period. We may charge a reasonable, cost–based fee for other accountings within that same 12-month period. Our Privacy Official will determine any charges for the accounting request.

FORM—Accounting Response. The Disclosure Accounting Processing page of FORM 40-Disclosure Accounting Request is designed to coordinate the response to an individual's accounting request.

PROCEDURE—Accounting Response. Our Privacy Official will process an individual's request for disclosure accounting as follows:

- Determine if there are fees for the individual's accounting request. If there are, notify the individual in advance of the fee so that the individual may elect to withdraw or modify the accounting request to reduce or avoid the fee.

- Track the processing of the accounting request on the Disclosure Accounting Processing page of FORM 40, and use the Direction to Account for Disclosure page of FORM 40 to direct our agencies and business associates to furnish the disclosure data needed to comply with the accounting request in order to augment the disclosure accounting data that the Privacy Official maintains through receipt of completed FORM 10–Disclosure Log/Minimum Necessary.

- Determine if any disclosure to health care oversight or law enforcement officials is subject to temporary suspension as reflected on FORM 41–Disclosure Accounting Suspension. See **Section 16(d)** below.

- Respond in writing to the individual's accounting request within 60 days. (The initial response may be written notice that a 30 day extension will be taken for reasons stated in the notice.) Use the Disclosure Accounting page of FORM 40 to inform the individual that the disclosure accounting is available or to transmit the disclosure accounting to the individual.

- Have the completed FORM 40 included in the individual's records, and retain a copy for the Privacy Official file.

b) **POLICY—Exempt Disclosures.** We do not have to account for the following:

- Disclosures made before April 14, 2003 (our Privacy Rules compliance date).
- Disclosures made for treatment, payment, or health care operations. See **Section 1(b)-Treatment, Payment, Health Care Operations.**
- Disclosures made to the individual or the individual's personal representative. See **Section 1(c)—POLICY-Individual or Personal Representative** and **Section 9-Personal Representatives**
- Disclosures made for notification of or to persons involved in an individual's health care or payment related to that health care, or for disaster relief. See **Section 2-Informal Permission for Certain Uses and Disclosures.**
- Disclosures made pursuant to authorization. See **Section 3-Authorization for Use or Disclosure.**
- Disclosures made in a limited data set. See **Section 7-Limited Data Set.**
- Disclosures made for national security or intelligence purposes. See **Section 4(q)—Government Personnel and Programs.**
- Disclosures made to correctional institutions or law enforcement officials regarding inmates or individuals in lawful custody. See **Section 4(p)—Inmates and Others in Lawful Custody.**
- Disclosures made incident to otherwise permitted or required uses or disclosures. See **Section 1(d)—POLICY-Incidental Use or Disclosure.**

c) **POLICY—Accounting Information.** We will track, and require our business associates to track, accountable disclosures, and make the tracking information available to our Privacy Official on request, so that we may fulfill our obligations to make disclosure accounting to individuals on request.

FORM—Disclosure Logging. FORM 10-Disclosure Log/Minimum Necessary is designed to log the necessary data for each accountable disclosure. See **Section 27–Standard Procedure for Logging Disclosures for Accounting**.

PROCEDURE—Accounting Information. The agency head, or designee, of each agency must ensure the full and timely cooperation of their workforce in tracking accountable disclosures and supplying the needed accountable disclosure data to fulfill our disclosure accounting obligations. The information that must be tracked to fulfill our disclosure accounting obligations is as follows:

i) Accounting Content for Disclosure. The following information for each accountable disclosure of protected health information (including disclosures to or by our business associates) must be recorded and maintained for at least 6 years to support our disclosure accounting obligations:

- The disclosure date;
- The name and, if known, address of each person or entity that received the disclosure;
- A description of the protected health information disclosed; and
- A statement of the purpose of the disclosure, or a copy of any written request for the disclosure from HHS or another government agency or organization to which the protected health information was disclosed pursuant to a public interest or benefit activity.

ii) Accounting Content for Repetitive Disclosures. For multiple disclosures to HHS for a single compliance review or complaint investigation, or to another government agency or organization to which we disclosed protected health information pursuant to a single public interest or benefit purpose, we need provide the individual only:

- The required accounting content listed above for the first of the repetitive disclosures made within the period covered by the individual's request;
- The frequency, periodicity, or number of the repetitive disclosures during the accounting period; and
- The date of the last disclosure during the accounting period.

iii) Accounting Content for Large Research Studies. When we make disclosures for particular research involving 50 or more individuals, for which an Institutional Review Board or privacy board has waived authorization in compliance with the Privacy Rules, see **Section 4(o)—Research**, we may account for disclosures during the period covered by the individual's accounting request that may have included that individual's protected health information by providing:

- The name of the research protocol or activity;
- A plain language description of the research protocol or activity, including its purpose and criteria for selecting particular records;
- A brief description of the type of protected health information disclosed;

- The dates or period during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the period covered by the individual's request;

- The name, address, and telephone number of the research sponsor and the researcher to whom the disclosures were made;

- A statement that the individual's protected health information may or may not have been disclosed for a particular research protocol or other research activity; and

- Assistance in contacting the research sponsor and the researcher, if it is reasonably likely that the individual's protected health information was disclosed for the research protocol or activity.

d) **POLICY—Temporary Accounting Suspension.** We will temporarily suspend accounting for disclosures to health oversight agencies or law enforcement officials from whom we receive notice that an accounting would likely impede their enforcement activity.

FORM—Temporary Accounting Suspension. Use FORM 41–Disclosure Accounting Suspension to document a direction by a health oversight agency or law enforcement official to temporarily suspend accounting of disclosures to the agency or official.

PROCEDURE—Temporary Accounting Suspension. Our Privacy Official must approve any temporary suspension of disclosure accounting. If you receive direction by a health oversight agency or law enforcement official to temporarily suspend accounting of disclosures to the agency or official, you must:

- Try to obtain documentation or information from the health oversight agency or the law enforcement official confirming that the suspension is needed to avoid impairing enforcement activity and specifying the duration of the suspension.

- If the health oversight agency or law enforcement official orally orders the suspension, inform the agency or official that the suspension will end within 30 days unless we receive written confirmation of the suspension within that 30 day period.

- Complete FORM 41-Disclosure Accounting Suspension to document the suspension request, attaching any documentation furnished by the health oversight agency or law enforcement official, and promptly send the completed FORM 41 to our Privacy Official. Include a copy in the individual's records.

- Follow any direction you receive from our Privacy Official.

If the health oversight agency or law enforcement official did not furnish written support for the suspension, our Privacy Official will notify the health oversight agency or law enforcement official in writing that we can suspend accounting for our disclosures to the agency or official no more than 30 days, unless we receive written confirmation within that 30 day period.

PROCEDURE—Agencies. The agency head, or designee, of each affected agency must ensure the agency continues to log accountable disclosures during a temporary suspension period. See **Section 27–Standard Procedure for Logging Disclosures for Accounting**. We have to account for these disclosures after the temporary suspension ends.

e) **POLICY—Designations.** We must identify in writing the titles of persons or offices responsible for receiving and processing disclosure accounting requests.

FORM—Designations. FORM 51–Designated Personnel and Record Sets is used to identify the personnel responsible for receiving and processing disclosure accounting requests.

PROCEDURE—Designations. The agency head, or designee, of each affected agency must document on FORM 51-Designated Personnel and Record Sets the persons or job categories responsible for receiving and processing disclosure accounting requests in the agency. Send the completed FORM 51 to our Privacy Official and maintain a copy in the agency's file. Promptly update FORM 51 upon any change in designated personnel.

f) **POLICY—Documentation.** We must document, on paper or electronically, the information required for us to report accountable disclosures in response to disclosure accounting requests, each disclosure accounting request we receive, each disclosure accounting we provide, the designation of personnel, and any other documentation regarding our compliance with respect to disclosure accounting.

FORM—Disclosure Log. FORM 10–Disclosure Log/Minimum Necessary is used to track each accountable disclosure so that we may fulfill our disclosure accounting obligations.

PROCEDURE—Documentation. You must include in the individual's records and furnish to our Privacy Official the information required for us to report accountable disclosures, each disclosure accounting request received, and each disclosure accounting provided. You must also furnish our Privacy Official the designation of personnel and any other documentation regarding our compliance with respect to restriction requests. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

17. Restriction Requests.

a) **POLICY—Restriction Requests.** We will allow an individual to request that we restrict our use or disclosure of his or her protected health information for treatment, payment, health care operations, or with specified family members or others. We have no obligation to agree to such request. We will comply, and notify our business associates to comply, with any such agreement we make (except in an appropriate medical emergency).

