

## DHHS POLICIES AND PROCEDURES

**Section VIII:** Privacy and Security  
**Title:** Privacy Manual  
**Chapter:** Administrative Policies, Workforce  
**Current Effective Date:** 2/1/16, 5/1/05, 11/15/15/  
**Revision History:** 7/14/03, 11/15/15  
**Original Effective Date:** 4/14/03

### PURPOSE

The purpose of this policy is to address the North Carolina Department of Health and Human Services (NC DHHS) privacy requirements regarding the use and disclosure of individually identifiable health information by full time and part time employees, hereinafter referred to as “workforce”. Additionally, this policy covers students, volunteers, trainees, contractors, personnel working through a temporary agency, and other persons whose conduct in the performance of work for an agency is under the direct control of the agency, whether or not they are paid by the agency, who are hereinafter referred to as “extended workforce”.

*This policy shall apply to all DHHS agencies that maintain individually identifiable health information.*

#### Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule addresses the protection of individually identifiable health information and mandates that covered entities provide appropriate privacy training to their workforce and extended workforce on the agency's policies and procedures regarding protected health information.

The HIPAA Privacy Rule also requires that appropriate sanctions be established for the workforce and extended workforce for failure to comply with privacy requirements, including making reasonable efforts to lessen any resulting harmful effects of unauthorized use or disclosure of information.

DHHS has determined that every agency in the department that maintains individually identifiable health information must comply with this workforce policy to ensure that members of the DHHS workforce and extended workforce understand the importance of privacy protections and the consequences of inappropriate uses or disclosures of individually identifiable health information.

## **POLICY**

Agencies shall ensure that members of their workforce and extended workforce make reasonable efforts to protect individually identifiable health information from intentional or unintentional use or disclosure that is in violation of the department's privacy policies and/or agencies' procedures. In the event that an agency should become aware of a privacy policy violation, the agency must make reasonable efforts to lessen any resulting harmful effects. Each agency shall ensure the protection of individually identifiable health information in a manner consistent with all requirements specified within this policy.

This policy covers students, volunteers, trainees, contractors, personnel working through a temporary agency, and other persons whose conduct in the performance of work for an agency is under the direct control of the agency, whether or not they are paid by the agency, who are hereinafter referred to as "extended workforce".

## **IMPLEMENTATION**

The HIPAA Privacy Rule addresses the protection of individually identifiable health information and mandates that covered entities provide appropriate privacy training to their workforce and extended workforce on the agency's policies and procedures regarding protected health information.

DHHS has determined that every agency in the department that maintains individually identifiable health information must comply with this workforce policy to ensure that members of the DHHS workforce and extended workforce understand the importance of privacy protections and the consequences of inappropriate uses or disclosures of individually identifiable health information.

Each agency shall ensure that its workforce and extended workforce are trained with respect to the protection of individually identifiable health information in accordance with the DHHS Privacy Policies and agency procedures, as appropriate in the performance of their job responsibilities. Training shall be provided to workforce/extended workforce with direct, inadvertent, or incidental access to such health information. This training is required for current members of the workforce and extended workforce, as well as new members of the workforce/extended workforce within a reasonable time after their employment. HIPAA training is available to all employees on the LMS system, and must be completed on a yearly basis.

Each agency shall develop procedures that ensure the appropriate privacy training of members of their workforce and extended workforce. Privacy training must be customized and categorized according to the level of access to individually identifiable health information required to fulfill job responsibilities. Basic privacy training must include awareness of the vulnerabilities of the health information in each agency's possession and procedures that must be followed to ensure the protection of that information as necessary for each individual to carry out his/her required

job functions, including possible consequences for violation of privacy policies or procedures. Basic training is sufficient for some categories of staff, such as those staff members who are subject to inadvertent or incidental exposure to individually identifiable health information.

