

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	Data Protection Policy
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

The Department of Health and Human Services (DHHS) collects and processes a significant volume of data and information required to provide services to the residents of North Carolina. DHHS data includes sensitive individually-identifiable health information, personal, financial and operational information that must be protected in accordance with state and federal law. This policy establishes a comprehensive data protection process within all DHHS Divisions/Offices that includes data stewardship, data management, data transmission and data encryption as appropriate.

Policy

DHHS data shall be protected from unauthorized or accidental disclosure, misuse, modification or loss. This comprehensive policy is comprised of four (4) components:

Data Stewardship - Promotes data security, by designating roles and responsibilities for the appropriate control and stewardship of DHHS data. To effectively implement information security, there must be an assignment of responsibility to protect information and as well as provide accountability within an organization.

Data Management – Ensures the safe storage and handling of sensitive information. Data security is provided through the implementation of physical, technical and administrative security controls.

Data Transmissions – Ensures that sensitive data are protected during transmission. Security controls are needed to both prevent unauthorized access as well as protect the data from being read if accessed.

Data Protection Controls – Provides a broad set of requirements on protecting sensitive/critical data for the DHHS Divisions/Offices.

Roles and Responsibilities

DHHS Privacy and Security Office - The DHHS Privacy and Security Office (PSO) shall develop standards and implementation guidelines that will include the following: Data

Stewardship, Desktop Security, Data Access and Control, Data Protection Controls, Laptop/PDA Security, Records Management, Data Storage and Archiving, Email Security, Property Control, Application/Database Security, and Network Security. Enterprise-wide procedures will be developed through a joint effort of the PSO and the DHHS Security Work Group (SWG) to ensure they meet the needs of the DHHS Divisions/Offices. The procedures established shall, to the extent possible, control, reduce or eliminate the risk of breaches of data protection.

Office of Information Technology Services - The Office of Information Technology Services (ITS) shall be responsible for ensuring adequate security on the North Carolina Integrated Information Network (NCIIN). In addition, to providing Internet access and email security, ITS is responsible for maintaining the security of DHHS mainframe applications. The ITS Security Office publishes IT security policies and standards that DHHS is required to implement.

The Division of Information Resources Management – The Division of Information Resources Management (DIRM) shall be responsible for implementing and providing adequate security for the DHHS applications/systems maintained for divisions/offices. The security requirements will be implemented in accordance with DHHS security procedures and standards as developed by ITS and DHHS PSO.

DHHS Divisions/Offices - DHHS Divisions/Offices shall be responsible for implementing and providing adequate security for any application/system not maintained by DIRM. In this context, the DHHS Divisions/Offices shall be responsible for the classification of all data (see DHHS Data Classification Policy for details) and for evaluating and ensuring the adequacy of all security controls at the DHHS Divisions/Offices. For those applications/systems maintained by DIRM as an affiliate of a division/office, DIRM shall be responsible for ensuring the adequacy of the security controls.

If a DHHS Division/Office has outsourced work to a contractor, they are responsible for providing oversight to ensure the contractor is providing adequate security.

Implementation

Policy implementation shall comply with the referenced standards and management approved best practices.

1. Data Stewardship

Data Stewardship is a key element to ensuring data protection. It relies on an understanding of an individual's job responsibilities, training and accountability. To ensure this objective is achieved, each division/office shall ensure that security is addressed in job descriptions, as applicable. These job descriptions shall include the data security responsibilities associated with the assigned tasks. The DHHS Divisions/Offices shall ensure that data security responsibilities have been defined for all DHHS contractors and volunteers. In addition,

every individual in the DHHS workforce shall receive security training and be informed of their security responsibilities. Special training emphasis will be given to the DHHS Policy “Acceptable Use for DHHS Information Systems.”

2. Data Management

DHHS information shall be handled in a manner that will protect it from unauthorized access, modification or loss. In general, DHHS shall follow the ITS statewide [Policy and Guidelines for Data Handling](#). The DHHS PSO shall develop DHHS enterprise-wide procedures for handling and storing sensitive data.

A. Desktop and Laptop Security

All DHHS computer desktops and laptops shall be secured to minimize unauthorized access and minimize the risk of computer viruses’ and malware’s being introduced. DHHS shall implement the [ITS Desktop and Laptop Security Standard](#). The DHHS PSO shall develop DHHS enterprise-wide desktop security and laptop security procedures.

B. Mail Server Security

All DHHS electronic mail shall be protected from unauthorized access. The ITS organization shall ensure the security of DHHS electronic mail and adhere to the [ITS Electronic Mail Security Standard](#). All sensitive mail attachments shall be sent either password-protected or via encrypted transmissions.

C. Records Management

The DHHS PSO shall develop a records management standard that will address both federal and state regulatory requirements for handling sensitive information. The PSO in coordination with other responsible divisions/offices shall develop a standard and implementation guidelines for addressing the ITS components of a comprehensive records management system.

The DHHS Divisions/Offices shall implement record management practices through the design and operation of reliable record management systems. These may be dedicated electronic record management systems or business systems and processes which manage paper-based records and thereby function as record management systems.

The DHHS Divisions/Offices shall review and modify the record retention schedule for all data owned. Each DHHS Division/Office shall identify data record types and retention periods in order to comply with state and federal regulations. Each DHHS Division/Office shall review and modify program record retention and disposition schedules for the data owned by the division/office.

- D. Protecting Data on Information Systems/Applications
DHHS Divisions/Offices shall protect data on all sensitive and critical applications/systems by implementing controls that are commensurate with the security level required to protect the data contained in those systems. The PSO shall develop guidelines for implementing controls on all sensitive, critical and non-sensitive applications/systems.

3. Sensitive Data Transmissions

Sensitive data (e.g., an individual's health information) must be adequately protected when transmitted either physically or electronically. In general, the protection of sensitive data follows three rules:

- A. If sensitive electronic data resides in a DHHS Division/Office, administrative, physical and technical security controls must be implemented to limit unauthorized access to the data.
- B. If sensitive electronic data is being sent over the network to a federal agency or outsourced entity (business associate or vendor), the data being transmitted must be either encrypted or sent in a password-protected file.
- C. If sensitive data is being physically transported off-site to another location, the data shall be protected by implementing the standards to mitigate risk.

4. Data Protection Controls

The DHHS PSO shall develop and maintain data protection standards and enterprise-wide implementation procedures for the DHHS Divisions/Offices. Data protection determinations shall be made with the assistance of the assigned information security official and affiliated staff at each DHHS Division/Office.

The DHHS PSO will develop and maintain standards that apply to DHHS business requirements. These requirements may utilize Internet Protocol Security (IPSEC), Digital Certificates or other encryption standards.

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer (DHHS.Security@ncmail.net). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)

Exceptions

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [*ITS Waiver and Appeals Policy*](#).