HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

* HIPAA *

PRIVACY IMPLEMENTATION HANDBOOK

PENNSYLVANIA DEPARTMENT OF PUBLIC WELFARE

Revised September 2013

TABLE OF CONTENTS

APPENDICES

NOTE: Appendix A is a mandatory form for business associates. Appendix B is the preferred form for written authorizations. Appendices C-H are optional forms that the individual may use; however, the individual may write a letter/request instead of using the standard forms contained in Appendices C-H of this Handbook. If the individual uses an authorization other than the one in Appendix B, it must comply with all applicable requirements, including those set forth in the Privacy Rule and other privacy/confidentiality laws, and approved by the Departments's privacy office/the Department's legal office. Because many written authorizations do not meet all applicable requirements, program offices should inform those seeking disclosures requiring written authorization to use the Department's approved form.

1.0 OVERVIEW

The federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, as revised, set forth national requirements and standards for the privacy and security of protected health information (PHI).

HIPAA/HITECH privacy regulations (as amended), also known as the "privacy rule" apply to covered entities and their business associates. Covered entities include health care plans, health care clearinghouses and health care providers that transmit any health information in electronic form. Business associates are individuals and entities performing duties on behalf of a covered entity if those duties involve the creation, receipt, maintenance, use, or disclosure of PHI. A health care clearinghouse is a public or private entity that processes or facilitates the processing of health information from another entity into standard data elements or a standard transaction, or receives a standard transaction from another entity and processes it into nonstandard data for the receiving entity. A health care plan is an individual or group plan that provides, or pays for the cost of medical care. A health care provider is any person or organization that furnishes, bills or is paid for health care in the ordinary course of business. The electronic transmission requirement applies only to health care providers. The Department of Public Welfare clearly performs functions as a health care plan and in some contexts, as a health care provider.

Generally, the privacy regulations prohibit the use or disclosure of PHI except in accordance with the regulations. The regulations define and limit the circumstances under which covered entities may use or disclose PHI to others. Permissible uses and disclosures under the regulations generally include three categories:

1. Use and disclosure for treatment, payment or health care operations.
2. Use and disclosure requiring individual authorization.
3. Use and disclosure not requiring authorization for specified purposes.

These terms will be further defined and clarified in this Handbook.

The HIPAA privacy regulations require the Department to take certain actions, including:

1. Appoint a privacy officer/establish a privacy office.
2. Develop minimum necessary use/disclosure policies including appropriate procedures to obtain consent or authorization for releases of personal health information.

3. Draft and execute business associate agreements.
4. Develop an accounting of disclosures capability.
5. Develop a procedure to request alternative means of communication.
6. Develop a procedure to request restricted use.
7. Develop a complaint procedure.
8. Develop an amendment request procedure.
9. Develop an access, inspection and copying procedure.
10. Develop an anti-retaliation policy.
11. Train the workforce.
12. Develop and disseminate a notice of privacy practices.

1.1 Purpose of Handbook

The Department developed this handbook to specify Departmental policies and procedures to ensure compliance with HIPAA/HITECH privacy regulations, as amended. For additional guidance on confidentiality policies and procedures for specific program areas, please consult the relevant program office(s) for any bulletins, handbooks, memoranda, etc. on those subjects.

2.0 DEFINITIONS

Authorization. A document signed and dated by the individual who authorizes use and disclosure of their PHI for reasons other than treatment, payment or health care operations or other purpose not requiring written authorization. The authorization must contain a description of the PHI, the names or class of persons permitted to make a disclosure, the names or class of persons to whom the covered entity may disclose, an expiration date or event, an explanation of the individual's right to revoke and how to revoke, and a statement about potential redisclosures.

Breach. The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted and that compromises the security or privacy of the PHI.

Business associate. A person or entity who, on behalf of a covered entity or an organized health care arrangement, performs or assists in the performance of one of the following:

1. 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.

2. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for such covered entity or organized health care arrangement.

Business associate agreement. A contract between a covered entity and a business associate that does all of the following:

1. Establishes the permitted and required uses and disclosures of personal health information (PHI) by the business associate.

2. Provides that the business associate will use protected health information only as permitted by the contract or as required by law, use appropriate safeguards, report any disclosures not permitted by the contract, ensure that agents to whom it provides PHI will abide by the same restrictions and conditions, make PHI available to individuals and make its record available to U.S. Department of Health and Human Services.

3. Authorizes termination of the contract by the Department if the Department determines that there has been a violation of the contract.

The business associate agreement is usually part of a contract made in the procurement process, but can also stand alone or be part of a memorandum of understanding, grant agreement or other document.

CMS. Centers for Medicare & Medical Assistance Services within the United States Department of Health and Human Services.

COMPASS Community Partner. An organization, service provider or community service group, such as a hospital, clinic or long-term care facility that assists individuals applying for human services through COMPASS.

Compliance date. The date by which a covered entity must comply with a standard, implementation specification, requirement or modification specified in this handbook.

Consent. A document signed and dated by the individual that a covered entity may obtain prior to using or disclosing PHI to carry out treatment, payment or health care operations. A consent is not required under the privacy rule.

Covered entity. A health care provider who transmits any health information in electronic form in connection with a transaction covered by the privacy rule; a health care plan or a health care clearinghouse.

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

DHHS. The United States Department of Health and Human Services.

Department. The Pennsylvania Department of Public Welfare.

Designated record set. The medical records and billing records, including electronic records, about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health care plan; or medical records and billing records used by or for the covered entity to make decisions about individuals.

Disclosure. The release, transfer, provision of access to or divulging of information outside the entity holding the information.

Health care. Care, services and supplies related to the health of an individual. Health care includes, but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, mental health or palliative care and sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health care clearinghouse. A public or private entity that does either of the following:

1. Processes 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 health information into nonstandard format or nonstandard data content for the receiving entity.

Health care plan. An individual or group plan that provides, or pays the cost of, medical care. Health care plan includes:

1. A group health care plan (created pursuant to the Employee Retirement Income Security Act of 1974 [ERISA]).

2. A health insurance issuer.

3. An HMO.

4. Part A or Part B of the Medicare program.

5. The Medical Assistance program.

6. An issuer of a Medicare supplemental policy.

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

8. An employee welfare benefit plan.

9. The health care program for active military personnel.

10. The veterans' health care program.

11. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS).

12. The Indian Health Service program under the Indian Health Care Improvement Act.

13. The Federal Employees Health Benefits Program.

14. An approved State child health care plan.

15. The Medicare+Choice program.

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

17. Any other individual or group plan.

Health care provider. A provider of services and any other person or organization who furnishes, bills or is paid for health care in the normal course of business and who transmits any health information in electronic form in connection with a covered function.

Health information. Any information, including genetic information, whether oral or recorded in any form or medium, that does both of the following:

1. Is created or received by a health care provider, health care plan, public health authority, employer, life insurer, school or university or health care clearinghouse.

2. Relates to the physical or mental health or condition of an individual, the provision of health care to an individual or payment for the provision of health care to an individual.

For purposes of implementing the privacy rule, the Department of Public Welfare intends to treat all client information as health information and afford them the corresponding privacy protection.

Health maintenance organization (HMO). A federally qualified HMO and an organization recognized as an HMO under State law.

Health care operations. Health care operations include any of the following activities:

1. Conducting quality assessment and quality improvement activities.

2. Reviewing the competence or qualifications of health care professionals.

3. Evaluating practitioner and provider performance, health care plan performance and conducting training programs of non-health care professionals, accreditation, certification, licensing or credentialing activities.

4. 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.

5. Conducting or arranging for medical review, legal services and auditing functions including fraud and abuse detection and compliance programs.

6. 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.

7. Business management and general administrative activities of the entity.

Health oversight agency. An agency or authority of the United States, Pennsylvania or a political subdivision of a state, or a person or entity acting under a grant of authority from such public agency that is authorized by law to

oversee the health care system 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.

Individual. The person who is the subject of PHI.

Individually identifiable health information. Health information, including demographic (such as names, addresses, telephone numbers, etc. See Section 19.2 relating to document privacy and security policy) information collected from an individual that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify an individual.

For purposes of implementing the privacy rule, the Department of Public Welfare intends to treat all individual records (including electronic records) as if they were health information and afford them the corresponding privacy protection.

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

Law enforcement official. An officer or employee of any agency or authority of the United States, Pennsylvania or a political subdivision of a state who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, and to prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

Marketing. (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct

or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Notice of privacy practices. A notice to the individual of the uses and disclosures of PHI and the individual's rights and the covered entity's legal duties with respect to PHI.

Organized health care arrangement. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider or an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities.

Personal representative. A person authorized by law to act on behalf of an individual. The representative will be treated as the individual for purposes of disclosure of PHI.

Privacy rule. The Federal privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended, and related federal law regarding the confidentiality of PHI.

Protected health information (PHI). Individually identifiable health information that is maintained or transmitted in any form or medium. PHI excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA). It excludes information regarding a person who has been deceased for more than 50 years, although such information is usually safeguarded under other applicable law (for example, Medicaid confidentiality provisions, 55 Pa. Code Chapter 105),

For purposes of implementing the privacy rule, the Department intends to treat all individual records, including electronic records, as if they were health information and afford them the corresponding privacy protection.