FORM—Restriction Requests. Use FORM 42–Restriction Request to document an individual's request to restrict use or disclosure of protected health information.

PROCEDURE—Restriction Requests. If you receive an individual's restriction request, complete or have the individual complete the first page of FORM 42–Restriction Request, then promptly transmit the entire FORM 42 to our Privacy Official. You must not tell the individual that we will or will not agree to the restriction request.

FORM—Restriction Response. The Restriction Request Processing page of FORM 42-Restriction Request is designed to coordinate the response to an individual's restriction request.

PROCEDURE—Restriction Response. Only our Privacy Official may agree to an individual's restriction request on our organization's behalf. Our Privacy Official will process each restriction request as follows:

- Track the processing of the restriction request on the Restriction Request Processing page of FORM 42.
- If we decline the restriction request, use the Denial of Restriction Request page of FORM 42 to notify the individual that we do not agree to the request.
- If we accept the restriction request, use the Agreement to Restriction Request page of FORM 42 to inform the individual that we have agreed to restriction, though the restriction agreement will not limit the individual's right of access to his or her protected health information, see **Section 14-Access**, prevent uses or disclosures for public interest or benefit activities, see **Section 4-Public Interest or Benefit Use or Disclosure,** or prevent uses or disclosures to health care providers if needed in a medical emergency for treatment of the individual.
- If we agree to the restriction, use the Notification of Restriction on Protected Health Information page of FORM 42 to notify affected agencies and business associates of their obligation to comply with the restriction.

- Have the completed FORM 42 included in the individual's records, and retain a copy for the Privacy Official file.

PROCEDURE—Agencies. The agency head, or designee, of each affected agency must ensure that the workforce members are informed of a restriction as specified on the Notification of Restriction on Protected Health Information from our Privacy Official, and implement procedures to prevent any use or disclosure contrary to any restriction agreement we make. Personnel of each agency must consult the agency head, or designee, or our Privacy Official before using or disclosing protected health information subject to a restriction agreement, if there is any question whether a particular use or disclosure may be contrary to that restriction agreement.

b) POLICY—Medical Emergency Exception. We may use restricted protected health information or disclose it to a health care provider, notwithstanding a restriction agreement, if the information is needed in a medical emergency for treatment of the individual who is the subject of our restriction agreement.

PROCEDURE—Medical Emergency. When requested to disclose restricted protected health information for treatment in a medical emergency of the individual who is the subject of our restriction agreement, you must:

- Exercise professional judgment to determine that a medical emergency exists that justifies using or disclosing the restricted protected health information.

- Document the basis for your determination, whether it resulted in using, disclosing or withholding the restricted protected health information.

- Send your documentation to our Privacy Official, and include a copy in the individual's records.

PROCEDURE—Disclosure Made in Medical Emergency. If you disclose restricted protected health information to a health care provider for treatment in a medical emergency of the individual who is the subject of our restriction agreement, you must:

- Ask the health care provider to not further use or disclose the restricted protected health information.

- Document your request, and send your documentation to our Privacy Official. Include a copy in the individual's records.

Our Privacy Official will follow up with the health care provider to document our request that there will be no further use or disclosure of the restricted protected health information.

c) **POLICY—Unenforceable Restrictions.** We will neither agree to, nor comply with, a restriction request to prevent (a) use or disclosure through our facility directories, see **Section 2(b)-Provider Facility Directories**, (b) use or disclosure for permitted public interest or benefit activities, see **Section 4-Public Interest or Benefit Use or Disclosure**, or (c) disclosure to HHS for compliance investigation or enforcement, see **Section 5-Required Disclosures**.

PROCEDURE—Unenforceable Restrictions. If we agree to a restriction request, our Privacy Official will inform the individual in writing that the restriction agreement cannot prevent uses or disclosures for public interest or benefit activities or disclosures to HHS for compliance investigation or enforcement.

PROCEDURE—Government Request for Restricted Protected Health Information. You must promptly notify our Privacy Official if you receive a request for restricted protected health information from HHS or another government agency or organization. Follow the direction of our Privacy Official regarding the response to such request.

d) **POLICY—Restriction Termination.** We may terminate a restriction agreement either (a) with the concurrence of the individual or (b) unilaterally by written notice of termination to the individual. When we terminate a restriction agreement unilaterally, we will continue to comply with the restriction with respect to protected health information we created or received subject to the restriction.

FORM—Restriction Termination. Use FORM 43–Restriction Termination to document termination of a restriction agreement, including any concurrence to the termination by the individual.

PROCEDURE—Restriction Termination. Only our Privacy Official may terminate a restriction agreement on our organization's behalf. If your agency wants to terminate a restriction agreement, complete the first page of FORM 43-Restriction Termination, and submit the entire FORM 43 to our Privacy Official. If our Privacy Official concurs that the restriction agreement should be terminated, our Privacy Official will do the following:

- Use the Notice of Termination of Restriction Agreement page of FORM 43 to notify the individual that we are terminating the restriction agreement, and to request that the individual concur in the termination.

- Use the Notification of Restriction Agreement Termination page of FORM 43 to inform the agency head, or designee, of affected agencies and business associates of the termination of the restriction agreement, with instruction whether the restriction will continue to apply to protected health information that was created and received subject to the restriction agreement.

- Have the completed FORM 43 included in the individual's records, and retain a copy for the Privacy Official file.

PROCEDURE—Agencies. If a restriction continues to apply to protected health information after termination of a restriction agreement, the agency head, or designee, of each affected agency must isolate that protected health information and ensure that workforce members continue to apply the restriction to that protected health information.

If a restriction ends with termination of the restriction agreement, the agency head, or designee, of each affected agency will instruct workforce members that the protected health information is no longer restricted and may accordingly be treated the same as other protected health information under these Privacy Policies and Procedures.

e) POLICY—Documentation. We must document, on paper or electronically, each restriction request received, our response, each restriction agreement made, each restriction agreement terminated, and any other documentation regarding our compliance with respect to restriction requests.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official each restriction request received, our response, each restriction agreement made, each restriction agreement terminated, and any other documentation regarding our compliance with respect to disclosure accounting. Our Privacy Official will retain this documentation until 6 years after the later of its creation or last effective date.

18. Confidential Communication.

a) POLICY—Confidential Communication. We will allow an individual to request confidential communications (that is, the use of alternative means or alternative locations when we communicate protected health information to the individual), if the request is reasonable and in writing.

NOTE: For District health care components which perform health plan functions the individual must also give us a clear statement that all or part of the protected health information could endanger the individual if not communicated by the requested alternative means or to the requested alternative location.

FORM—Confidential Communication Requests. Use FORM 44–Confidential Communication Request to document an individual's request that protected health information be communicated by alternative means or to an alternative location.

PROCEDURE—Confidential Communication Requests. If you receive an individual's request that we use alternative means or locations when communicating protected health information to the individual, complete or have the individual complete the first and second pages of FORM 44-Confidential

Communication Request, then promptly transmit the entire FORM 44 to our Privacy Official. You are not allowed to require an individual to explain the basis for requesting confidential communications, nor may you question the validity of the individual's representation that confidential communication is needed because of danger to the individual. You must not tell the individual that we will or will not accommodate the confidential communication request.

FORM—Confidential Communication Response. The Confidential Communication Request Processing page of FORM 44 is designed to coordinate the response to an individual's request for confidential communication.

PROCEDURE—Confidential Communication Response. Only our Privacy Official may approve a request for confidential communication of protected health information. Our Privacy Official will process each confidential communication request as follows:

- Track the processing of the confidential communication request on the Confidential Communication Request Processing page of FORM 44.

- Respond to the individual by means and location appropriate to the confidential communication request. Our Privacy Official will inform the individual whether we will accommodate the confidential communication request or whether the request cannot be accommodated without additional information.

- If the individual's request contains (a) a reasonable alternative address or means of contact, (b) a clear statement that all or part of the protected health information could endanger the individual if not communicated by the alternative means or at the alternative location, and (c) an explanation how any applicable premium payment, claim payment, or other payment related to the activities underlying the protected health information subject to the request will be handled, use the Accommodation of Confidential Communication Request page of FORM 44 to inform the individual that the request will be accommodated. The response must use the means or location appropriate to the confidential communication request.

- If we accommodate the confidential communication request, use the Notification of Confidential Communication Requirement page of FORM 44 to notify affected agencies and business associates of their obligation to comply with the confidential communication request.

- If the individual's request does not contain the requisite information listed above, use the Denial of Confidential Communication Request to inform the individual that we will not accommodate the confidential communication request without additional, specified information. The response must use the means or location appropriate to the confidential communication request.

- Have the completed FORM 44 included in the individual's records, and retain a copy for the Privacy Official file.

