

DEPARTMENT OF PERSONNEL & ADMINISTRATION		HIPAA Policy No.	5
		Current Effective Date	May 1, 2006
		Original Effective Date	May 1, 2006
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT		Approved by: Jeffrey C. Schutt	
SANCTIONS		Date: <i>4/25/06</i>	

I. Purpose

To provide guidelines for the imposition of sanctions for HIPAA privacy or security violations.

II. Policy

It is the policy of the Department of Personnel and Administration (DPA) to impose sanctions for any violation of the HIPAA Privacy Rule or the HIPAA Security Rule. Sanctions will vary based on the severity of the action, whether the action was intentional or not, whether the action represents a pattern of behavior, and the extent of the harm that results from the action.

The following are guidelines to be used in determining the level of the offense and the appropriate sanction. These guidelines are based, in part, on State Personnel Board rules and the technical assistance on Corrective and Disciplinary Actions prepared by the Division of Human Resources (DHR) and published on its web site.

Level 1 Offenses: Carelessness with PHI; unintentional use or disclosure of PHI.

Examples: Leaving a document containing PHI on a copy or fax machine; discussing PHI in a public area; leaving a computer monitor unattended with PHI visible on the screen.

Sanctions: For a first offense, a meeting with the employee is recommended. Repeat offenses require harsher sanctions, beginning with corrective action.

Level 2 Offenses: Intentional, inappropriate access of PHI, without disclosure; accessing more PHI than the minimum necessary; accessing PHI without a legitimate business reason.

Examples: Looking up birth dates or addresses; accessing the records of a friend, family member, co-worker, or state employee out of curiosity; accessing the PHI of a public official.

Sanctions: At a minimum, corrective action is recommended, even for first offenses. Repeat offenses require harsher sanctions, such as disciplinary action up to and including termination.

Level 3 Offenses: Willful or intentional disclosure of PHI; improper disclosure of PHI; improper use of PHI for personal gain or with ill will.

Examples: Accessing PHI to get information to use in personal matters like a divorce or custody proceeding; using information from improperly accessed PHI to tell co-workers about the medical condition of another co-worker; disclosing PHI to the media; selling PHI; compiling a mailing list from PHI for sale or for personal use; using or disclosing PHI for employment-related decisions.

Sanctions: For these offenses, even a first time offense, the recommendation is for disciplinary action, up to and including termination.

In addition, any member of DPA's workforce who knowingly and willfully violates the HIPAA Privacy Rule or the HIPAA Security Rule may be subject to criminal investigation and prosecution or civil monetary penalties.

III. Procedures

The above guidelines are to be used in conjunction with State Personnel Board Rules and Personnel Director's Administrative Procedures on corrective and disciplinary actions when imposing sanctions

for HIPAA violations. Each situation involving a potential HIPAA violation is to be evaluated individually, and appropriate sanctions determined at that time. Situations involving cabinet appointees shall be evaluated by the Governor and sanctions determined by the Governor.

IV. Definitions/Abbreviations

Workforce: Under HIPAA, workforce means employees, volunteers, trainees, and other persons under DPA's direct control, whether or not they are paid by DPA. For HIPAA purposes, the term workforce is expanded to include those individuals who may, at times, work for or act on behalf of the health plans (such as benefits administrators), even though they are not under DPA's direct control.

V. Revision History

<u>Date</u>	<u>Description</u>
May 1, 2006	Original document

VII. References/Citations

<u>HIPAA Security Rule</u>	
45 CFR 164.308(a)(1)	Security Management
45 CFR 164.308(a)(1)(ii)(c)	Sanction Policy
<u>HIPAA Privacy Rule</u>	
45 CFR 164.530	Administrative Requirements
45 CFR 164.530(e)(1)	Sanctions