Psychotherapy notes. Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, 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. An agency or authority of the United States, Pennsylvania, a political subdivision of a State or a person or entity acting under a grant of authority from or contract with such public agency that is responsible for public health matters as part of its official mandate.

Privacy office. The Department's privacy office.

Program office coordinator. The program office's privacy/client information coordinator.

Research. A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to general knowledge.

Subcontractor. A person to whom a business associate delegates a function, activity, or service, other than as in the capacity of a member of the workforce of such business associate.

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

Use. 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.

3.0 PRIVACY OFFICIALS

3.1 Purpose

Covered entities must designate a privacy official to help develop and implement privacy policies and procedures to assure compliance with the privacy rule. See 45 CFR § 164.530(a)(1).

3.2 Policy

The Department's privacy office assists the Department in activities related to the development, implementation, maintenance of and adherence to the Department's policies and procedures covering the use and access to, PHI in compliance with Federal and state laws and regulations.

3.3 Privacy Office Responsibilities

The role of the privacy office is to:

1. Provide guidance and assist in the identification, development, implementation and maintenance of information privacy policies and procedures in coordination with the administration (Commonwealth and Department), program office privacy coordinators and the Department's Bureau of Informations Systems/Security Officer.

2. Provide advice regarding risk assessments and ongoing compliance activities.

3. Work with program offices to help ensure that the Department has and maintains appropriate privacy authorization forms, privacy notices and materials reflecting current policies and procedures.

4. Provide advice on privacy materials for Department employees with access to PHI.

5. Provide advice to program offices on privacy issues pertaining to contractors, business associates and other appropriate third parties.

6. Participate in the development of business associate agreements.

7. Assist BIS staff as they establish a mechanism to track disclosures of PHI.

8. Work cooperatively with individual program offices regarding client rights to inspect, amend and restrict access to PHI, when appropriate.

9. Help establish a process for receiving, documenting, tracking, investigating and taking action, when appropriate, on complaints concerning the Department's privacy policies and procedures.

10. Help ensure compliance with privacy practices and provide advice regarding sanctions for failure to comply with privacy policies for employees in the Department's workforce, in cooperation with Human Resources.

11. Help to foster information privacy awareness within the Department and business associates.

12. Where necessary, serve as a liaison to business associates.

13. Where appropriate, assist the Department's Security Officer in reviewing information security plans throughout the organization's network to ensure alignment between security and privacy practices, and act as a liaison to the Department's BIS.

14. Advise Department employees involved with release of PHI.

15. Monitor changes in applicable federal and state privacy laws.

16. Work with clients and client advocates to refine the Department's policies and procedures.

17. Cooperate with the U.S. Department of Health and Human Services (DHHS), Office for Civil Rights (OCR), and Department auditors in any appropriate compliance review or investigation.

3.4 Program Office Privacy Coordinator

All program offices must appoint a Privacy/Client Information Coordinator (program office coordinator). The program office coordinator (or designee) is responsible for the following:

1. Assure program office compliance with this handbook.

2. Manage and document initial and ongoing privacy training for all program office employees (including contracted personnel).

3. Manage and monitor the business associate agreements.

4. Manage the tracking of disclosures through the use of the Disclosure Tracking System.

5. Conduct ongoing compliance monitoring activities.

6. Provide evaluation and other data upon request.

7. Participate in program office coordinator meetings.

8. Contact the Department's BIS (specifically, the Department's Security Officer), who will in turn contact the Privacy Office/the Department's legal office, to report suspected breaches of PHI. Working with the Department's Security Office and privacy office/legal office, the program office privacy coordinator (or designee) will promptly coordinate a fact-finding investigation of all relevant facts, submit that report to the Security Officer and implement the Security Officer's decisions on next steps, which include breach notification where necessary.

4.0 MINIMUM NECESSARY STANDARD

4.1 Purpose

The Department must restrict access and use of PHI to the minimum necessary to accomplish the intended purpose of the disclosure. See 45 CFR § 164.502(b).

4.2 Policy

1. The Department will determine electronic and manual access to PHI by the scope and responsibilities of an employee's position.

2. General rule: With a few exceptions (see Section 4.3), use and disclosure of PHI is limited to the minimum necessary to meet the purpose of the disclosure.

3. The Department will not use, disclose or request an entire medical record except when the entire medical record is necessary to accomplish the purpose of the use, disclosure, or request.

4.3 Exceptions to the Minimum Necessary Standard

The following are exceptions to the "minimum necessary" standard:

1. Disclosures to or requests by a health care provider for treatment.
2. Disclosures made to the individual.
3. Disclosures made under authorizations requested by the individual.
4. Disclosures made to the Secretary of DHHS that are related to the compliance and enforcement of the administrative simplification provisions of HIPAA.
5. Uses and disclosures that are required by law or court order so long as any restrictions provided by law are complied with.

4.4 Procedure

1. The program office will determine whether a use or disclosure is limited to the amount of PHI necessary to achieve the purpose of the use or disclosure.
2. When necessary, the program office will request guidance from the privacy office.

5.0 USE AND DISCLOSURE

5.1 Purpose

Circumstances under which a covered entity, including the Department, may use or disclose PHI are specified at 45 CFR §§ 164.502 through 164.512.

5.2 Policy

The Department will limit uses and disclosures to those permitted or required by the relevant privacy provisions and other applicable law. Although HIPAA may not require written consent or authorization for a particular use or disclosure of PHI, other laws may require oral or written permission. For example, although HIPAA sometimes permits disclosure of PHI pursuant to subpoena, state law does not (see, for example, 55 Pa. Code Chapter 105 relating to Safeguarding Information). Moreover, the law governing drug and alcohol, HIV and mental health information is often more protective of an individual's privacy and must be kept in mind when determining if the individual must first sign or otherwise authorize release of his or her PHI prior to its use or disclosure. Some laws may

prohibit disclosure despite written authorization. For example, with narrow exception involving long term care, genetic information may not be used or disclosed for insurance underwriting purposes.

5.3 Permitted Uses and Disclosures

Under the privacy rule, there are 5 general types of permitted uses and disclosures:

1. When the disclosure is to the individual who is the subject of the PHI—or to the individual's personal representative.

2. When the use or disclosure is to carry out treatment, payment or health care operations (no consent to release information is necessary).

3. When the Department receives a valid authorization (for example, Appendix B) for releases that are for other than treatment, payment or health care operations. The Department also recognizes authorizations of other organizations. If it is unclear whether an authorization meets all HIPAA requirements, please contact the privacy office/Department's legal office. If an individual is unable to physically sign an authorization, but can evidence their agreement, the authorization may be signed by two witnesses who evidence the assent.

4. Where the Department is using the information for a facility directory or sharing information with a relative, close friend or other person identified by the individual. In these circumstances, the individual must explicitly agree (via written authorization or orally) or have the opportunity to object. The ability to agree or object is not necessary if the situation is an emergency or the individual lacks the capacity to agree or object.

5. Where the uses and disclosures do not require authorization or an opportunity to agree or object. See Section 5.5 (relating to uses and disclosures that do not require HIPAA authorization).

5.4 Required Accounting of Disclosures

An accounting of disclosures is required under the following circumstances:

1. When an individual requests an accounting of the disclosures of his/her PHI or when he/she asks to inspect and/or copy his/her PHI.

2. When PHI is requested by the Secretary of the DHHS to investigate or determine the covered entity's compliance with the privacy standard.

5.5 Uses and Disclosures that Do Not Require HIPAA Authorization

The following uses and disclosures do not require an authorization or an opportunity to agree or object (but may require permission to release the information pursuant to other laws):

1. Uses and disclosures for treatment, payment or healthcare operations. Treatment includes the provision, coordination or management of health care and related services, including the coordination or management of health care by a health care provider with a third party and consultation between health care providers relating to a patient. For example, a covered entity could disclose a portion of a minor's PHI to a foster parent if that disclosure was necessary to coordinate the provision of medical care to the minor by the covered entity and the foster parent.

2. Uses and disclosures required by law.

3. Uses and disclosures for public health activities (for example, cancer and trauma registries, the FDA, etc.), if approved by the privacy office/the Department's legal office.

4. Disclosures about victims of abuse, neglect or domestic violence that are required by law.

5. Uses and disclosures for health oversight activities authorized by law (for example, disclosures to CMS) if approved by the privacy office/the Department's legal office.

6. Disclosures for judicial and administrative proceedings pursuant to a court order, if approved by the privacy office/the Department's legal office.

7. Disclosures for judicial and administrative proceedings pursuant to a subpoena (in some circumstances), if approved by the privacy office/the Department's legal office.

8. Disclosures for law enforcement purposes (for example, disclosure of a cash assistance recipient's current address to a police officer if the recipient is a fugitive felon), if approved by the privacy office/the Department's legal office.

9. Uses and disclosures about decedents to coroners, medical examiners and funeral directors, if approved by the privacy office/the Department's legal office.