PROCEDURE—Agencies. The agency head, or designee, of each affected agency must ensure that the workforce members are informed of a confidential communication obligation, and that the agency communicates the protected health information subject to the confidential communication obligation to the individual only by the alternative means or at the alternative location specified in the Notification Confidential Communication Requirement from our Privacy Official. Personnel of each agency must consult the agency head, or designee, or our Privacy Official before making a communication of protected health information, if there is any question whether that communication should be treated as a confidential communication.

b) **POLICY—Minors.** State law that requires disclosure of minor's protected health information to a parent, guardian or person acting in loco parentis takes priority over a minor's request for confidential communication. See **Section 9– Personal Representatives**.

PROCEDURE—Minors. If you have any question whether communication of a minor's protected health information should be treated as a confidential communication, consult your agency head, or designee, or our Privacy Official before you make the communication.

c) **POLICY—Documentation.** We will retain, on paper or electronically, each request for confidential communication, our response, and all other documentation relating to our compliance with our obligations with respect to confidential communication requests until 6 years after the later of their receipt or last effective date.

PROCEDURE—Documentation. You must include in the individual's records and furnish our Privacy Official each request for confidential communication, our response, and any other documentation relating to our compliance with our obligations with respect to confidential communication requests. Our Privacy Official will retain this documentation until 6 years after the later of its receipt or last effective date.

V. ADMINISTRATIVE REQUIREMENTS

19. Privacy Policies and Procedures.

a) **POLICY—Adoption.** We will adopt and implement written privacy policies and procedures for protected health information designed to comply with our obligations under the Privacy Rules. These Privacy Policies and Procedures satisfy this obligation.

PROCEDURE—Implementation and Compliance. Each member of our workforce with access to protected health information must, at all times, comply with the policies and follow the procedures set out in these Privacy Policies and Procedures. Consult with the agency head, or designee, of your agency, or our Privacy Official before you use or disclose protected health information, if there is any doubt regarding whether such use or disclosure is permitted by these Privacy Policies and Procedures or by the Privacy Rules.

b) **POLICY—Revisions.** Only the appropriate senior officials of the District, with the advice and concurrence of our Privacy Official, may change these Privacy Policies and Procedures.

i) **Mandatory Revision.** We will promptly change these Privacy Policies and Procedures as necessary and appropriate to comply with each material change in the Privacy Rules or other applicable federal or state privacy law, and promptly implement the change.

We will promptly make appropriate revisions to our Privacy Practices Notice whenever the change in law materially affects the accuracy of the Notice content.

NOTE: District health care components that perform health plan functions must distribute our revised Notice to our enrollees within 60 days of the effective date of the change in law. See **Section 13(c)—Privacy Practices Notice Distribution**.

ii) **Elective Revision.** We may change our privacy practices at any time by amending these Privacy Policies and Procedures, provided they remain in compliance with the Privacy Rules and all other applicable federal and state privacy law.

If the change materially affects the content of our Privacy Practices Notice, we will make corresponding changes to our Notice. We will not implement the change in these Privacy Policies and Procedures until after the effective date of the revised Notice.

NOTE: District health care components that perform health plan functions must distribute our revised Notice to our enrollees within 60 days of the effective date of the change in law. See **Section 13(c)—Privacy Practices Notice Distribution**.

PROCEDURE—Reservation to Change Notice. Each Privacy Practices Notice we distribute must contain the statement that we reserve the right to change our Notice. That statement is mandatory if we are to be permitted to apply a material change in these Privacy Policies and Procedures to all protected health information without regard for when we created or received the protected health information. See **Section 13(b)—POLICY-Revision to Privacy Practices Notice**.

c) **POLICY—Documentation.** We must retain, on paper or electronically, each set of our Privacy Policies and Procedures, and all documentation reflecting each change in our Privacy Policies and Procedures and any corresponding change in our Privacy Practices Notices, until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must furnish our Privacy Official any documentation regarding changes in our Privacy Policies and Procedures and corresponding changes in our Privacy Practices Notices. Our Privacy Official will retain each set of our Privacy Policies and Procedures and all documentation reflecting changes in them and in our Privacy Practices Notices until 6 years after the later of their creation or last effective date.

20. Privacy Personnel, Training, Workforce Management, Administrative Practices.

a) POLICY—Privacy Personnel.

i) Privacy Official. Our Privacy Official is responsible for developing, maintaining, and implementing these Privacy Policies and Procedures, and for overseeing our full compliance with these Privacy Policies and Procedures, the Privacy Rules, and other applicable federal and state privacy law.

Our Privacy Official is Gerry Roth

Telephone: 202-727-8001

E–mail: gerry.roth@dc..gov

Office: 1350 Pennsylvania Ave, NW, Suite 307, Washington, DC 20004

Additionally each Agency will designate a Privacy Official who will be responsible for developing, maintaining, and implementing Privacy Policies and Procedures, and for overseeing our full compliance with both these and their Agency specific Privacy Policies and Procedures, the Privacy rules, and other applicable Federal and State privacy law(s). These individuals, following the guidance provided by the District's Privacy Official, will take the lead role in their agencies' privacy efforts.

PROCEDURE—Delegation. Our Privacy Official may delegate specific duties and responsibilities to designees with the documented concurrence of appropriate senior officials of the District.

ii) Contact Offices. We will maintain contact offices for individuals to obtain our Privacy Practices Notice and other information on our privacy practices. Our contact offices will also accept complaints about our privacy practices.

Our contact offices are:

To be determined

PROCEDURE—Contact Office Supervision. Our Privacy Official will supervise, direct, and control the operations of, and the personnel assigned to, our contact offices.

b) POLICY—Workforce Training. Each member of our workforce who may have access to or use of protected health information will receive training on our

Privacy Policies and Procedures, as necessary and appropriate for the member to carry out his or her job functions.

FORM—Training Log. FORM 52–Privacy Training Certificate is designed to document each workforce member's completion of privacy training.

PROCEDURE—Training Timing.

i) **Current Workforce.** Existing workforce must complete privacy training by April 14, 2003 (our Privacy Rules compliance date).

ii) **New Hires.** Newly hired members of our workforce must receive privacy training before they may have access to or use of protected health information.

iii) **Retraining.** Existing workforce members must receive retraining no later than 45 days after there is material change in their job functions or in our Privacy Policies and Procedures that affects their access to or use of protected health information.

PROCEDURE—Training Process. Our Privacy Official will be responsible for conducting the privacy training of our workforce, including determining the appropriate training content needed by particular trainees to carry out their job functions. The head of the District's Office of Personnel, or designee, will coordinate with our Privacy Official to schedule privacy training for our current workforce by our Privacy Rules compliance date, and of newly hired members of our workforce as promptly as practical, but before the new hires are given access to or use of protected health information.

The head of the District's Office of Personnel, or designee, will coordinate with our Privacy Official to schedule privacy retraining for existing workforce members as promptly as practical, but no later than 45 days after the material change in their job functions or our Privacy Policies and Procedures that affects their access to or use of protected health information.

PROCEDURE—Training Documentation. Our Privacy Official will document completion of training of each workforce member on our Privacy Policies and Procedures, using FORM 52–Privacy Training Certificate. The Privacy Official will send a copy of the completed FORM 52 to the head of the District's Office of Personnel, or designee, for inclusion in the personnel file of the workforce member trained.

c) **POLICY—Workforce Sanctions.** Workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law would subject the employee to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements.

PROCEDURE—Workforce Sanctions. Our Privacy Official will coordinate with the head of the District's Office of Personnel, or designee, to develop, document, and disseminate to the agency head, or designee, of each agency a list of sanctions (in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements) for workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law. The agency head, or designee, will disseminate this list of sanctions to each workforce member in their agencies.

PROCEDURE—Reporting Workforce Privacy Violations. Each member of our workforce is obligated to report promptly any suspected violation of our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law to the agency head, or designee, and our Privacy Official. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Official.

d) **POLICY—Mitigation.** We will have and implement contingency plans to mitigate any deleterious effect of an improper use or disclosure of protected health information by a member of our workforce or by our business associates.

PROCEDURE—Mitigation Implementation. Our Privacy Official will coordinate with the head of the District's Office of Personnel, or designee, to develop contingency plans to mitigate, to the extent possible, any deleterious effect of improper use or disclosure of protected health information by a member of our workforce or by our business associates in violation of these Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law. Each member of our workforce will cooperate fully with the mitigation efforts of our Privacy Official.

e) **POLICY—Retaliatory Acts.** We will not, and we will not tolerate any workforce member who attempts to, intimidate, threaten, coerce, discriminate or retaliate against an individual who:

- Exercises any right, including filing complaints, under the Privacy Rules or other privacy laws.
- Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.
- Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of protected health information).