Each agency's procedures shall also provide for the documentation and retention of training attendance. Documentation of training shall include the workforce/extended workforce member's name, job title, date of training and type of training provided (e.g., basic privacy, comprehensive privacy). Training attendance documentation shall be retained for no less than six (6) years from the last date of the individual's active participation as a member of the workforce or extended workforce. When contractor staff are working as members of the extended workforce (i.e., directly controlled by the agency versus a business associate relationship) and are working under a departmental contract, the department contract administrator shall retain the training documentation for those contractors.

When a change is made to DHHS Privacy Policies or agency procedures, each workforce member whose function(s) are impacted by the change shall receive the instruction necessary to implement the change within a reasonable amount of time after the change becomes effective.

All current agency workforce/extended workforce members with direct, inadvertent, or incidental access to individually identifiable health information shall be required to sign a Confidentiality Agreement acknowledging their understanding of the agency's privacy policies and procedures and the consequences of any violation.

All new workforce/extended workforce members with direct, inadvertent, or incidental access to individually identifiable health information shall be required to sign a Confidentiality Agreement within a reasonable amount of time after employment, but no later than upon completion of privacy training.

Confidentiality Agreements shall be retained for at least as long as the individual remains a member of the workforce or extended workforce.

Sanctions against employees who fail to comply with the DHHS privacy policies and/or agency procedures shall be in accordance with the State Personnel Act and related personnel policies, except that the sanctions for educators subject to Chapter 115C of the North Carolina General Statutes (NCGS) shall be in accordance with NCGS 115C-325. Appropriate sanctions for non-compliant contractors and other workforce members who are not state employees shall be imposed consistent with the terms of their contracts or operative working arrangements.

Agencies must review each incident individually, taking into consideration the severity of the incident, circumstances surrounding the incident, the harm done to the client and to the agency, and any possible repercussions as a result of the use or disclosure made by staff. All instances of sanctioning shall be documented through existing personnel processes.

The DHHS Privacy Officer and Agency Privacy Official, if one is designated in the agency, shall be notified of any privacy violations and, to the extent permitted by law, any sanctions applied.

DHHS agencies shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the following reasons:

- exercising his/her privacy rights;
- participating in any process relating to privacy compliance;
- filing a complaint with the Secretary of the U.S. Department of Health and Human Services;
- participating in a privacy related investigation, privacy compliance review, proceeding, or hearing; or
- engaging in reasonable opposition to any act or practice that the person believes to be unlawful as long as the action does not involve disclosure of individually identifiable health information.

Retaliation shall not occur for individuals who make a disclosure to a health oversight agency, public health authority, or an attorney retained by or on behalf of the individual to determine legal options, provided that the individual believes in good faith that an agency has done any of the following:

- performed an unlawful act;
- violated professional or clinical standards; or
- endangered a client or the public through the care, services, or conditions provided.

An agency is not considered to have violated HIPAA Privacy Rules if a member of its workforce or extended workforce who is the victim of a criminal act discloses individually identifiable health information to a law enforcement officer about the suspected perpetrator and the health information is the minimum needed to appropriately address the criminal act.

All business practices shall provide for preventing intentional unauthorized disclosure of individually identifiable information to unauthorized parties through written or oral interactions, as well as minimizing unintentional conveyance. Business practices shall also provide for reasonable efforts to lessen any resulting harmful effects in the event that an agency should become aware of a HIPAA Privacy Rule violation by the agency or an agency's business associate.

HIPAA covered agencies, DHHS Internal HIPAA Business Associates, and any DHHS agency that performs oversight or other services for a DHHS HIPAA covered entity shall require agency workforce and extended workforce to wear some form of visible identification when performing job responsibilities for that agency. An agency that promotes a residential environment for their clients may be excluded from staff identification at the discretion of the appropriate agency management.

Each agency must determine a reasonable method of employee identification. The method need not be costly. When workforce or extended workforce members conduct business in person that is likely to include the sharing of an individual's health information, the workforce/extended workforce member shall prominently display official agency identification that contains the member's name.

*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](#).*