10. Uses and disclosures for cadaveric organ, eye or tissue donation, if approved by the privacy office/the Department's legal office.

11. Uses and disclosures to avert a serious threat to health or safety (for example, disclosures of information relating to suspected terrorist activity.), if approved by the privacy office/the Department's legal office

12. Uses and disclosures for specialized government functions, including military and veterans activities, if approved by the privacy office/the Department's legal office.

13. Disclosures for workers' compensation, if approved by the privacy office/the Department's legal office.

If it is unclear whether a use or disclosure requires an authorization or opportunity to agree or object, the program office should seek clarification from the program office coordinator, and if necessary, the program office coordinator should contact the privacy office/the Department's legal office before using or disclosing the information.

5.6 De-Identification of Information

Health information that does not identify an individual, and to which there is no "reasonable basis" to believe that information can be used to identify any individual, is not subject to the privacy rule and may be disclosed.

There are two mechanisms under which a covered entity may determine that health information is not individually identifiable:

1. A person with appropriate knowledge and experience, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines and documents that the risk is negligible that the information (either alone or in combination with other reasonably available information) could be used to identify an individual.

2. The following 18 identifiers are removed regarding the individual, relatives, employers, or household members:

    a. Names.
    b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geocodes, except for the initial three digits of a zip code if, according to current Census data:
        - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and,

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

c. All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
d. Telephone numbers.
e. Fax numbers.
f. Electronic mail addresses.
g. Social Security numbers.
h. Medical record numbers.
i. Health care plan beneficiary numbers.
j. Account numbers.
k. Certificate/license numbers.
l. Vehicle identifiers and serial numbers, including license plate numbers.
m. Device identifiers and serial numbers.
n. Web Universal Resource Locator (URL).
o. Internet protocol (IP) address number.
p. Biometric identifiers, including finger or voice prints.
q. Full face photographic images and any comparable images.
r. Any other unique identifying number, characteristic or code.

In addition, the Department must be assured that the information could not be used alone or in combination with other information to identify an individual who is the subject of the information.

5.7 Verification Requirements

1. The privacy rule requires that, prior to any disclosure (whether for treatment, payment or health care operation, pursuant to an authorization or other permissible disclosure), a covered entity verify the identity of the person requesting PHI and the authority of that person to have access to the PHI.

2. If the person requesting PHI is a public official, the Department may rely upon the following to verify their identity:

   a. Presentation of an agency identification badge, credentials or other proof of status.

b. Requests made on governmental letterhead.
c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding or purchase order, that establishes that the person is acting on behalf of the public official.

3. If the person requesting PHI is a public official, the Department may rely upon the following to verify their authority.

   a. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.

   b. If a request is made pursuant to legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

4. These verification requirements are met if the Department "relies on the exercise of professional judgment" in making a use or disclosure, or acts on a good faith belief in making the disclosure regarding serious threats to health or safety.

5.8 Disclosures to Legislative Offices

1. Disclosure of PHI to Legislative Offices require a valid authorization (Appendix B), signed by the individual. The authorization form also requires special written authorization for the release of HIV and substance abuse and mental health information (See Appendix B).

2. Requests from a legislative office may:

   a. Come directly from legislative staff to the program office. The program office must require legislative staff to acquire the signed authorization from the individual prior to releasing PHI.

   b. Come directly to the Department's Office of Legislative Affairs. In this instance, the Office of Legislative Affairs (OLA) must require legislative staff to acquire the signed authorization from the individual prior to releasing PHI.

3. The program office may share requested information with OLA staff performing their duties.

5.9 Disclosures to Advocates, COMPASS Community Partners and Providers

1. Disclosure of PHI to advocates (who are not COMPASS community partners or acting on behalf of a health care provider) require a valid authorization (Appendix B) signed by the individual, unless Department staff knows that the advocate is currently representing the client and disclosure is for the purpose of administering public assistance (payment or program operations). The authorization form requires special permission for the release of HIV, substance abuse and mental health information.

2. The Department also recognizes authorizations of other organizations. If it is unclear whether an authorization meets all HIPAA requirements, please contact the privacy office/legal office.

3. Disclosures of PHI to community partners or representatives acting on behalf of a health provider do not require specific authorization if these disclosures are for treatment, payment or healthcare operations.

4. Disclosures of PHI to advocates pursuant to a court order do not require authorization.

5.10 Disclosures Involving Marketing or Sale of PHI

1. With some exceptions, PHI may not be used or disclosed for marketing activities. Permissible marketing activities generally require written authorization. Consult with the privacy office/the Department's legal office to determine if such use or disclosure is permissible and if it requires authorization.

2. Generally, the Department may not receive remuneration in exchange for a permissible use or disclosure of PHI. Consult with the privacy office to determine if and to what extent use or disclosure involving remuneration is permissible.

5.11 Knowledge of Violation

Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

5.12 Breaches Involving PHI

1. Acquisition, access, use, or disclosure of protected health information in a manner not permitted under the privacy rules, as amended, is presumed to be a breach unless the Department or its business associate, whichever applies, demonstrates that there is a low probability that PHI has been compromised, based on a risk assessment of at least the following four factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.

2. For breaches of PHI, the Department (or business associate pursuant to business associate agreement) must provide notification of the breach to affected individuals, the DHHS Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

    a. Individual Notice

    Breach notification to affected individuals must be in writing by first-class mail, or by e-mail if the affected individual has agreed to receive such notices electronically. If the Department/business associate (whichever applies) has insufficient or out-of-date contact information for 10 or more individuals, substitute individual notice is required, either by posting the notice on the Department's/business associate's web site (whichever applies) or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the Department/business associate has insufficient or out-of-date contact information for fewer than 10 individuals, the Department/business associate may provide substitute notice by an alternative form of written, telephone, or other means.

    These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm,

and prevent further breaches, as well as contact information for the covered entity. For substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact to determine if their PHI was involved in the breach.

b. Media Notice

For breaches affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, the Department/business associate is required to provide notice to prominent media outlets serving the state or local area. Such notification will likely be provided in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

c. Notice to the DHHS Secretary

In addition to notifying affected individuals and the media (where appropriate), the Department//business associate must notify the DHHS Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the DHHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, the Department/business associate must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the Department/business associate may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

3. The Department's Security Officer is responsible for handling the Department's breach notifications.

6.0 BUSINESS ASSOCIATES

6.1 Purpose

In order to disclose PHI to a business associate, a program office must receive satisfactory assurance that the business associate will appropriately safeguard the information. Under the privacy rule, satisfactory assurances must be obtained in a contract or other written agreement. See 45 CFR § 164.502(e)(1). The Department's legal office has developed a Business Associate Agreement that all program offices must use, which is updated and available on the Department's web site. Program offices may adapt the agreement to meet their needs and the needs of their business associates with prior approval of the adapted language from the privacy office/the Department legal office. (See Appendix A).

6.2 Policy

Program offices will review the relationships between the Department and the individuals and entities it deals with to determine when it is necessary and appropriate to execute a business associate agreement. If questions arise, the program office will contact the privacy office.

6.3 Satisfactory Assurances

The satisfactory assurance requirement does not apply to:

1. Disclosures made to a provider for treatment.

2. Disclosures made to a plan sponsor.

3. Uses by and disclosures to a government agency that determines enrollment or eligibility for Medical Assistance or another public benefit program if such activity is authorized by law.

6.4 Business Associate Requirements

The business associate language establishes permitted and required uses and disclosures and requires the business associate to follow privacy and security requirements. Those requirements include:

1. Use or disclose information only as permitted by law, regulation or agreement/contract.

2. Appropriately safeguard the PHI.

3. Report any misuse of PHI.

4. Secure satisfactory assurances from any subcontractor.

5. Grant individuals access and ability to amend their PHI.

6. Make an accounting of disclosures available to individuals.

7. Release applicable records to the DHHS Secretary if requested.

8. Upon termination, return or destroy all protected health information.

9. Report any knowledge of a violation or potential violation of this policy to the contract manager or program office coordinator.

10. Meet all federal and state requirements that directly apply to business associates, as well as all requirements that apply under the terms of the specific business associate agreement.

Note: The Business Associate Agreement must authorize termination if the business associate violates its terms.

6.5 Program Office Responsibilities

1. Program offices, with support from procurement staff, must identify their business associates, what information they receive, for what purpose the information is received and how that information will be used. If the business associate is also a governmental entity, a memorandum of agreement may provide satisfactory assurances.

2. Program offices must maintain updated lists of their business associates.

3. The program office is responsible for identifying contracts or other arrangements that must be created or modified (amended or appended to) to incorporate the Business Associate Agreement (Appendix A). If necessary, the program office coordinator will request guidance from the privacy office.

4. The program office must use the standard Business Associate Agreement (Appendix A) except where the privacy office approves otherwise.

5. If necessary, the program office may adapt Appendix A to meet its needs and the needs of its business associates, with prior approval of the privacy office.