PROCEDURE—Prevention of Retaliatory Acts. A member of our workforce who suspects that another workforce member has violated the ban on retaliatory acts must report the suspicion to our Privacy Official. Reports may be made

anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Official.

f) **POLICY—Waivers.** We will not require an individual to waive any right under the Privacy Rules, including the right to complain to HHS, as a condition of providing claims payment, enrollment or benefits eligibility to the individual.

PROCEDURE—Prevention of Waivers. A member of our workforce who suspects that another workforce member has violated this ban on waivers must report the suspicion to our Privacy Official. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Official.

g) **POLICY—Documentation and Record Retention.** We will retain the documentation required by our Privacy Policies and Procedures and the Privacy Rules until 6 years after the later of its creation or last effective date.

PROCEDURE—Document and Record Retention. Our Privacy Official will be our repository of documentation regarding our privacy practices and compliance with our Privacy Policies and Procedures and the Privacy Rules. Our Privacy Official will maintain in written or electronic form:

- Our Privacy Policies and Procedures and each revision of them. See **Section 19-Privacy Policies and Procedures**.
- Our Privacy Practices Notices, each revision of them, and all documentation relating to our distribution of them. See **Section 13-Privacy Practices Notice**.
- Each authorization and authorization revocation. See **Section 3-Authorization for Use or Disclosure**.
- Each request from individuals for access, amendment, disclosure accounting, restriction, or confidential communication, and all other documentation relating to our compliance with our obligations with respect to individuals' rights. See **Part IV-Individual's Information Rights**.
- Each complaint and any material generated as a result of investigating and resolving the complaint. See **Section 22-Complaints and HHS Enforcement**.
- Documentation evidencing designation of our Privacy Official and any delegation of duties and responsibilities to the Privacy Official's designees, designation of personnel and record sets, and designations with respect to covered entity structures. See **Section 12-Covered Entity Structures**, **Part IV-Individual's Information Rights**, and **Section 20(a)—POLICY-Privacy Personnel**.

- Documentation relating to personal representative relationships, business associate relationships, group health plan and plan sponsor relationships, limited data sets, and de-identified health information. See **Part II-Data Policies and Procedures** and **Part III-Relationship Policies and Procedures**.

- Documentation relating to compliance with informal permission for certain uses and disclosures. See **Section 2-Informal Permission for Certain Uses and Disclosures.**

- Documentation of workforce training and sanctions, mitigation plans, and other administrative requirements. See **Section 20-Privacy Personnel, Training, Workforce Management, Administrative Practices**.

- Other documentation requested or required under our Privacy Policies and Procedures or demonstrating our compliance with our obligations under the Privacy Rules.

PROCEDURES—Agencies. The agency head, or designee, of each agency will implement document retention practices consistent with these Privacy Policies and Procedures to ensure that our Privacy Official receives the original or exact duplicates of all documentation we are required to retain. The agency head, or designee, of each agency will include in individual records within their agency's custody the original or exact duplicate, as appropriate, of that documentation that these Privacy Policies and Procedures specify for inclusion in individual's records.

Each agency may retain a copy of documents as may meet the agency's needs or convenience in performing functions and duties for our organization. To avoid undue document storage expense and space, no agency should retain documents that have also been furnished to our Privacy Official for more than 6 years after their creation or last effective date.

21. Data Safeguards.

a) POLICY—Data Privacy Protection. The agencies, as defined by the District of Columbia's hybrid entity designation, which are covered by the HIPAA Privacy Rules, (CFR 160 and 164) are covered by the computing safeguards and associated District of Columbia standards for computing resource usage as described herein. The computer facilities and systems covered and associated to this policy are, but are not limited to, the computers, printers, networks, routers, and related computing equipment, as well as the associated data files, software programs and/or documents managed or maintained by a District and its designated cover entities. These Computing Safeguards apply to, and include, computer facilities, computer rooms, data wiring closets, telecommunication and data distribution areas, computer labs, offices, classrooms, and furnishings operated and maintained as computing resources by the District's agencies.

District of Columbia standards for computing resource usage

1. Each agency will determine the level of access to protected health information available via their computing resources for their workforce members.

2. No member of a agency's workforce shall knowingly damage or misuse computing equipment or the data accessed from that equipment.

3. Technical safeguards will be employed, where reasonable, at each of the agency's work areas in such a manner to promote the security of protected health information and to protect protected health information from the unauthorized access thereof.

4. Workforce member will utilize access to those computing devices assigned or designated for their use.

5. Workforce members shall utilize only their assigned or designated logons and passwords issued by the agency or the District.

6. Computer and computing resources users must observe intellectual property rights, including software copyright laws.

7. A user of the agency's computing resources shall not threaten or harass a member of the agency's workforce.

8. All use of the agency computing resources is subject to federal, state, and local law regarding the use of hardware, software, and associated materials.

b) POLICY-Faxing of Protected Health Information To ensure the security and confidentiality of protected health information utilized by the agencies of the District of Columbia, it is the policy when transmitting documents containing "PHI" via a facsimile machine or via a computer based facsimile device to observe and apply the necessary requirements of minimum necessary determination procedure. (Minimum Necessary Determination-- Procedure Section VII). All facsimile devices dealing with, either in the transmission or receipt of documents containing PHI should be out of public areas and secured in a private area within the operational facility of the agency. The process of generating, obtaining and transmitting a document or documents with PHI in them, shall be herein called *"faxing"*.

PROCEDURE -- Fax Cover Sheet -- When faxing information that is PHI or a document that contains PHI, you must fax a coversheet declaring that there is Protected Health Information attached within the transmission. The coversheet should indicate number of pages that is being transmitted, instructions on who to contact if the transmission is sent to the non-addressed party and a message to destroy the PHI document if not received by the party it was designated for. If an authorization is

required to be sent releasing the information to the recipient, then this also must be transmitted.

PROCEDURE—Agencies. The agency head, or designee, of each agency will implement our policies and procedures regarding the privacy, security, and integrity of protected health information. Any question regarding the meaning or application of any provision of these Privacy Policies and Procedures or any other policy and procedure we may adopt must be addressed to our Privacy Official before you act.

22. Complaints and HHS Enforcement.

a) POLICY—Complaints. We will timely investigate and appropriately respond to each written complaint received by our contact offices or a workforce member regarding our compliance with these Privacy Policies and Procedures or the Privacy Rules.

FORM—Complaints. Use FORM 53–Complaint to document each complaint received about compliance with our Privacy Policies and Procedures or the Privacy Rules.

PROCEDURE—Complaint Receipt. Complete, or have the complainant complete, the first and second pages of FORM 53–Complaint. Promptly transmit the entire FORM 53 to our Privacy Official. You must not tell the complainant what we will or will not do in response to the complaint.

FORM—Complaint Response. The Complaint Investigation and Processing page of FORM 53-Complaint is designed to coordinate the response to a complaint.

PROCEDURE—Complaint Response. Only our Privacy Official may respond to a complaint on our organization's behalf. Our Privacy Official will process a complaint as follows:

- Investigate the complaint, using the Complaint Investigation and Processing page of FORM 53 to document the investigation, findings, and conclusions.
- Use the Report on Complaint page of FORM 53 to notify the complainant of our resolution of the complaint.
- Institute appropriate action to correct the matters complained of, if corrective action is warranted.
- Mark any portion of FORM 53 that is subject to the attorney-client or attorney work product privilege as "privileged and confidential," send the completed FORM 53 to our Privacy Official.

PROCEDURE—Agencies. The agency head, or designee, of each agency must ensure the full and timely cooperation of agency workforce members with complaint investigation conducted by our Privacy Official regarding compliance with our Privacy Policies and Procedures or the Privacy Rules.

b) POLICY—HHS Enforcement and Compliance Cooperation. We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our organization. Our Privacy Official will keep sufficient non-privileged records of our compliance to be able to submit compliance reports in the time, manner, and with the information HHS requests to ascertain our compliance.

PROCEDURE—Compliance Cooperation. Our Privacy Official, will coordinate our response to any HHS compliance review, complaint investigation or other inquiry, to ensure that all applicable obligations of our organization are fulfilled and all applicable rights and privileges of our organization are preserved and protected.

Our Privacy Official, will arrange for HHS to have access to our facilities, books, records, accounts, and other non-privileged information sources (including protected health information without individual authorization or notice, see **Section 5-Required Disclosures**), during normal business hours (or at other times if HHS presents appropriate lawful administrative or judicial process).

Our Privacy Official, will endeavor to obtain non-privileged information required by HHS that is in the exclusive possession of our business associates, other agents, institutions or persons who fail or refuse to furnish the information directly to HHS.

