Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

John Chappuis, Deputy Director

Date: January 3, 2003

Revised Date: May 13, 2004

Policy Title:	Physical Security for Protected Health Information		
Policy Number:	014	**Version:**	1.1
Approved By:	John Chappuis		
Date Approved:	June 22, 2004		

Purpose:

This policy addresses the actions necessary to create an environment that protects the security of Protected Health Information ("PHI"). See HIPAA Policy #1, Privacy of Protected Health Information 11-4-02, for definition of PHI.

Policy:

Employees of DPHHS must make reasonable efforts to provide for the security of Protected Health Information.

1. Security of PHI held in electronic medium (includes discs, tapes, computers, etc.)

   a. Each employee is responsible for his/her own uses and disclosures of PHI;

   b. Employees must sign confidentiality statements before obtaining computer access to PHI;

   c. Employees will be granted access to only the level of PHI that is required by their job duties and position description. (For levels of access, see HIPAA Privacy Policy, #13, Employee Access to PHI, December 17, 2002.);

   d. Log-off screens must be used to assure no unauthorized access to computers with PHI. A screen saver set to activate within five minutes, locking the workstation manually, or a complete computer log-off can be used;

   e. Employees may not share passwords or computer access. (See Information Security and database Access Policy 12-15-96.)

   f. Each employee must ensure that PHI on computer screens is not visible to unauthorized persons. This can be accomplished through the use of polarized screen covers, placement

of computers out of the visual range of persons other than the authorized user, clearing information from the screen when not actually being used, or minimizing all applications when away from the work space or when approached by an unauthorized person.

g. E-mail messages containing PHI are not available as public information;

h. E-mail messages containing PHI sent outside of the State email system must either be encrypted or the PHI must be contained in a password-protected attachment. The password should be provided to the intended recipient via separate contact; and

i. When an employee leaves DPHHS, their computer access must be immediately terminated and their password discontinued. Interim access to critical information is the responsibility of the Supervisor.

2. Security of PHI held on paper

a. Envelopes containing PHI may be opened by administrative staff, date stamped, returned to the envelope, and then placed in the intended recipient's mailbox in a sealed manner;

b. Only PHI in current use should be exposed on an employee's desktop. All other paper forms of PHI should be covered in file folder or placed face down on the desktop when not in use;

c. When the employee is away from the desk for an extended period of time (such as for meal break or to go home for the day) all PHI should be contained in a locked filing cabinet;

d. When it is no longer necessary to keep PHI, it must be shredded; and

e. When PHI is to be faxed, the employee will verify the validity of the fax number prior to transmission and will confirm successful transmission to the correct number. If faxed PHI is received, it should either be given to the recipient promptly, or placed in a sealed envelope and placed in the employee's mailbox.

3. Security of PHI in other media, such as oral or telephone communication.

a. Face to face and telephone conversations regarding PHI should be kept to a minimum and should use identifying information as little as possible. For example, a conversation could identify the client with a number rather than a name. In all cases, the conversation must be limited to the minimum information necessary to accomplish the purpose of the communication;

b. Oral conversations about PHI should be conducted in a manner and setting that minimizes the amount of the conversation that can be overheard by other individuals;

c. Sign-in sheets for clinics may be used, but they shall not request the reason for visit; and

d. When receiving telephone calls requesting PHI, the DPHHS employee must validate the identity of the caller before releasing information. In most cases, the request for PHI should be made in writing with a properly signed authorization, or in person with a mechanism to identify the individual requesting the PHI disclosure. In cases where the DPHHS employee may have regular communication with a business associate regarding PHI, the DPHHS employee takes responsibility for validating the identity of the business associate.