6. Report any knowledge of a violation or potential violation of this policy to the program office coordinator.

7.0 ACCOUNTING OF DISCLOSURES

7.1 Purpose

Individuals have a right to receive an accounting of various instances when PHI about them is disclosed by a covered entity. See 45 CFR § 164.528. The Department has developed general policies and procedures to address the accounting of instances when PHI has been used or disclosed for purposes other than treatment, payment, health care operations or pursuant to an individual authorization.

7.2 Policy

1. The Department will allow individuals to receive an accounting of instances where PHI about them is used or disclosed, except:

    a. To carry out treatment, payment and health care operations.
    b. To the individuals of PHI about themselves.
    c. For a facility's directory.
    d. For notification of persons involved in the individual's care.
    e. For national security or intelligence purposes.
    f. To correctional institutions or law enforcement custodial situations.
    g. To comply with an individual authorization.

2. The Department will provide an accounting that includes disclosures that:

    a. Are required by law.
    b. Are made pursuant to public health activities or oversight (for example, to CMS).

c. Involve the reporting of communicable diseases.
d. Involve the reporting of Adverse Drug events.
e. Are made to certain registries (for example, Trauma, Cancer, Birth Defects).
f. Involve the reporting of abuse, neglect or domestic violence.
g. Are made pursuant to judicial or administrative proceeding, including subpoena.
h. Are made for law enforcement activities, excluding custodial situations (for example, disclosures about a fugitive felon.)
i. Are made to a coroner/medical examiner or funeral director.
j. Are made to avert serious threats to health or safety (for example, suspected terrorist activities.)
k. Are made to business associates and are not for treatment, payment or healthcare operations.

3. The Department will not provide an accounting of instances where PHI about individuals is used or disclosed prior to April 14, 2003.

4. The program offices must use the HIPAA Disclosure Tracking System (DTS), a specified Department-wide database for documenting and maintaining an accounting of when individuals' PHI has been disclosed for purposes other than treatment, payment or health care operations or other circumstances specified in 7.2 (relating to policy).

    a. The program office must designate staff persons to input disclosures into the HIPAA Disclosure Tracking System (DTS).
    b. Program office staff persons must enter data into the DTS within 5 working days of the disclosure.
    c. The program office must maintain an up-to-date listing of DTS Users and regularly update the User list for the DTS.
    d. The requests for an accounting will be processed by the program office.
    e. If questions arise, the program office will contact the privacy office

7.3 Procedure

1. The program office must train its program office users on the proper use and access to the HIPAA Disclosure Tracking System.

2. The Department must allow an individual to obtain an accounting of instances when his/her PHI has been disclosed for the purposes specified in 7.2 (relating to policy).

3. The Department must allow an individual to receive an accounting of disclosures of PHI made by the Department in the six years prior to the date on which the accounting is requested, but not prior to April 14, 2003. A Request for Accounting of Disclosures form is attached at Appendix C.

4. Each accounting of a disclosure must include the following:

    a. The date of disclosure.
    b. The name of the entity or person who received the PHI and, if known, the address of such entity or person.
    c. A brief description of the PHI disclosed.
    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the request for disclosure.

5. The program office will act on the individual's request for an accounting not later than 60 days after receipt of the request by:

    a. Providing the individual with the accounting requested, or
    b. Extending the time to provide the accounting by no more than 30 days.

6. In the event that the program office extends the time to provide the accounting, within 60 days after receipt of the request, the program office will provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting. The program office may have only one extension.

7. The program office handling the accounting will document and retain all of the following for a period of at least 6 years, or from the date of its creation or the date when it last was in effect, whichever is later:

    a. The information required to be included in an accounting.
    b. The written accounting that is provided to the individual.
    c. The title of the persons or office responsible for receiving and processing requests for an accounting by the individual.

8. The program office must provide the first accounting to an individual in any 12 month period for free. For each subsequent request for an accounting by the same individual within the 12 month period, the Department may impose a reasonable, cost-based fee provided that the Department informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

9. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

8.0 ALTERNATIVE MEANS OF COMMUNICATION

8.1 Purpose

The individual may request to receive communications regarding his/her PHI by an alternative means or location. See 45 CFR § 164.522(b)(1).

8.2 Policy

1. Where the Department acts as a health care provider, the Department will take necessary steps to accommodate reasonable requests by an individual to receive confidential communications of PHI by alternative means.

2. Where the Department acts as a health care plan, the Department will provide confidential communications by alternative means or at alternative locations when the disclosure of all or part of that information could endanger the individual.

8.3 Procedure

1. The Department requires an individual seeking confidential communication to make the request in writing. A Request for Alternative Means or Location of Communication form is attached at Appendix D.

2. Where the Department acts as a health care provider, the Department will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

For circumstances where the Department acts as a health care plan, the request for confidential communication of PHI will clearly state that the disclosure of all or part of that information could endanger the individual. If the individual does not include this explanation in the initial request, the Department will contact the individual and offer the individual an opportunity to provide a statement that the disclosure could endanger the individual, if accurate.

3. If reasonable, an alternative means or location will be designated before communication of PHI is made.

4. The program office, using professional judgment and considering all relevant factors, in consultation with the individual will be responsible for deciding the alternative means or location to communicate PHI to an individual (for example, use of P.O. Box instead of street address or requesting communications via E-mail.)

5. Once it is determined an alternative is appropriate, authorized Department personnel will access the individual's PHI using proper access and authorization procedures.

6. If a request for alternate means or location is granted, the requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by persons who do not have appropriate access clearance to that information.

7. Department personnel will appropriately document the request and delivery of the PHI.

8. The program office will consult with the privacy office about any questions or concerns.

Knowledge of a violation or potential violation of this policy must be reported directly to the appropriate program office coordinator.

9.0 REQUESTING RESTRICTIONS ON USES AND DISCLOSURES

9.1 Purpose

An individual has the right to request restrictions to the use and disclosure of his/her PHI. See 45 CFR § 164.522(a). If the program office agrees to the requested restrictions, it may not make uses or disclosures that are inconsistent with such restrictions, unless such uses or disclosures are

mandated by law. This provision does not apply to health care provided to an individual on an emergency basis.

9.2 Policy

The Department will allow an individual to request that uses and disclosures of his/her PHI be restricted. The Department will agree to reasonable, advisable and feasible restrictions. Except as otherwise required by law, the Department must grant the individual's request to restrict disclosure to a health plan if the purpose of disclosure is not for treatment and the medical services to which the request applies have been paid out-of-pocket in full.

9.3 Procedure

1. The Department will allow an individual to request to restrict the use and disclosure of PHI. A Request for Restrictions on the Use and Disclosure of Protected Health Information form is attached at Appendix E.

2. Upon agreeing to such a restriction, the Department will not violate such restriction, except when the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment. The Department will request the emergency health care provider to not further use or disclose the information.

3. If the Department agrees to an individual's requested restriction, the restriction does not apply to the following uses and disclosures:

    a. To an individual accessing his/her own protected health information.
    b. To an individual requesting an accounting of his/her own PHI.
    c. Facility directories.
    d. Instances for which an authorization, or opportunity to agree or object is not required. Unless otherwise required by law, the Department must, however, grant the individual's request to restrict disclosure to a health plan if the purpose of disclosure is not for treatment and the medical services to which the request applies have been paid out-of-pocket in full.

4. The Department may terminate its agreement to a restriction in the following situations:

a. The individual agrees to or requests the termination in writing.
b. The individual orally agrees to the termination and the oral agreement is documented.
c. Unless it is required to comply with the individual's request for restriction, if the Department informs the individual that it is terminating the agreement to a restriction. Such termination is only effective with respect to PHI created or received after informing the individual of the termination.

5. The Department will document the restriction and related documentation and retain that documentation for at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

6. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

10.0 COMPLAINT PROCEDURES

10.1 Purpose

Covered entities will provide a process for individuals to make complaints to the covered entity concerning its privacy policies and procedures, its compliance with those policies and procedures, or its compliance with the privacy rule itself. The covered entity is also required to document all complaints received and their disposition. See 45 CFR § 164.530(d).

10.2 Policy

The complaint process gives an individual an opportunity for review of decisions, actions or failures to act that impact privacy rights and helps the Department to identify policies and procedures that are unfair, wrong or not in agreement with the law.

10.3 Filing a Complaint

1. A statement informing individuals of the process to complain about violations of the Department's privacy policies and procedures is contained in the privacy notice that the individual receives upon enrollment in a program. The privacy notice is available in English and Spanish on the Department's website.

2. The complaint must be filed within 180 days of when the individual knew or should have known that the act or failure to act occurred.

3. The individual should submit the complaint to the privacy office describing the act or failure to act that adversely affects the individual's privacy rights. The individual must submit the complaint in writing or electronic format. A sample complaint form is attached at Appendix F. Use of this form is not required.

4. The individual may also file a complaint with the United States Department of Health and Human Services, Office for Civil Rights. See Section 10.7 (relating to complaints to DHHS, enforcement and penalties).

10.4 Program Office Responsibilities

1. Upon request, the program office will assist the individual with filing the complaint.

2. The program office may not limit or interfere with the right to make a complaint in any way.

3. If the individual submits a complaint to the program office coordinator, the program office coordinator must immediately forward the complaint to the privacy office.

4. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

5. At the privacy office's request and direction, the program office will investigate the allegations in the individual's complaint, make findings of fact based on the circumstances surrounding the complaint and convey all pertinent information to the privacy officer. After conferring with the privacy office, the program office will document whether and what corrective steps are necessary.

10.5 Privacy Office Responsibilities

1. The privacy office will work with the program office during the course of the investigation, assist in making findings of fact based on the circumstances surrounding the complaint, and in coordination with the program office, document whether and what corrective steps are necessary.

2. The privacy office will work with the program office to determine the outcome of the investigation and disposition of the complaint within 90 days of receipt of the complaint.

3. The privacy office will retain a copy of the final disposition and will keep a log of all complaints it receives and their current disposition.

4. The privacy office will send (or request that the program office send) a copy of the final disposition to the individual.

5. The final determination is binding on the program office.

10.6 Individual's Right to Appeal

1. The individual may file appeals to the Department of Public Welfare, Bureau of Hearings and Appeals, 2330 Vartan Way 2nd Floor, Harrisburg, PA 17110 or complain directly to the DHHS, Office for Civil Rights, Region III, Office for Civil Rights, U.S. Department of Health and Human Services, 150 S. Independence Mall West, Suite 372, Philadelphia, PA 19106-3499. See Section 10.7 (relating to complaints to DHHS, enforcement and penalties).

2. An appeal to the Department of Public Welfare must be filed in writing within 30 days of the date the decision was mailed.

10.7 Complaints to DHHS, Enforcement and Penalties

1. Any person who believes a covered entity has not complied with the requirements of the privacy rule may file a complaint with the DHHS. This complaint must be filed in writing (either written or electronically) within 180 days after he/she became aware that, or should have become aware that, the violation occurred, unless DHHS waives this requirement for good cause. DHHS may then investigate the complaint, including a review of pertinent policies, procedures and practices of the covered entity and the circumstances underlying any alleged acts or omissions concerning compliance.

2. DHHS may conduct compliance reviews of covered entities. The Department is required to cooperate with any complaint investigation or compliance review process and must permit DHHS access to its facilities, books, records, accounts and other

sources of information. The privacy office will submit compliance reports to DHHS upon request.

3. Where there is a finding of noncompliance, DHHS will provide written notice of such to the Department and, if there is a complainant, to the complainant. DHHS will attempt to resolve the matter by informal means whenever possible. If the matter cannot be resolved informally, DHHS may issue to the Department and complainant (if applicable) written findings documenting noncompliance.

4. The privacy rule sets forth stringent penalties for covered entities and business associates that violate it. Penalties for violations occurring before February 18, 2009 include civil money penalties of up to $100 per violation, with the total amount imposed on a covered entity for all violations of an identical requirement or prohibition during a calendar year not to exceed $25,000.

    a. For violations occurring on or after February 18, 2009, civil penalties are based on a tiered system, as follows:

        - Tier A is for violations in which the offender did not realize he or she violated the Act and would have handled the matter differently if he or she had. This may result in a $100 to $50,000 fine for each such violation, and the total imposed for all such violations of an identical provision may not exceed $1,500,000 for the calendar year.
        - Tier B is for violations due to reasonable cause, but not willful neglect. This may result in a $1,000 to $50,000 fine for each such violation, and the total imposed for all such violations of an identical provision may not exceed $1,500,000 for the calendar year.
        - Tier C is for violations due to willful neglect that the organization ultimately corrected. This may result in a $10,000 to $50,000 fine for each such violation, and the total imposed for all such violations of an identical provision may not exceed $1,500,000 for the calendar year.
        - Tier D is for violations of willful neglect that the organization did not correct. This may result in a $50,000 fine for each such violation, and the total imposed for all such violations of an identical provision may not exceed $1,500,000 for the calendar year.

b. Criminal penalties for violations occurring before and after February 18, 2009 include:

- Up to $50,000 and/or up to one year in prison for knowingly improperly obtaining or disclosing PHI.
- Up to $100,000 and/or up to five years in prison for obtaining PHI under false pretenses.
- Up to $250,000 and/or up to ten years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use the information for commercial advantage, personal gain or malicious harm.

Note: The HITECH Act also allows states' attorneys general to levy fines and seek attorney's fees from covered entities on behalf of victims. Courts now have the ability to award costs, which they were previously unable to do

11.0 AMENDMENT PROCEDURES

11.1 Policy

An individual who believes the PHI in his/her record is incorrect or incomplete may request an amendment to the information. See 45 CFR § 164.526.

11.2 Procedures

1. If the individual requests help, the staff person responsible for accessing the record must assist the individual in completing the Request for Amendment of Health Information form at Appendix G.

2. Upon completion of the form, the staff person responsible for accessing the record must add any comments to the form. The original will be placed in the individual's record and a copy will be given to the individual.

3. The staff person responsible for accessing the record must act on the request for amendment no later than 30 days after receipt of the request for amendment.

4. Provided the staff person responsible for accessing the record gives the individual written notice of a delay and the reason for the

delay, the office may have a 30-day extension to process the request.

5. If the request for amendment is granted, the staff person responsible for accessing the record must document at the site of the information that is being corrected or amended indicating "See amendment form" and will sign and date the documentation. The amendment form will be attached to the amended entry and the individual informed that the amendment is accepted. For changes on a computer system, the amendment must be documented via alert, case narrative or other appropriate mechanism.

6. Copies of the amendment/correction form must be provided to the Department's business associates or others who have access to the information subject to amendment and may have relied or might rely on that information to the detriment of the individual.

7. The Department will inform the individual within 30 days that the amendment is accepted and request the individual's identification of persons who received PHI and require the amendment. The Department will inform the persons identified by the individual, as well as other applicable persons/agencies, of the amendment.

8. Documentation will be made on the amendment form indicating to whom the amendment form was sent, the date and the staff member who sent the amendment form.

9. Whenever a copy of the amended entry is disclosed, a copy of the amendment form will accompany the disclosure.

10. The request may be denied if the PHI was not created by the Department or is accurate and complete.

11. If the staff person accessing the record denies the requested amendment, he/she must provide the individual with a timely denial that contains the basis of the denial, the individual's right to file a complaint in accordance with the Department's HIPAA complaint procedures and a statement that the individual may request that the request and denial be provided with all future disclosures.

12. The Department will permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Department may prepare a written rebuttal to the individual's statement of

disagreement. The Department will provide a copy of the rebuttal to the individual.

13. For future disclosures, the Department will identify the protected health information in the record that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Department's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the record.

14. If a request for amendment is made directly to the privacy office, the privacy office will work directly with the program office to make a determination, or take action on the request, as appropriate.

15. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

12.0 RIGHT OF INDIVIDUALS TO ACCESS, INSPECT AND OBTAIN COPY

12.1 Purpose

An individual has the right to access, inspect and obtain a copy of PHI in a designated record set for as long as the information is maintained. See 45 CFR § 164.524.

12.2 Policy

1. The Department will take necessary steps to respond appropriately to individual requests to access, inspect and/or obtain a copy of his/her PHI that is maintained in a designated record set. This policy will not impede other laws that permit free copying for an individual.

2. The Department will produce the individual's record that is available at the site where requested. For example, if the client requested information from the County Assistance Office, the client's case record at the CAO will be provided.

3. An individual does not have the right under HIPAA to access the following types of information:

    a. Psychotherapy notes that are kept separate from the record.
    b. Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or

proceeding. This policy does not preclude discovery in administrative or judicial proceedings.

4. In the case of mental health records covered by 55 Pa. Code Ch. 5100 (relating to mental health procedures), contact the Department's legal office (also referred to as the Department's Office of General Counsel).

12.3 Procedure

1. The Department requires an individual to direct requests for access, inspection, or a copy of PHI to the program office that has the requested information. A Request to Access, Inspect or Obtain a Copy of Protected Health Information form is attached at Appendix H.

2. The individual will be informed that a request for access is required to be in writing.

3. Upon receipt of a request, personnel with appropriate authority will act on the request by:

   a. Informing the individual of the acceptance and providing the access requested; or,
   b. Providing the individual with a written denial. See Section 12.4, (relating to Denying Access to Inspect and Obtain a Copy of Protected Health Information).

4. Action taken pursuant to 12.3.3 (relating to procedure) must be taken:

   a. No later than 30 days after the request is made; or,
   b. If the request is for PHI that is not maintained or accessible on-site, no later than 60 days after the request is made.

5. If the Department cannot take action on a request for access to PHI within the relevant time periods listed in 12.3.4 (relating to procedure), the Department may extend the time required by 30 days and inform the individual of the delay and the reason for the delay. The Department is allowed only one such extension.

6. Personnel with appropriate authority will access the individual's PHI using proper access and authorization procedures.

7. The individual will be allowed access, inspection and/or copies of

the requested PHI in a secure and confidential manner, such that the information cannot be accessed by other persons who do not have appropriate access authority to that information.

8. The Department will provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format.

9. If the request is for information maintained electronically in one or more designated record sets and if the individual requests an electronic copy of such information, the Department will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Department and the individual.