PROCEDURE—Agencies. You must immediately notify our Privacy Official of any inquiry from HHS or any other government official. You must await instruction from our Privacy Official before responding to these inquiries or providing any documents or other information on behalf of our organization.

Do not obstruct or interfere with any lawful process, warrant, order or subpoena that may be presented. If the officials insist they have the right of immediate search and seizure of our organization's records, equipment or other matters specified in the process presented, do not obstruct or interfere with them. Instead, use your best efforts to contact our Privacy Official and to observe and document everything that the officials search, seize, say, and do.

PROCEDURE—Verification. You must verify the identity and authority of an HHS representative seeking protected health information before you may disclose the protected health information to the HHS representative. See **Section 25–Standard Procedure for Identity and Authority Verification**.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary the protected health information disclosed to HHS for complaint investigation or compliance enforcement or review.

PROCEDURE—Disclosure Log. You must log each disclosure to HHS for accounting. See **Section 27–Standard Procedure for Logging Disclosures for Accounting**.

VI. STATE LAW POLICIES AND PROCEDURES

23. State Privacy Law.

POLICY—State Law Compliance. We will comply with all state privacy laws to which our organization is subject that do not conflict with the Privacy Rules. We will comply with any state privacy law that conflicts with the Privacy Rules only if the state privacy law provides greater protections or rights to individuals or imposes greater protected health information use or disclosures restriction on us than do the Privacy Rules.

PROCEDURE—State Law Compliance. Only our Privacy Official may determine if a particular state law is applicable to our organization and, if so, whether it is preempted by the Privacy Rules. You must consult our Privacy Official if there is any question whether a particular state law or regulation, including any judicial or administrative interpretation of such state law or regulation, applies to protected health information or to your activities with respect to protected health information.

23A. Special Policies and Procedures Pertaining to Mental Health Information

The District of Columbia Mental Health Information Act of 1978 ("the MHIA") establishes special requirements for safeguarding the privacy of mental health information. Chapter 23A explains how those requirements differ from the standard HIPAA policies and procedures that generally govern privacy of protected health information.

Mental health information is any information in any form obtained by a mental health professional in attending a client in a professional capacity that identifies, or could be used to identify, the client, or that pertains to the diagnosis or treatment of the client's mental or emotional condition. The Mental Health Information Act prohibits mental health professionals, mental health facilities, and data collectors (defined below) from using or disclosing mental health information, except under the narrowly prescribed circumstances discussed in this chapter. The Act also places limitations on re-disclosure of mental health information, which apply to *any person or entity*. Be sure to consult your agency's Privacy Officer if you have any doubt about whether you are dealing with mental health information, whether a special policy or procedure applies to your situation, or what a particular rule means.

DEFINITIONS

The following definitions apply to the use and disclosure of mental health information as discussed in this chapter.

Administrative information means a client's name, age, sex, address, identifying number or numbers, dates and character of sessions (individual or group), and fees.

Authorization means a written form signed by an individual that authorizes the use or disclosure of the individual's protected mental health information (1) by Network providers for purposes other than the provision of mental health services or mental health supports, or (2) by persons or entities other than Network providers for any purpose, including the provision of mental health services or mental health supports.

Data collector means a person, other than the client, mental health professional and mental health facility who regularly engages, in whole or in part, in the practice of assembling or evaluating client mental health information.

Department of Mental Health ("DMH") means the District of Columbia Department of Mental Health, the successor in interest to the District of Columbia Commission on Mental Health Services. DMH as used herein encompasses the Mental Health Authority and two provider entities operated directly by DMH (the Public Core Services Agency and Saint Elizabeth's Hospital).

Joint consent means a written form signed by an individual that grants permission for participating Network providers to use and disclose protected mental health information in order to carry out the provision of mental health services or mental health supports.

Joint consent process means a process established by the Department of Mental Health to enable all participating Network providers to rely on a single form in which an individual consents to the use of his or her protected mental health information by Network providers for the purposes of delivering treatment, obtaining payment for services rendered, and performing certain administrative health care operations such as quality assurance, utilization review, accreditation, and oversight. The terms "treatment," "payment," and "health care operations," as used herein, encompass the meanings given them in the HIPAA implementing regulations (at 45 CFR § 164.501), as well as the phrase "provision of mental health services and mental health supports," used herein.

Mental health information means any written, recorded or oral information acquired by a mental health professional in attending an individual in a professional capacity which either (1) identifies, or could be used to identify, the individual, or (2) relates to the diagnosis or treatment of the individual's mental or emotional condition.

Mental health facility means any hospital, clinic, office, nursing home, infirmary, or similar entity where professional services are provided; and any individual or entity that is licensed or certified by, or has entered into an agreement with, DMH to provide mental health services or supports.

Mental health professional means any of the following persons engaged in the provision of professional services: (a) a person licensed to practice medicine; (b) a person licensed to practice psychology; (c) a licensed social worker; (d) a professional marriage, family, or child counselor; (e) a rape crisis or sexual abuse counselor who has undergone at least 40 hours of training and is under the supervision of a licensed social worker, nurse, psychiatrist, psychologist, or psychotherapist; (f) a licensed nurse who is a professional psychiatric nurse; or (g) any person reasonably believed by the client to be one of the foregoing persons.

Mental health provider or "MH provider" means (a) any individual or entity, public or private, that is licensed or certified by the DMH to provide mental health services or mental health supports; (b) any individual or entity, public or private, that has entered into an agreement with DMH to provide mental health services or mental health supports; and (c) DMH, including Saint Elizabeth's Hospital, the Public Core Services Agency and the Mental Health Authority.

Network means the District of Columbia Mental Health Provider Network, an organized health care arrangement created pursuant to sections 114 and 116(f) of the District of Columbia Department of Mental Health Establishment Amendment Act of 2001, effective December 18, 2001 (D.C. Law 14-56; D.C. Official Code §§ 7-1131.14(6) and 7-1201.01)(2001), and consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

Network Provider means a mental health provider that participates in the Network. Network providers utilize the joint consent process for authorization to use or disclose protected mental health information in carrying out the provision of mental health services or mental health supports.

Organized health care arrangement means an organized system of health care, such as the Network, in which more than one provider participates, and in which the participating providers hold themselves out to the public as participating in a joint arrangement, and either (1) participate in joint activities that include utilization review, in which health care decisions by participating providers are reviewed by other participating providers or by a third party on their behalf; or (2) participate in quality assessment and improvement activities, in which mental health services or mental health supports provided by participating providers are assessed by other participating providers or by a third party on their behalf.

Participating provider means Network Provider.

Personal notes means (1) mental health information disclosed to a mental health professional in confidence by other persons on condition that such information not be disclosed to the individual or other persons; and (2) the mental health professional's speculations.

The special policies and procedures in this chapter are supplementary to the policies and procedures contained in the other chapters. This means that, when requesting, using, disclosing, or otherwise dealing with mental health information, you should follow the policies and procedures discussed in the other chapters, except when there are separate policies or procedures set out in this chapter. For ease of reference, each special policy or procedure presented in this chapter is keyed to the corresponding policy or procedure that appears in the other chapters.

I. USE AND DISCLOSURE POLICIES AND PROCEDURES

1. Fundamental Policies on Use and Disclosure of Protected Health Information

1.b) i-v Treatment, Payment, Health Care Operations.

Within the District of Columbia Mental Health Provider Network ("the Network"), participating providers may use and may disclose mental health information to other participating providers for purposes of treatment, payment, and healthcare operations, but only to the minimum extent necessary, and only if the individual has authorized such use and disclosure by executing a joint consent.

Outside the Network, mental health information may be used and disclosed only if (1) the individual has executed an authorization specific to the intended use or disclosure (see Chapter 3 as modified by the corresponding section below), or (2) one of the conditions described in Chapter 4 (as modified by the corresponding section below) applies. In addition, employees may disclose mental health information to other employees within the same mental health facility to the minimum extent necessary to facilitate the delivery of professional services to the individual.

vi) Fundraising for Our Organization.

Since our organization does not engage in fundraising, this section does not apply to us.

vii) Underwriting and Other Insurance Function Health Care Operations.

We may not use mental health information for this purpose without the individual's authorization.

1.d) Incidental Use and Disclosure.

Incidental use and disclosure of mental health information is not permitted.

2. Informal Permission for Certain Uses and Disclosures.

We may not use or disclose mental health information pursuant to informal permission. The uses and disclosures described in this section can only be made pursuant to the individual's written authorization.

