

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Privacy Manual
Chapter:	Administrative Policies, Privacy Protections
Current Effective Date:	5/1/05
Revision History:	10/9/03
Original Effective Date:	4/14/03

Purpose

The purpose of this policy is to establish the process for developing and implementing specific policies to protect the privacy of individually identifiable health information.

All North Carolina Department of Health and Human Services (NC DHHS) agencies must comply with this policy.

Policy

DHHS shall develop policies that are appropriate for its agencies to implement in order to protect the privacy of individually identifiable health information that is created, received, and maintained during its regular course of business. Policies will be reasonably designed to comply with state and federal laws, taking into account the scope of the requirement and the nature of activities undertaken that relates to individually identifiable health information. The Health Insurance Portability Accountability Act (HIPAA) Privacy Rule will be the primary resource for DHHS privacy policies.

Department-Wide Policies

DHHS shall evaluate each privacy policy based primarily on the HIPAA Privacy Rule to determine if the policy should be applied to all agencies within the department regardless of the HIPAA impact. Determination, by the DHHS Office of the Secretary, for a department-wide approach to policy requirements will take into account the most efficient and effective methods for ensuring the protection of individually identifiable health information and equitable client rights, while promoting consistency in the management of health information throughout the department.

The purpose statement in each privacy policy will include a scope statement designating the DHHS agencies that must comply with each policy.

Division/Office Responsibility

It is the responsibility of DHHS agencies to develop procedures for implementing policies for which they must comply. Because agencies conduct their business operations somewhat

differently, specific procedures for implementing department privacy policies must be developed at the agency level. Required procedural elements to be addressed by DHHS agencies will be identified by the department.

Retention and Disposition

Policies, procedures, and privacy documentation required by the HIPAA Privacy Rule must be maintained in writing in accordance with the *General Schedule for State Agency Records* issued by the NC Department of Cultural Resources, Division of Archives and History, Archives and Records Section, Government Records Branch.

Compliance

DHHS agencies must comply with the privacy policies developed and implemented according to this process by April 14, 2003. This date represents the compliance date specified in the HIPAA Privacy Rule.

Implementation

The department shall develop policies that address essential administrative privacy requirements so DHHS agencies will use and/or disclose individually identifiable health information in a confidential and secure manner. All policies shall be located in the *DHHS Policy and Procedure Manual* that is maintained by the Office of the DHHS Secretary. The policies to be developed will address the following privacy requirements:

- **Privacy Officer**
As specified in DHHS Directive Number III-11, the department shall designate a privacy officer to oversee all ongoing activities related to the development, maintenance, and adherence to department policies regarding the privacy of and accessibility to individually identifiable health information, in accordance with state and federal laws and best business practices.
- **Training**
The department shall develop policies regarding training of all members of its workforce who are likely to have access to individually identifiable health information. At a minimum, training shall be provided for newly developed privacy policies, during new employee orientation, and whenever significant changes are made to privacy policies.
- **Safeguards**
The department shall develop policies that specify administrative, technical, and physical safeguards that protect the privacy of individually identifiable health information from unauthorized use or inadvertent disclosure to persons other than the intended recipient. Measures taken will relate directly to the size of the agency and the type of activities that the agency undertakes.

- **Business Associates**
The department shall develop policies regarding the identification of “Business Associates” and develop agreements that will limit the business associate’s uses and disclosures of individually identifiable health information to those permitted by the agreements.
- **Limitations on Information Access**
The department shall develop policies that limit access to individually identifiable health information by members of its workforce, as well as other requesters of information, to the “minimum necessary” information required to fulfill a need or request. Verification of the identity and authority of requesters for individually identifiable health information shall be required prior to disclosure of the requested information.
- **Use and Disclosure**
The department shall develop policies that specify the conditions necessary before divisions/offices can use or disclose individually identifiable health information including policies on required authorizations, instances when authorizations are not required, and requirements for the use of individually identifiable health information for research, marketing, or fund raising purposes.
- **Client Rights**
The department shall develop policies that will afford clients appropriate protections and controls over their individually identifying health information maintained by DHHS offices and divisions. Such controls shall include notifying clients of the privacy practices in the division/office and the client’s right to request access to or amendment of their health information.
- **Documentation of Complaints**
The department shall develop policies that provide a mechanism for receiving complaints from individuals regarding DHHS agency compliance with department privacy requirements. Documentation must include identification of a contact person (or office), a record of the complaints that are filed, and a brief explanation of complaint resolution, if any.
- **Sanctions**
The department shall develop policies that specify appropriate sanctions against members of its workforce who fail to comply with department privacy requirements. Sanctions will be appropriate to the nature of the violation. Such sanctions will not apply to whistleblower activities, nor to complaints or investigations.
- **Mitigation**
The department shall develop policies that define its mitigation procedures for use or disclosure of individually identifiable health information that is in violation of department requirements. Any harmful effect that is known to the department of a use or disclosure of individually identifiable health information that is in violation of its policies will be mitigated in an effort to prevent such future occurrences.

- Refraining from Intimidating or Retaliatory Acts**
 The department shall develop policies that prohibit intimidation, threats, coercion, discrimination, or other retaliatory action against individuals who file a privacy complaint against the department; testify, or assist in an investigation or review of the department; or oppose any act or practice thought to be unlawful. The department will not require a client to waive his/her right to file a complaint with DHHS or the federal Department of Health and Human Services Secretary as a condition for the provision of treatment, payment or enrollment in a health plan, or eligibility for health care benefits.
- Transition Phase**
 The department privacy policies will address transition requirements for authorizations or other express legal permissions used by DHHS agencies. To the extent permitted by the HIPAA Privacy Rule, agencies may grandfather in and rely upon authorizations or other express legal permissions obtained prior to April 14, 2003, to ensure that important functions of the health care system are not impeded. However, authorizations or other express legal permissions made on or after April 14, 2003, must meet the DHHS privacy policy requirements.
- Policy and Procedure Changes**
 The department shall modify, in a prompt manner, its privacy policies as necessary and appropriate to comply with changes in the state and federal law and ongoing business practices. Changes to policies may be made at any time, provided such changes are documented and implemented according to DHHS policy requirements. DHHS offices shall modify, in a prompt manner, their individual privacy procedures to conform to revised department privacy policies.

Reference

DHHS Directive Number III-11; 45 CFR 164.530

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