10. If requested by the individual, the Department will arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing of PHI.

11. Appropriate personnel will document the request and delivery of the PHI.

12. Any fees imposed on the individual for a copy of the protected health information or a summary or explanation of such information will be:

    a. Collected by the program office at the time of receipt of the request and the proper completion of the request form.
    b. Only for the cost of the following:
        - Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual.
        - Postage, when the individual has requested the copy, summary or explanation be mailed.
    c. The program office may waive the fee at any time.

13. If a request for access, inspection or to obtain a copy is made directly to the privacy office, the privacy office will work directly with the program office to make a determination or take action on the request, as appropriate.

14. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

12.4 Denying Access to Inspect and Obtain a Copy of PHI

1. The Department will deny access and such denial will be not be subject to review by the privacy office in the following situations:

    a. The PHI is:
        - Psychotherapy notes.
        - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

    b. The Department is acting under the direction of a correctional institution upon an inmate's request for a copy of the PHI and obtaining a copy would jeopardize the health, safety, security, custody or rehabilitation of the individual or of other inmates, or of any office, employee or other person at the correctional institution or person who is responsible for transporting the inmate.

    c. Access to PHI that was created or obtained by the Department in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research, and has been informed that the right of access will be reinstated upon completion of the research.

    d. The individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied if the denial of access under the Privacy Act would meet the requirements of that law.

    e. The individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

2. The Department may deny access provided the individual is given the right to have such denials reviewed by the privacy office in the following situations:

    a. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual.

    b. The PHI makes reference to another person (unless such other person is a health care

provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

c. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

3. If access is denied on one of the grounds permitted under paragraph 2, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Department. The Department will provide or deny access in accordance with the determination of the reviewer.

4. The denial of individual access to PHI must be sent to the individual in writing and contain the basis of the denial, a statement, where applicable, of the individual's review rights and the individual's right to file a complaint in accordance with the complaint procedures at 10.0 (relating to complaint procedures).

5. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator**.**

13.0 ANTI-RETALIATION

13.1 Purpose

The Department is committed to preventing retaliation against individuals for exercising their rights under HIPAA, and other applicable federal, state and local laws and regulations. To support this commitment, the Department will maintain and update, as appropriate, written policies and procedures to prevent retaliation.

13.2 Policy

The program office must comply with Governor's Office Management Directive 205.16 dated November 22, 1995 titled "Compliance with the Whistleblower Law, Act 1986-169."

13.3 Procedure

1. The program office will not intimidate, threaten, coerce, discriminate against or take retaliatory action against:

    a. Any individual for the exercise of any right or participation in any process established under the privacy rule.
    b. Any individual or other person for:
        - filing a complaint under the privacy rule.
        - testifying, assisting or participating in an investigation, compliance review, proceeding or hearing.
        - opposing any act or practice made unlawful under the privacy rule.

2. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator**.**

14.0 TRAINING AND EDUCATION

14.1 Purpose

A covered entity must train all members of its workforce who have access to PHI, on the policies and procedures required by the privacy rule, as necessary and appropriate for the members of the workforce to carry out their job functions. See 45 CFR § 164.530(b). This policy is designed to give guidance and ensure compliance with the training requirements.

14.2 Policy

The Department will provide training to its workforce in accordance with 45 CFR § 164.530(b).

14.3 Procedure

1. The Department must determine the training components required for *every* member of its workforce who have access to PHI, given each individual's specific job duties and contact with or access to such PHI.

2. The program office is responsible to develop or modify, and provide, basic HIPAA training to all members of its workforce, and job specific training to applicable members of its workforce.

3. Training must be provided to Departmental employees, as well as

contracted personnel functioning in regular staff positions at Departmental office locations.

4. All members of the Department's workforce must receive basic HIPAA training which covers the general requirements for the protection of health information and the Department's basic privacy and security policies and procedures.

5. Basic HIPAA training does not need to be repeated if an employee transfers from one program office to another within the Department, as long as there is a written record of the completion of the basic HIPAA training.

6. Job-specific HIPAA training must be provided to those members of the workforce who have job duties related to direct access to PHI.

7. Basic HIPAA training to all members of the workforce, and job-specific training to applicable members of its workforce must be provided:

    a. To each member of the Department's workforce by no later than the compliance date for the covered entity.
    b. To each new member of the workforce within a reasonable period of time after the person joins the Department's or program office's workforce after the compliance date.
    c. To each member of the Department's workforce whose functions are affected by a material change in the policies or procedures of this handbook within a reasonable period of time after the material change becomes effective.

8. The program office must develop and implement procedures to ensure the ongoing training and documentation of training to new members of the workforce.

9. The program office must maintain documentation of the basic and job specific training provided to each applicable member of the Department's workforce including: name of employee, employee number, the date of training, hours of training, content of training, training method (video, face-to-face, CBT, other) and the training source/instructor.

10. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

15.0 NOTICE OF PRIVACY PRACTICES - CONTENT

15.1 Purpose

Notice must be given to individuals of the use and disclosure of PHI as well as the individual's rights and a covered entity's legal duties with respect to PHI. See 45 CFR § 164.520. This policy is designed to give guidance and to ensure compliance with the Notice of Privacy Practices requirements.

15.2 Policy

1. The Department will give adequate notice to individuals regarding the use or disclosure of their PHI, their rights with respect to such use or disclosure and the Department's legal duties pursuant to 45 CFR § 164.520.

2. The content of the notice regarding the use and disclosure of PHI shall comply with the requirements of 45 CFR § 164.520.

15.3 Procedure

1. The Department's Notice of Privacy Practices will be drafted by the privacy office and will contain all the requirements required under the privacy rule.

2. The Department will promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the Department legal duties or other privacy practices stated in the notice, to the extent required by the privacy rule, as amended.

3. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

16.0 NOTICE OF PRIVACY PRACTICES - DISTRIBUTION

16.1 Purpose

Notice must be given to individuals of the use and disclosure of PHI as well as the individual's rights and covered entities' legal duties with respect to PHI. See 45 CFR § 164.520. This policy is designed to give guidance and to ensure compliance with the Notice of Privacy Practice requirements.

16.2 Policy

1. The Department will provide a formal notice to individuals regarding the use or disclosure of PHI pursuant to 45 CFR § 164.520.

2. The provision of the notice given to individuals regarding the use and disclosure of PHI pursuant to 45 CFR § 164.520 will comply with the policies and procedures described herein.

16.3 Procedures for Offices that Operate as a Health Care Provider

1. The notice will be provided to individuals with whom the Department has a direct relationship as follows:

    a. No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider.
    b. Upon request.
    c. On or after the effective date of a revision.
    d. Promptly, at the service delivery site for individuals to request and to take with them.
    e. By posting in a clear and prominent location where it is reasonable to expect individuals seeking services from the covered health care provider to read the notice.

2. For the Department's direct provider sites, the notice will be:

    a. Available at the site for individuals to request and to take with them.
    b. Posted in a clear and prominent location where it is reasonable to expect individuals seeking service to read the notice.

3. The Department will prominently post its notice on its web site, and make the notice available electronically through the web site.

4. The Department will obtain written acknowledgment of receipt of the privacy notice and document compliance with and maintain the notice, by retaining copies of the acknowledgements and notices for a period of at least 6 years from the date of creation or the date when it last was in effect, whichever is later.

5. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

16.4 Procedures for Offices that Operate as a Health Care Plan

1. The notice will be provided:

    a. No later than the compliance date to individuals currently enrolled in services, and thereafter, at the time of enrollment, to individuals who are new enrollees.
    b. A health plan that posts its notice on its web site must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan. A health plan that does not post its notice on a web site must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.
    c. To the head of the household, or named enrollee, whichever is appropriate.
    d. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation has been stabilized.

2. No less frequently than every 3 years, the health care plan must notify individuals of the availability of notices and how to obtain them.

3. The Department will prominently post its notice on any web sites that it maintains that provides information about its services or benefits, and make the notice available electronically through the web site.

4. The Department will retain copies of the notice issued by the Department for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

5. Knowledge of a violation or potential violation of this policy must be reported directly to the program office coordinator.

17.0 PROTECTED HEALTH INFORMATION FOR DECEDENTS

17.1 Purpose

A covered entity must comply with use and disclosure rules for deceased persons. Use and disclosure rules for PHI of decedents are generally the same as for any other individual

17.2 Policy

Where requests are made on behalf of the deceased, the Department must:

1. Verify the identity of the person requesting protected health information of a deceased individual and the authority to have access to that information.

2. Obtain written documentation if disclosure is conditioned on representations § 164.514(h).

17.3 Personal Representatives

An executor or administrator authorized by law to act on behalf of an individual's estate is a personal representative. The personal representative will be treated as the individual for purposes of disclosure of PHI.

17.4 Permitted Disclosures

The Department may disclose PHI without written authorization, only with the approval of the privacy office/the Department's legal office, under the following circumstances and only if more stringent law does not prohibit use or release:

1. To law enforcement officials if there is suspicion that the death may be due to criminal conduct. See § 164.512(f)(4).