3. Authorization for Use or Disclosure.

3.a) Authorization

With respect to mental health information, the only exceptions to the requirement that we have written authorization from the individual before each use or disclosure of protected mental health information are (1) when we are using or disclosing information for the provision of mental health services or supports within the Network pursuant to a joint consent executed by the individual, and (2) when one of the circumstances exists which are enumerated in Chapter 4, as modified by the corresponding section below.

FORMS - Authorization Any written authorization for the use or disclosure of mental health information must meet the following requirements. The authorization must:

(1) Specify the nature of the information to be disclosed, the type of persons authorized to disclose such information, to whom the information may be disclosed and the specific purposes for which the information may be used both at the time of the disclosure and at any time in the future;

(2) Advise the individual of the right to access his or her record of mental health information;

(3) State that the consent is subject to revocation, except where an authorization is executed in connection with a client's obtaining a life or non-cancelable or guaranteed renewable health insurance policy, in which case the authorization shall be specific as to its expiration date which shall not exceed 2 years from the date of the policy; or where an authorization is executed in connection with the client's obtaining any other form of health insurance, in which case the authorization shall be specific as to its expiration date which shall not exceed 1 year from the date of the policy;

(4) Be signed by the person or persons authorizing the disclosure; and

(5) Contain the date upon which the authorization was signed and the date on which the authorization will expire, which shall be no longer than 60 days from the date of authorization.

PROCEDURE - Copies of the authorization must be (1) provided to the individual and the person authorizing the disclosure; (2) included along with the disclosure; and (3) placed in the individual’s record of mental health information.

3.b) Marketing.

Since our organization does not engage in marketing, this section does not apply to us.

3.c) Fundraising for Others.

Since our organization does not engage in fundraising for others, this section does not apply to us.

3.d) Psychotherapy Notes.

Psychotherapy notes may be disclosed under the circumstances described in section 3.a. above, with the exception of those psychotherapy notes that constitute personal notes made by the mental health professional. Personal notes are defined as (1) mental health information disclosed to the mental health professional in confidence by other persons on condition that such information not be disclosed to the individual or other persons; and (2) the mental health professional's speculations. Personal notes can never be disclosed, with or without authorization, except in litigation brought by the individual against the mental health professional alleging malpractice or wrongful disclosure of mental health information. As a precaution, psychotherapy notes and personal notes must be maintained separately from an individual's main record of mental health information so as to avoid their incidental disclosure in connection with an otherwise valid disclosure of the record.

4. Public Interest or Benefit Use and Disclosures

4.a) Public Interest or Benefit Use and Disclosure

The circumstances under which mental health information may be used or disclosed without authorization for public health, public interest, public benefit, and law enforcement activities are generally much narrower than for other protected health information, and are limited to the specific circumstances described in the following subsections:

4.b) [Reserved]

Collection of fees: A mental health professional or mental health facility may disclose the administrative information necessary for the collection of fees from an individual if the individual or the individual's representative has received written notification that the fee is due and has failed to arrange for payment within a reasonable time after such notification.

4.c) Public Health Activities

We may disclose without authorization only the minimum mental health information necessary to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety.

4.d) Public Health and Safety Threats

Mental health information may be disclosed on an emergency basis to one or more of the following: an individual's spouse, parent, legal guardian, a duly accredited officer or agent of the District of Columbia in charge of public health, the Department of Mental Health, an individual or entity that is licensed or certified by, or has entered into an agreement with, DMH to provide mental health services or supports, an officer authorized to make arrests in the District of Columbia, or an intended victim if a mental health professional reasonably believes that the disclosure is necessary to initiate emergency psychiatric

hospitalization of the individual pursuant to D.C. Code § 21-521 or to otherwise protect the individual or another person from a substantial risk of imminent and serious physical injury.

Mental health information disclosed to the Metropolitan Police Department pursuant to this provision will be maintained separate and apart from any permanent police record. MPD will refrain from further disclosing the information except as a court-related disclosure under section 4.k. below. Upon the expiration of any applicable statute of limitations, if no court proceeding is pending, MPD will destroy the information. If a court action is pending, MPD will destroy the information at the termination of the judicial action.

4.e) Provider's Treatment Activities for Workplace Health and Safety

We may not disclose mental health information to an employer for this purpose without the individual's authorization.

4.f) Worker's Compensation

We may not disclose mental health information for this purpose without the individual's authorization.

4.g) Deaths

We may not disclose mental health information for this purpose without the authorization of a personal representative as defined in Chapter 9, as modified by the corresponding section below.

4.h) Organ Donation

We may not disclose mental health information for this purpose without the individual's authorization.

4.i) Required by Law

We may disclose without authorization the minimum mental health information necessary to meet the requirements of D.C. Official Code § 21-586 (concerning financial responsibility for the care of hospitalized persons) and to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety.

4.j) Health Oversight Activities

We may disclose to qualified personnel the minimum mental health information necessary to carry out management audits, financial audits, or program evaluation of a mental health professional or mental health facility, provided that such personnel have demonstrated and provided assurances, in writing, of their ability to comply with all applicable federal and District privacy laws, including the

requirement that they avoid revealing, directly or indirectly, the identity of any individual whose information they receive.

4.k) Judicial and Administrative Proceedings

We may disclose the minimum necessary mental health information in a civil or administrative proceeding in which the individual, or the individual's representative or, in the case of a deceased person, any party claiming or defending through, or a beneficiary of, the individual, initiates his mental or emotional condition or any aspect thereof as an element of the claim or defense.

In litigation for the collection of fees, no mental health information other than administrative information shall be disclosed, except to the extent necessary (1) to respond to a motion of the individual or the individual's representative for greater specificity; or (2) to dispute a defense or counterclaim.

i) Order. We may disclose mental health information in response to a judicial or administrative order, provided we disclose only the expressly ordered information.

ii) Process. We may not disclose mental health information in response to a subpoena or other process unless either the individual has executed an authorization or a judge has authorized the disclosure in writing after the individual has received notice and an opportunity to be heard on the question of disclosure.

4.l) Law Enforcement

i.) - vii.) We may not disclose mental health information to a law enforcement officer without the individual's authorization under the circumstances enumerated in Chapter 4, Section l., unless otherwise expressly authorized by one of the subsections contained in this section.

4.m) Adult Abuse, Neglect, Domestic Violence

We may disclose the minimum necessary mental health information for this purpose if required to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety.

4.n) Child Abuse or Neglect

We may disclose the minimum necessary mental health information for this purpose only if required to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety.

4.o) Research

We may disclose the minimum necessary mental health information for research provided the requirements in Chapter 4, section o., and subsection 4.j above are satisfied.

4.p) Inmates and Others in Lawful Custody

We may not disclose mental health information for this purpose without the individual's authorization.

4.q) Government Personnel, Programs, and National Security

We may not disclose mental health information for this purpose without the individual's authorization.

II. DATA POLICIES AND PROCEDURES

7. Limited Data Set

We may use and disclose limited data sets as described in Chapter 7 (1) for health care operations if the individuals whose mental health information is affected have executed joint consents, or (2) for research, or public health purposes, if one of the public interest or benefit conditions described in Chapter 4, as modified by section 4 above, exists.

III. RELATIONSHIP RULES

9. Personal Representatives

9.c) Personal representatives of Adults and Emancipated Minors

For purposes of authorizing use of, disclosure of, or access to, mental health information, a personal representative may be a person specifically authorized by the individual in writing, or by a court, as the legal representative of the individual, or a person otherwise authorized by law to make health care decisions on behalf of the individual.

9.d) Personal Representatives of Unemancipated Minors

The Mental Health Information Act provides that use and disclosure of mental health information must be authorized by both the minor and the minor's parent or legal guardian in the case of a minor between ages 18 and 14, absent the circumstances enumerated in Chapter 9, Section d.iv. For minors 14 years of age or less, disclosures may be authorized as provided in Chapter 9, Section d. The Act also provides that access (within the meaning of Chapter 14) to a minor's

mental health information may be authorized by the minor or by a person specifically authorized by the minor in writing, or by a court, as the legal representative of the minor. Otherwise, access may be authorized as provided in Chapter 9, Section d.

11. Group Health Plans and Plan Sponsors.

This section does not apply to our operations.

IV. INDIVIDUAL'S INFORMATION RIGHTS

13. Privacy Practices Notice

The provisions of Chapter 13 apply to the Department of Mental Health only in its capacity as a participating provider in the District of Columbia Mental Health Network, the organized health care arrangement created specifically to allow for the use of a joint consent process. Accordingly, Chapter 13, sections (b) through (e), should guide the actions of DMH employees with respect to privacy practices notice. The application of Chapter 13 to employees of other District agencies depends on what use the agency makes of mental health information. You should consult with your agency's Privacy Officer for guidance regarding privacy practices notice.

