COMMONWEALTH OF PENNSYLVANIA **DEPARTMENT OF AGING** **Harrisburg, PA 17101**	**PENNSYLVANIA DEPARTMENT OF AGING**	
	1. File Number: APD #03-01-07	**2. Disposition:** Note well and file for reference
	3. Issuance Date: May 8, 2003	**4. Effective Date:** Immediately
	5. Program Area: AAA Administration	
6. Origin: Office of Program Management	**7. Contact:** Analysis, Program Reporting & Research Division (717) 783-6207	

AGING PROGRAM DIRECTIVE

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION AND HOW THE REQUIREMENTS IMPACT THE PENNSYLVANIA AGING NETWORK**

TO: EXECUTIVE STAFF
DIVISION OF CONTRACT MANAGEMENT & APPEALS
BUREAU OF HOME & COMMUNITY BASED SERVICES
PA COUNCIL ON AGING
AREA AGENCIES ON AGING
PA ASSOCIATION OF AREA AGENCIES ON AGING
ADMINISTRATION ON AGING

FROM: Signed 5/8/03
Ivonne G. Bucher, Director
Office of Program Management
Department of Aging

REGULATORY REFERENCES: 45 CFR Parts 160 and 164
45 CFR Parts 160, 162, 164

PURPOSE: The purpose of this Aging Program Directive (APD) is to state the Department of Aging's position on the impact of the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information on the Aging Network.

BACKGROUND: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) enacted health care reform in the following areas:

1) Standardization of electronic data exchange for administrative and financial transactions. ("Security Standards")
2) The protection of security and confidentiality of electronic health information. ("Privacy Standards")

In regard to Privacy Standards, HIPAA required the U.S. Department of Health and Human Services (HHS) to implement a comprehensive federal law to protect identifiable health information ("PHI"). HHS published final regulations, entitled *Standards for Privacy of Individually Identifiable Health Information* on December 28, 2000. The HIPAA privacy regulations, effective April 14, 2001, and amended August 14, 2002, create a national establishment of safeguards to protect the privacy of health information and place limitations on the manner in which it is disseminated (67 Fed. Reg. § 157; 45 C.F.R. Parts 160 and 164 or http://www.hhs.gov/ocr/hipaa/privruletxt.txt). With the exception of small health plans, covered entities were required to comply with the privacy standards by April 14, 2003.

The regulations only affect entities that: (1) fall within the definition of a health plan, health care clearinghouse or a health care provider or (2) are a business associate of these 'covered entities.' The following definitions are provided to aid in understanding this Directive:

- **Covered entity**. A health plan, a healthcare clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA rules.

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

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

  (a) Processes health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
  (b) Receives a standard transaction from another entity and processes health information into nonstandard format or nonstandard data content for the receiving entity.

- **Health care provider**. A provider of services, a provider of medical or health services and any person or organization who furnishes, bills, or is paid for health care in the normal course of business.

- **Health information**. Any information, whether oral or recorded in any form or medium that:

  (a) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse.
  (b) Relates to the physical or mental health or condition of any individual, the provision of health care to an individual or payment for the provision of health care to an individual.

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

- **Hybrid agency**. Means a single legal entity (1) that is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates health care components in accordance with the HIPAA regulations for the purpose of defining the health care components as being a HIPAA compliant entity with the non-health care components not being subject to the HIPAA regulations.

- **Business associate**. A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entities work force.

- **Protected health information**. Individually identifiable health information that is transmitted by electronic media, maintained in any medium, or transmitted or maintained in any other form or medium.

The complete definitions can be found at 45 C.F.R. § 160.103.

The Department of Aging (PDA) has reviewed the HIPAA privacy requirements in regard to programs it solely administers and programs it supports at the Area Agency on Aging level through grants and allocations.

REQUIREMENTS: Generally, the Privacy Rule prohibits disclosure of PHI except in accordance with the regulations. Each organization which has access to PHI must do an analysis to determine whether or not it is a covered entity. The regulations define and limit the circumstances under which covered entities may use or disclose PHI to others. Permissible uses under the rules include three categories: (1) use and disclosure for treatment, payment and healthcare operations; (2) use and disclosure with individual authorization; and (3) use and disclosure without authorization for specified purposes.

The Privacy Regulations require Covered Entities to:

a) Appoint a privacy officer charged with creating a comprehensive Privacy Policy
b) Develop minimum necessary policies
c) Amend Business Associate contracts
d) Develop accounting of disclosures capability
e) Develop procedure to request alternative means of communication
f) Develop procedure to request restricted use
g) Develop complaint procedure
h) Develop amendment request procedure
i) Develop individual access procedure
j) Develop anti-retaliation policy
k) Train workforce
l) Develop and disseminate privacy notice

DEPARTMENT OF AGING'S RESPONSIBILITIES:

1) PDA concludes it is a Hybrid Agency under HIPAA.
2) PDA concludes that the PACE Program is the only program within its jurisdiction that is a covered entity under HIPAA.
3) PDA will voluntarily meet privacy standards set forth in the HIPAA regulation for all Human Resource and Service programs through a separate PDA "Privacy and Security Plan".
4) PDA does not consider itself to be a Business Associate, as it does not perform any functions and/or activities on behalf of a covered entity.
5) PDA is a Health Oversight Agency in regard to AAAs who declare themselves HIPAA-covered entities. A Health Oversight Agency may have access to PHI as necessary to fulfill health care and government oversight responsibilities. A Health Care Oversight Agency is not subject to the HIPAA regulations.
6) PDA will not share HIPAA liability with any agency should they fail a HIPAA audit.

CONCLUSIONS – AREA AGENCIES ON AGING (AAAs):

Recognizing the ways AAAs have organized themselves and the way they operate in their local community, the Department assumes there may be some difference in the way various AAAs approach HIPAA. To assist AAAs with this determination, Covered Entity Decisions Tools can be found on the CMS web site at:

http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

1) Each Area Agency on Aging is responsible to determine its responsibilities under HIPAA.
2) AAAs who declare themselves as entities under HIPAA are responsible to determine Business Associate status for the agencies they interact with.
3) The Ombudsman Program operates as a Health Oversight Agency and has access to PHI information as it relates to the program outside of HIPAA requirements.
4) The Protective Services Program operates as a Health Oversight Agency and has access to PHI information as it relates to the program outside of HIPAA requirements.