2. To coroners/medical examiners for identification, cause of death or other duties. See § 164.512(g)(1).

3. To funeral directors as necessary to carry out their duties. See § 164.512(g)(2).

4. To organ/tissue donation procurement agencies. See § 164.512(h).

5. To conduct research on decedent's information. See

§ 164.512(i)(1)(iii), subject to approval by an independent review board.

6. To physicians of a living individual for that individual's medical treatment. The Department must obtain documentation from the physician that the disclosure is necessary.

7. If the requested information is regarding an individual who died over 50 years ago.

18.0 PROTECTED HEALTH INFORMATION FOR MINORS

18.1 Purpose

Control of an unemancipated minor's health information is generally given to the parent, guardian or person acting in loco parentis, except where state or other applicable law addresses the situation. See 45 CFR § 164. 502(g)(3).

18.2 Policy

1. The Department will give control of an unemancipated minor's health information to the parent, guardian or person acting in loco parentis, except where the parent does not control the minor's health care decision-making under state or other applicable law.

2. The treatment of health information of unemancipated minors pursuant to § 164.502(g)(3) will comply with the policies and procedures described herein.

3. This policy will not prevent caretakers from providing and accessing necessary medical care for the minors in their care.

18.3 Procedure

Under the following situations, the parent does not control the minor's health care decisions and, thus, does not control the PHI related to that care:

1. When state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service, the parent is not the minor's representative. For example, under Pennsylvania law, an adolescent has the right to consent to family

planning services or mental health treatment without the consent of his/her parents, and if the adolescent obtains such services without the consent of the parent, then the parent is not the personal representative under the privacy rule for those services.

2. When a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that conversation or relationship.

3. When a health care professional, in his/her professional judgment, reasonably believes that the child has been or may be subject to abuse, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

4. When caretakers are responsible for the care of a minor, these caretakers shall be able to provide and access the health information necessary for the treatment of the minors in their care.

5. When the minor can lawfully obtain the health care service without the consent of a parent, guardian or other person acting in loco parentis and the minor, a court or another person authorized by law consents to that health care service. Please refer to applicable program office bulletins on information sharing as it pertains to children/minors for more detailed guidance.

19.0 DOCUMENT PRIVACY AND SECURITY

19.1 Purpose

The HIPAA privacy and security regulations require that documents containing PHI, including documents pertaining to public assistance, including medical assistance, SNAP, child care, TANF and CHIP and documents pertaining to the Department in its role as health care provider (for example, services in state facilities) be kept confidential.

19.2 Policy

1. This policy must not impede service delivery or prevent efficient office practices (telephone messages, interview notes). The policy must protect information in the individual's record and limit incidental disclosures.

2. All documents (including paper and electronic documents) containing identifying information must be kept confidential and secure .

3. Identifying information includes: names, address, social security numbers, employee numbers, CIS/HCSIS numbers, account numbers, e-mail addresses, internet addresses, fax numbers, vehicle ID numbers, birth dates, discharge dates, employment dates, photographs and descriptions of persons that could identify a specific individual.

19.3 Procedure

1. Intraoffice, interoffice and outside mail may not be out of sight at any time during pick-up or delivery. This applies to areas that are accessible to the public during the process of picking-up and delivering mail. This does not apply to mail distribution areas/rooms or mail on someone's desk.

2. All documents containing identifying information must be shredded prior to disposal. Documents waiting to be shredded must be stored in a lidded shredding bin or in a secure area. Documents must be shredded within 15 working days of designation to be shredded. Shredding or otherwise destroying PHI must render the PHI essentially unreadable, indecipherable, and otherwise incapable of being reconstructed prior to it being placed in a dumpster or other trash receptacle. For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

3. All floppy diskettes, CDs, flash drives and other media and devices that contain identifying information must be destroyed prior to disposal. Identifying information on diskettes must be deleted prior to disposal if possible. Diskettes to be disposed of (whether information is deleted or not deleted) must be sent to the DPW Office of Administration, Division of Support Services, DPW Warehouse, 905 Elmerton Avenue, Harrisburg, PA 17105, 717-783-8083, attention surplus officer, for proper disposal. The DPW Warehouse has a proper disposal box and procedures for disposal of diskettes.

4. An alternative to 19.3 (relating to document privacy and security procedure), #2 and #3, is to implement a contract/business associate agreement, which includes business associate assurances, with an appropriate professional shredding service that is HIPAA compliant. A shredding service may be used for disposal of paper documents, floppy diskettes or both. If a shredding service is used, the time frame for shredding in 19.3 #2 does not apply.

5. All documents containing identifying information must be kept in a locked file cabinet or in a locked office when unattended. This does not apply to offices located in secure buildings or to areas of buildings where public access is not permitted (e.g. employee access only).

6. All e-mail and facsimile (fax) communications containing identifying information must contain a confidential warning regarding unintended access to the information.

7. The Department will document and retain all HIPAA-related policies, procedures and privacy notices, client requests for accounting, restriction, amendment, alternate means of communication, requests to access his/her information, and responses and dispositions related to these client requests, as well as complaints and related responses and dispositions to complaints, disclosures required to be tracked, lists of records clients may access and any other documents the privacy rule requires be created or maintained. The Department will retain such documentation for at least 6 years from the date of its creation or the date when it last was in effect, whichever is later,

8. For additional information regarding HIPAA security, refer to the Department's Security Handbook. Contact the Department's Security Officer, within BIS.

9. Knowledge of a violation of this policy must be reported directly to the program office coordinator.

20.0 GENERAL BUSINESS PRACTICES

20.1 Purpose

HIPAA Privacy and Security regulations require that protected health information be kept confidential and secure in daily practice.

20.2 Policy

All staff must maintain the confidentiality and security of PHI in daily practice, and must promptly report suspected breaches to the program office coordinator (or designee), who must in turn promptly report such incidents to the Department's Security Office, within BIS. The Security Officer will seek advice from the privacy office/legal office regarding suspected breaches.

20.3 Procedure

1. All staff must speak quietly and confidentially when discussing PHI.

2. All staff must avoid discussing PHI in hallways, elevators or other common areas.

3. All staff must apply the minimum necessary standard. For example, staff must leave only the minimum information on voice mail or an answering machine.

4. All staff must use passwords, screen savers and other appropriate personal computer access protections.

5. All staff must confirm fax numbers prior to sending protected health information. Incoming and outgoing faxes containing PHI must be retrieved immediately.

6. All staff must check copiers to be sure that originals are not forgotten.

7. Knowledge of a violation of this policy must be reported directly to the program office coordinator.

21.0 COMPLIANCE ASSESSMENTS AND MONITORING

21.1 Purpose

The privacy rule permits the Department of Health and Human Services to conduct compliance reviews to evaluate a covered entity's compliance with the privacy rule.

21.2 Policy

The Department will conduct periodic compliance reviews to measure, monitor and document compliance with the privacy rule.

21.3 Procedure

1. The program office will conduct compliance assessments and quality monitoring.

2. Compliance assessments, quality assessments, reports and other documentation must be provided to the privacy office

3. The privacy office/legal office may revise this handbook to support compliance with the privacy rule.

APPENDIX A

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the Pennsylvania Department of Public Welfare (Covered Entity) and _____ (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164,), as amended, 42 C.F.R. §§ 431.301-431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa.C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301 *et seq*., and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be used or disclosed only in accordance with this Agreement and the standards established by applicable laws and agency guidance.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. **Definitions.**
   a. "Business Associate" shall have the meaning given to such term under HIPAA, the HITECH Act, applicable regulations and agency guidance.
   b. "Covered Entity" shall have the meaning given to such term under HIPAA, the HITECH Act and applicable regulations and agency guidance.
   c. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
   d. "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A

and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

e. "Privacy Rule" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

f. "Protected Health Information" or "PHI" shall mean any information, transmitted or recorded in any form or medium; (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations and agency guidance. PHI also includes any and all information that can be used to identify a current or former applicant or recipient of benefits or services of Covered Entity (or Covered Entity's contractors/business associates).

g. "Security Rule" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

h. "Unsecured PHI" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH regulations and agency guidance or as otherwise defined in the HITECH Act.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

3. BUSINESS ASSOCIATE OBLIGATIONS:

a) **Limits On Use And Further Disclosure Established By Agreement And Law.** Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Agreement or as required by law and agency guidance.

b) **Appropriate Safeguards.** Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

c) **Reports Of Improper Use Or Disclosure.** Business Associate hereby agrees that it shall report to _____at _____**,** within two (2) days of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

d) **Reports Of Security Incidents.** In addition to following the breach notification requirements in section 13402 of the HITECH Act and related regulations, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____**,** within two (2) days of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance.

(e) Subcontractors And Agents. Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

(f) **Right Of Access To PHI.** Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set,

to have access to and copy that individual's PHI within five (5) business days of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and the individual. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within five (5) business days. Business associate shall further conform with and meet all of the requirements of 45 C.F.R. § 164.524 and other applicable laws, including the HITECH Act and related regulations, and agency guidance.

(g) Amendment And Incorporation Of Amendments. Within five (5) business days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act and related regulations, and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within five (5) business days.