14. Access

14.a) Right to Inspect and Copy.

We will respond to all requests for access to mental health information within thirty days of receipt of the written request without exception, including providing the requesting party either with photocopies or the opportunity to inspect and photocopy the requested information.

A mental health professional, responsible for the diagnosis or treatment of the individual, shall have the opportunity to discuss the mental health information with the individual at the time of such inspection. In the case of a request for access directed to a data collector, the data collector may grant access directly to the requestor or indirectly by providing the requested information to a mental health professional designated by the requestor. If the mental health professional designated by the requestor is not the person who disclosed the information to the data collector, he or she shall be in substantially the same or greater professional class as the professional who disclosed the information to the data collector.

14.b) Protected Health Information We May Withhold.

i). Denial of Access without Right of Review. Only personal notes may be withheld without right of review.

ii) Denial of Copies to Inmates. We may not withhold access to mental health information from inmates unless the criteria in the next subsection are satisfied.

iii) Denial of Access to Dangerous Information. A mental health professional or mental health facility may limit the disclosure of portions of an individual's record of mental health information to the individual only if the mental health professional primarily responsible for the diagnosis or treatment of such individual reasonably believes that such limitation is necessary to protect the individual from a substantial risk of imminent psychological impairment or to protect the individual or another person from a substantial risk of imminent and serious physical injury. The mental health professional shall notify the individual in writing of any denial of access, whether the denial is in whole or in part.

Procedure - Review of Access Denial for Endangerment. The individual may designate an independent mental health professional who shall be permitted to review the individual's record of mental health information. The independent professional shall be in substantially the same or greater professional class as the mental health professional who initially limited disclosure. The independent professional shall permit the individual to inspect and duplicate those portions of the individual's record of mental health information which, in his or her judgment, do not pose a substantial risk of imminent psychological impairment to the individual or pose a substantial risk of imminent and serious physical injury to the individual or another person. In the event that the independent mental health professional allows the individual to inspect and duplicate additional portions of the individual's record of mental health information, the mental health professional primarily responsible for the diagnosis or treatment of the individual shall have the opportunity to discuss the information with the individual at the time of transmittal, examination or duplication of information.

The individual may bring a lawsuit in the Superior Court within six months of being denied access if the independent mental health professional denies access in whole or in part, or if the individual is indigent and is unable to obtain the services of an independent mental health professional. In such a lawsuit, the mental health professional will have the burden of proving by a preponderance of the evidence that the denial of access was appropriate.

16. Disclosure Accounting

16.c) Accounting Information.

In addition to the requirements in Chapter 16, for each disclosure of mental health information, we must make a notation in the individual's record of mental health information regarding (1) the date of the disclosure, (2) the name

of the recipient, and (3) the contents of the disclosure. For disclosures made pursuant to an individual's authorization, a copy of the authorization must be placed in the individual's record of mental health information.

In addition, with the exception of disclosures made on an emergency basis as provided in subsection 4.d above, every disclosure of mental health information must be accompanied by a statement to the effect that "the unauthorized disclosure of mental health information violates the provisions of the District of Columbia Mental Health Information Act of 1978. Disclosures may only be made pursuant to a valid authorization by the client or as provided in title III or IV of that Act. The Act provides for civil damages and criminal penalties for violations."

16.d) Temporary Accounting Suspension

With respect to disclosures of mental health information, we may not suspend logging of disclosures or accounting for disclosures under any circumstances.

V. ADMINISTRATIVE REQUIREMENTS

20. Privacy Personnel, Training, Workforce Management, Administrative Practices

20.c) Workforce Sanctions

In addition to the workplace sanctions mentioned in Chapter 20, section c., there are potential civil and criminal penalties for violation of the Mental Health Information Act. Anyone who negligently violates the MHIA could be held liable for any monetary damages sustained by the individual plus court costs and attorney's fees. For a willful or intentional violation, the MHIA establishes a minimum damages award of $ 1,000.

A willful violation also constitutes a misdemeanor punishable by a fine of up to $1,000 or imprisonment for up to 60 days, or both. Obtaining mental health information from a mental health professional, mental health facility or data collector under false pretenses is also a misdemeanor, punishable by a fine of up to $ 5,000 or imprisonment of up to 90 days, or both.

27. STANDARD PROCEDURE - Logging Disclosures for Accounting

See Chapter 16, as modified by Section 16 above, for special requirements pertaining to logging disclosures of mental health information.

24. [RESERVED—Rules Modification]

VII. STANDARD PROCEDURES

25. STANDARD PROCEDURE—Identity and Authority Verification.

FORM—Verification of Identity and Authority. Use FORM 9–Identity and Authority Verification to document how you verify the identity and authority of any person, unknown to you, requesting protected health information.

PROCEDURE—Verification of Identity and Authority. Obtain appropriate identification and, if the person is not the individual who is the subject of the protected health information sought, evidence of authority. If you question whether you have obtained sufficient verification, consult our Privacy Official before you make any disclosure.

a) Evidence of Identification. Examples of appropriate identification include:

- Photographic identification card.
- Government identification card or badge.
- Appropriate document on government letterhead.

If a person purports to be acting on behalf of a public official, appropriate identification includes, if reasonable for the situation:

- A written statement of appointment on appropriate government letterhead.
- A contract, memorandum of understanding, purchase order or other evidence establishing the appointment to act on behalf of the public official.

b) Evidence of Authority. Examples of appropriate authority include, if reasonable for the situation:

- Identification as parent, guardian, or person acting in loco parentis with respect to minors; executor or administrator with respect to a deceased individual or an estate; power of attorney or other evidence of legal authority to act on behalf of an individual with respect to health care; or other evidence of appropriate relationship with the individual with respect to health care.
- A warrant, subpoena, order or other legal process issued by a grand jury, a court, or an administrative tribunal.
- A written statement of legal authority or, with respect to a properly identified government official, an oral statement of authority, if reliance on such oral statement is reasonable for the situation. You must document the oral statement on FORM 9.

DOCUMENTATION. Complete FORM 9-Identity and Authority Verification for each disclosure to document how you fulfilled our obligation to verify identity and authority. Include the completed FORM 9 in the individual's records and send a copy to our Privacy Official.

26. STANDARD PROCEDURE—Minimum Necessary Determination. You must make reasonable efforts to use, disclose, and request of a covered entity only the minimum necessary protected health information to accomplish the intended purpose. See **Section 6-Minimum Necessary.** If you question whether a use, disclosure or request you are about to make complies with the minimum necessary limitation, consult our Privacy Official before you make the use, disclosure or request.

FORM—Minimum Necessary Determination. Use FORM 10–Disclosure Log/Minimum Necessary to document your compliance with the minimum necessary limitation.

PROCEDURE—Minimum Necessary Determination.

a) Reliance on Requester. We may rely, if reasonable under the circumstances, on a request to disclose protected health information to be for the minimum necessary if the requester is:

- A covered entity.
- A professional (such as an attorney or accountant) who provides professional services to our organization, either as a member of our workforce or as our business associate, and represents that the requested information is the minimum necessary.
- A public official who represents that the information requested is the minimum necessary.
- A researcher who presents appropriate documentation or makes appropriate representations that the research satisfies the applicable requirements of the Privacy Rules. See **Section 4(o)—Research**.

We will not disclose protected health information requested by others until our Privacy Official has confirmed that we are not required to make a minimum necessary determination because of the character and representation of the requester. If you have question about relying on a request being for the minimum necessary, consult your agency head, or designee, or our Privacy Official before you make the disclosure.

- Use FORM 10–Disclosure Log/Minimum Necessary to document that no minimum necessary determination was required because you are permitted to rely on the requester.

- Include the completed FORM 10 in the individual's records. Send a copy to our Privacy Official.

b) **Making the Minimum Necessary Determination.** In all situations where we must make the minimum necessary determination, you must follow these procedures:

i) **Routine or Recurring Disclosures and Requests.** You may follow our standard protocols applicable to a particular routine or recurring disclosure of or request for protected health information. If you question whether a particular disclosure or request should be subject to our standard protocols, consult your agency head, or designee, or our Privacy Official before you make the disclosure or request.

- Use FORM 10–Disclosure Log/Minimum Necessary to document your minimum necessary determination based on application of the appropriate standard protocols.

- Include the completed FORM 10 in the individual's records. Send a copy to our Privacy Official.

ii) **Non–Routine and Non–Recurring Disclosures or Requests.** You must not disclose or request protected health information for a non–routine and non–recurring purpose until you review the situation on an individual basis against our criteria to ensure that only the minimum necessary protected health information for the purpose is disclosed or requested. If you question whether a particular disclosure or request should be subject to an individual review (rather than treated as routine or recurring) or how to conduct the individual review based on our criteria, consult your agency head, or designee, or our Privacy Official.

- If you are empowered or instructed by our Privacy Official to make the minimum necessary determination for a non–routine and non–recurring disclosure or request, use FORM 10–Disclosure Log/Minimum Necessary to document that your determination is in accordance with our criteria, and to document the disclosure. Include the completed FORM 10 in the individual's records, and send a copy to our Privacy Official.

- Otherwise, refer each non–routine and non–recurring disclosure of or request for protected health information to our Privacy Official for an individual review against our criteria to ensure that only the minimum necessary protected health information for the purpose is disclosed or requested.

c) **Entire Medical Record.** When an entire medical record is to be used, disclosed or requested, you must:

- Determine on an individual basis whether the situation justifies using, disclosing or requesting an entire medical record as the minimum necessary protected health information for the purpose.

- Use FORM 10–Disclosure Log/Minimum Necessary to document the justification.

- Send completed FORM 10 to our Privacy Official to obtain approval before you use, disclose or request an entire medical record. If you receive approval, you may then use, disclose or request the entire medical record. Document the disclosure on FORM 10–Disclosure Log/Minimum Necessary. Include the completed FORM 10 in the individual's records. Send a copy to our Privacy Official.

Minimum Necessary Determination Checklist

{This is a suggested checklist for your workforce to use to make minimum necessary determinations. Section D should be modified to list the criteria appropriate for your organization to make individual determinations of minimum necessary in particular situations.}

Instructions: If you cannot check a box in **Section A, B** or **C** below, you must apply the criteria in **Section D** to determine whether the disclosure or request is for the minimum necessary protected health information to accomplish the purpose.

Section A—Minimum Necessary Not Applicable

The disclosure or request is not subject to the minimum necessary limitation because:

☐ It involves a health care provider for purposes of treatment.

☐ It involves the individual who is the subject of the information or the individual's personal representative.

☐ It involves an authorization by an individual who is the subject of the information or the individual's personal representative.

☐ It involves HHS for complaint investigation or compliance enforcement or review.

☐ It is required by law.

☐ It is required for compliance with the HIPAA Administrative Simplification Rules.

Section B—Reliance on Requester

We can rely on the request to be for the minimum necessary because the request is from one of the following and such reliance is reasonable under the circumstances:

☐ A covered entity or a business associate of a covered entity.

☐ A professional who is member of our workforce or is our business associate providing professional services to us, and who represents that the requested information is the minimum necessary.

☐ A public official who represents that the requested information is the minimum necessary.

☐ A researcher who presents appropriate documentation or representation for the research.

Section C—Routine or Recurring Disclosure or Request

☐ The disclosure or request is routine or recurring, as listed on our standard protocol tables. The disclosure or request must be for no more than the protected health information indicated by the appropriate standard protocol on the applicable table.

Section D—Individual Determination

The disclosure or request must meet our criteria for minimum necessary as determined by the following **{substitute the list of criteria appropriate for your organization}**:

☐ Ascertain the purpose of the disclosure or request.

☐ Identify the particular protected health information to be disclosed or requested.

☐ Determine whether the particular protected health information is reasonably related to the purpose for the disclosure or request.

☐ Review the categories of protected health information established in our standard protocols for routine or recurring disclosures and requests, to determine the classifications and groupings of protected health information used by our organization for compliance with the minimum necessary limitation.

☐ Determine which of our categories of protected health information can reasonably be expected to satisfy the purpose of the disclosure or request. Disclose no more than the protected health information contained in the least inclusive of those categories.

☐ Determine whether the purpose of the disclosure or request can be accomplished with de-identified health information. If it can, then we may disclose or request only de-identified health information.

TABLE 1

MINIMUM NECESSARY USE OF PROTECTED HEALTH INFORMATION BY WORKFORCE MEMBERS

{Job Category—As examples:}	{DATA TYPE—Demographic Data}	{DATA TYPE—Medical History}	{DATA TYPE}	{DATA TYPE}	{DATA TYPE—Full Medical Record}
Admitting					
Billing					
Employed Physician					

{This table is provided as a suggested format for developing standard protocols for minimum necessary use by your workforce. See Section 6(b)—Workforce Use.}

{Various categories of workforce members who may need access to or use of protected health information to perform their job functions should be specified in the left–hand column (examples are listed for illustration). Various categories of protected health information to which particular workforce members may need to do their jobs should be specified across the top (examples are listed for illustration).}

{Where access should be provided routinely, the cell in the table should so indicate. Where access should be provided in certain circumstances only, the cell should specify those circumstances. Note that the Privacy Rules require that use of an entire medical record must be specifically justified.}

TABLE 2

MINIMUM NECESSARY DETERMINATION FOR PROTECTED HEALTH INFORMATION DISCLOSURES AND REQUESTS

{Disclosures/ Requests— As examples:}	{DATA TYPE— Demographic Data}	{DATA TYPE— Medical History}	{DATA TYPE}	{DATA TYPE}	{DATA TYPE—Full Medical Record}
Admitting					
Billing					
Peer Review					
Fraud Detection					
Employee Grievance					

{This table is provided as a suggested format for developing standard protocols for your organization's minimum necessary disclosures and requests. See Section 6(c)-Routine or Recurring Disclosures or Requests.}

{Various categories of business processes for which your organization may disclose or request protected health information should be specified in the left–hand column (examples are listed for illustration). Various categories of protected health information which may be needed for the particular business processes should be specified across the top (examples are listed for illustration).}

{Where disclosures or requests may be routine or recurring, the cell in the table should so indicate. Where disclosures or requests should be made in certain circumstances only, the cell should specify those circumstances. Note that the Privacy Rules require that disclosure of or request for an entire medical record must be specifically justified.}

27. **STANDARD PROCEDURE—Logging Disclosures for Accounting.** You must record each disclosure (whether oral or in writing) for which we are obligated to account upon an individual's request for disclosure accounting. See **Section 16-Disclosure Accounting**. If you question whether a particular disclosure needs to be recorded for disclosure accounting, see the list below for "types of disclosures which require logging", if you are still uncertain whether a disclosure should be logged consult your Privacy Official.

Types of disclosures which require logging for accounting:

1. Disclosures required by law
2. Disclosures for public health activities
3. Disclosures for FDA adverse event reporting
4. When the disclosure is to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation;
5. Disclosures to an employer about an individual who is a member of the workforce of the employer for certain work-related illnesses or injuries, or a workplace-related medical surveillance;
6. Disclosures to a government authority about victims of abuse, neglect or domestic violence
7. Disclosures for health oversight activities
8. Disclosures for judicial and administrative proceedings
9. Disclosures for law enforcement purposes
    a. as required by law including laws that require the reporting of certain types of wounds or other physical injuries
    b. pursuant to a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer
    c. a grand jury subpoena
10. Disclosures to law enforcement officials of limited information for identification and location purposes, the covered entity may disclose only the following information:
    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 and time of treatment
    g. Date and time of death, if applicable
    h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos
    i. PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue may not be disclosed
11. Disclosure of information in response to a law enforcement official's request regarding victims of a crime

12. A covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct
13. A covered entity may disclose to a law enforcement official PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity
14. When reporting to law enforcement official about a crime in emergency situations
15. Disclosures about decedents
    a. A covered entity may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law
    b. A covered entity may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties
16. Disclosures for cadaveric organ, eye or tissue donation purposes
17. Disclosures for research purposes
    a. only in circumstances when there is a *waiver*, in whole or in part, of the individual authorization required by Section I, 3, "Authorizations for Use and Disclosure"
18. Disclosures to avert a serious threat to health or safety
19. Disclosures for specialized government functions
    a. A covered entity may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities
    b. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the PHI of an individual who is a member of the Armed Forces upon the separation or discharge
    c. A covered entity may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority
    d. To Protective Services for the President and others.
    e. A covered entity that is a component of the Department of State may use PHI to make medical suitability determinations
    f. Covered entities that are government programs providing public benefits
20. Disclosures for workers' compensation
21. Disclosures for fundraising that are permitted without an authorization of the individual

FORM—Logging Disclosures. Use FORM 10–Disclosure Log/Minimum Necessary to document each accountable disclosure you make so that we may have a log of accountable disclosures to fulfill our disclosure accounting obligations.

PROCEDURE—Logging Disclosures.

- Document each accountable disclosure on FORM 10–Disclosure Log/Minimum Necessary by completing the Disclosure Log section.

- Include the completed FORM 10 in the individual's records. Send a copy to our Privacy Official.

Judy D. Banks
Interim Director of Personnel