(h) Provide Accounting Of Disclosures. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the individual or the Covered Entity within five (5) business days of a request for an accounting of disclosures.

(i) Requests for Restriction. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate

shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) Access To Books And Records. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.

(k) Return Or Destruction Of PHI. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(l) Maintenance of PHI. Notwithstanding Section 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in §3(h)) for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) Mitigation Procedures. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.

(n) Sanction Procedures. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.

(o) Grounds For Breach. Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known

of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance.

(p) Termination by Commonwealth. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

(q) Failure to Perform Obligations. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.

(r) Privacy Practices. Covered Entity will provide and Business Associate shall immediately begin using any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than 45 days from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

4. OBLIGATIONS OF COVERED ENTITY:

.

a) Provision of Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change

b) Permissions. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c) **Restrictions.** Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522 and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

SIGNED:

NAME, TITLE, ADDRESS DATE

NAME, TITLE, ADDRESS DATE

APPENDIX B

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

AUTHORIZATION FOR USE OR DISCLOSURE OF PERSONAL INFORMATION

1. I authorize the Department of Public Welfare to use/disclose individual information as described below from the records of:

   Name:_____
   Date of Birth:_____ Telephone:_____
   Address:_____
   ID number(s) (identify each type of number):_____
   _____

2. Reason for disclosure:_____
   _____
   (Describe each specific purpose - if disclosure is at individual's request and information to be disclosed does not include drug and alcohol treatment information, may state, "At the request of the individual")

3. I understand that:

   a. This authorization may be revoked at any time by writing to the individual/organization identified in Section 1 except to the extent that information has already been disclosed. If information has already been disclosed in reliance on this authorization, revoking it will only prevent future disclosure.

   b. The Department and its health and human services program will not condition treatment, payment, enrollment or eligibility on the provision of this authorization.

   c. Information (except drug and alcohol information) disclosed pursuant to this authorization may be subject to redisclosure by the individual/ organization identified in Section A.2 below and is no longer protected by federal privacy regulations.

   d. The Department, its programs, services, employees, officers, and contractors are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized.

e. I may refuse to sign this authorization.

PART A - General Information

A.1 Information to be disclosed (Identify specifically the information to be used/ disclosed. If information to be used or disclosed includes mental health, drug and alcohol, or HIV-related information, please complete section on back of this form that relates to that information):

_____

_____

A.2 This information is to be disclosed to:

_____

(Insert name or title of the individual/organization to whom disclosure is to be made)

A.3 This authorization expires as indicated:

_____ Once acted upon

_____ Other (specify date or event**)** _____

PART B - Special Categories of Medical Information

B.1 **Drug and Alcohol Information**:

If my medical record includes drug and alcohol information, I want to send that information to the individual/organization identified in Part A of this form.

_____ Yes _____ No or Not Applicable

This information will be disclosed from records protected by Federal Confidentiality rules (42 CFR Part 2). The Federal rules prohibit the individual/ organization identified in Part A of this form from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

B.2 **Mental Health Information**

If my medical record includes mental health information, I want to send that information to the individual/organization identified in Part A of this form.

_____ Yes _____ No or Not Applicable

B.3 **HIV/AIDS Information**

If my medical record includes HIV/AIDS information, I want to send that information to the individual/organization identified in Part A of this form.

_____ Yes _____ No or Not Applicable

This information will be disclosed from records protected by Pennsylvania law. Pennsylvania law prohibits further disclosures of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains, or is authorized by the Confidentiality of HIV-Related Information Act. A general authorization for the release of medical or other information is not sufficient for this purposes.

****

_____ _____

Signature of Individual or Personal Representative Date

If personal representative, state relationship to individual:

_____

_____ _____

Signature of Witness Date
(necessary for release of Mental Health and Drug and Alcohol information)

If individual is physically unable to sign, signature of second witness:

_____

Appendix C

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

REQUEST FOR ACCOUNTING OF DISCLOSURES

Date of Request: _____

Individual's Name: _____

Birth Date: _____

Recipient Social Security Number: _____

Individual's Address: _____
_____

Address to send Accounting of Disclosures (if different than above):
_____

Dates Requested:

I would like an accounting of all disclosures for the following time frame.
(Please note: the maximum time frame that can be requested is six years prior to the date of request. No accounting is available prior to April 14, 2003).

From: _____ To: _____

_____
Signature of Individual or Personal Representative Date

FOR DEPARTMENT USE ONLY:

Date Received: _____ Date Sent: _____

Extension requested: __ No __ Yes, Reason:
_____

Client notified in writing on this date: _____

Staff member processing request: _____

Appendix D

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

REQUEST FOR ALTERNATIVE MEANS OR LOCATION OF COMMUNICATION

Individual's Name: _____ Birth Date: _____

Recipient Number: _____

Individual's Address: _____
_____

Please explain what kind of alternative means or location of communication you are requesting, for example, if you would rather receive mail at work than at home.

Signature of Individual or Personal Representative _____

FOR DEPARTMENT USE ONLY:

Date Received _____ Amendment has been: ? Accepted ? Denied

Staff member processing request: _____

If accepted, type of alternative means. Explain changes in method and/or location.

If denied, explain why:

Appendix E

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

REQUEST FOR RESTRICTIONS ON THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Individual's Name: _____ Birth Date: _____

Recipient Number: _____

Individual's Address: _____

How would you like the use and disclosure of your protected health information restricted? Explain.

Signature of Individual or Personal Representative _____

FOR DEPARTMENT USE ONLY:
Date Received _____ Restriction has been: ? Accepted ? Denied

If accepted, type of Restriction.

If denied, explain why:

Appendix F

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

COMPLAINT

Individual's Name: _____ Birth Date: _____

Recipient Number: _____

Individual's Address: _____
_____

1. Please explain the nature of your complaint. (You may make a complaint concerning the Department's privacy policies and procedures, its compliance with those policies and procedures, or its compliance with the HIPAA Privacy rule.) (You may attach an additional piece of paper if necessary.)

2. I understand that this complaint must be filed within 180-days of when I knew of the action or inaction that is the basis of this complaint.
3. I understand that this complaint may be submitted directly to:

Privacy Office
Department of Public Welfare
Office of General Counsel
3rd Floor West, Health & Welfare Building
Harrisburg, PA 17120

4. I understand that I may submit my complaint directly to the Secretary of Health and Human Services by writing to: 200 Independence Avenue, SW, Washington, DC 20201

For Department Use Only:

Date received: _____ Received by: _____

Investigation Commenced: _____

Resolution:

Comments:

Appendix G

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

REQUEST FOR AMENDMENT OF HEALTH INFORMATION

Individual's Name: _____ Birth Date: _____

Recipient Number: _____

Individual's Address: _____
_____

Date of entry to be amended (if known): _____

Type of entry to be amended (if known): _____

1. Please explain how the entry is inaccurate or incomplete. What should the entry say to be more accurate or complete?

2. Would you like this amendment sent to anyone to whom we may have disclosed the information in the past? If so, please specify the name and address of the organization or individual.

3. If your request to amend health information is denied, please be advised that you have the right to: submit a written statement (not to exceed 60 words) disagreeing with the denial.

   The statement should be submitted to Privacy Office , Department of Public Welfare, Office of General Counsel, 3rd Floor West, Health & Welfare Building, Harrisburg, PA 17120.

4. If you choose to not complete a statement of disagreement, you may request that the Department provide your request for amendment and the denial with any future disclosures of your information.

5. You may file a complaint concerning this request for amendment directly to:

Privacy Office
Department of Public Welfare
Office of General Counsel
3rd Floor West, Health & Welfare Building
Harrisburg, PA 17120

6. You may submit a complaint directly to the Secretary of Health and Human Services by writing to: 200 Independence Avenue, SW, Washington, DC 20201

Signature of Individual or Personal Representative _____
Date:_____

FOR DEPARTMENT USE ONLY:
Date Received _____ Amendment has been: ? Accepted ? Denied

If denied, check reason for denial:
? Record was not created by this organization.
? Record is not available to the individual for inspection as required by federal law (e.g., psychotherapy notes).
? Record is not part of individual's designated record set.
? Record is accurate and complete.

Comments

Date Amendment made_____

_____ _____
Name of Staff Member Title

Appendix H

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

REQUEST TO ACCESS, INSPECT OR OBTAIN A COPY OF PROTECTED HEALTH INFORMATION

Individual's Name: _____ Birth Date: _____

Recipient Number: _____

Individual's Address: _____

I am requesting (check where applicable) ? access to and/or ? a copy of my record. I know that I do not have a right to access psychotherapy notes or information compiled in anticipation of a legal proceeding.

The fee for this request will be: _____ (to be completed by the program office)

I understand that action will be taken on this request within 30 days of the Department's receipt of the request. If the information is not readily accessible to the Department, action will be taken no later than 60 days after the request. I understand that the Department may extend the above time limits by 30 days.

_____ _____
Signature of Individual or Personal Representative Date

For Program Office Use Only:

Date received: _____ [ ] Approved [ ] Denied

Extension:

Staff member processing request: _____

Comments:

Date copy provided _____