Title:	**DPH Privacy and Security Manual**
Chapter:	**II. Administrative Policies, Administrative Requirements (Privacy Protections)**
Current Effective Date:	**September 22, 2003**
Original Effective Date:	**April 14, 2003**
Revision History:	**May 14, 2004**

Purpose

The purpose of the Division of Public Health (DPH) Administrative Requirements privacy policy is to establish the process for developing and implementing specific policies to protect the privacy of individually identifiable health information (IIHI) within DPH. This policy is in compliance with the DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, that establishes the NC Department of Health and Human Services (DHHS) requirements for privacy polices to protect IIHI.

Policy Scope: The policy applies across the Division to all DPH workgroup.

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule requires covered health care components to comply with "Administrative Requirement," as specified in 42 CFR Part 164.50. These administrative requirements specify the requirements that an organization designated as a covered entity under the regulation must meet to achieve compliance with the Privacy Rule.

Policy

The Division of Public Health shall develop policies that are appropriate for its workforce to implement in order to protect the privacy of IIHI that is created, received, accessed, 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 relate to individually identifiable health information. The NC DHHS Privacy Polices, the HIPAA Privacy Rule, "*North Carolina General Statutes and Administrative Rules*", and other applicable federal and state laws and regulations will be the primary resources for DPH privacy policies.

Division of Public Health Responsibility

The Division of Public Health shall evaluate each Privacy policy based primarily on the HIPAA Privacy requirement and its related DHHS Privacy policy to determine whether the policy should be applied to all sections and business units within the Division regardless of the HIPAA impact. Determination for a Division-wide approach to policy requirements will take into account the most efficient and effective methods for ensuring the protection of IIHI while promoting consistency in the management of health information throughout the Division of Public Health.

The Division is responsible for providing resources to analyze the impact and applicability of the proposed privacy policies on the Division, develop and coordinate Division-wide privacy policies and associated implementation procedures, and provide support and guidance to workgroups within the Division affected by the privacy policies.

DPH Section/Unit Responsibility

It is the responsibility of the Division of Public Health sections, branches, and units that are performing HIPAA-covered functions to integrate HIPAA Privacy compliance procedures into their operations. Because workgroups have different program requirements and may conduct their business operations somewhat differently, specific requirements for implementing DPH Privacy policies must be based on workgroup-level requirements. Required procedural elements to be addressed by DPH workgroups will be identified by the DPH Privacy Office.

Retention and Disposition

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

Compliance

The Division of Public Health 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

As specified by the DPH HIPAA Compliance Statement and the DHHS Privacy Policy, Administrative Policies, Privacy Protections, the Division of Public Health shall develop policies that address administrative Privacy requirements so DPH business units will use and/or disclose IIHI in a confidential and secure manner. All policies shall be located in the Division of Public Health Privacy and Security Manual that is maintained by the Division Privacy Office.

The DPH policies to be developed, implemented, and maintained address the following Privacy requirements:

- **Privacy Officer**
  As specified in Division of Public Health HIPAA-Compliance Directive, the Division shall designate a Privacy Officer to oversee all ongoing activities related to the development, maintenance, and adherence to DHHS Privacy Policies regarding the privacy of and accessibility to IIHI, in accordance with State and Federal laws and applicable to business practices at impacted units.

- **Training**
  DPH shall develop policies regarding Privacy Training of all members of its workforce who are likely to have access to IIHI. At a minimum, Training shall be provided for newly developed Privacy policies and procedures during new employee orientation, and whenever significant changes are made to the Division of Public Health Privacy and Security Manual.

- **Safeguards**
  DPH shall develop policies that specify administrative, technical, and physical safeguards to protect the Privacy of IIHI from incidental access, unauthorized internal use, or inadvertent external disclosure to persons other than the intended recipient. Measures taken will relate directly to the size of the section / unit and the type of HIPAA-covered business activities that the unit undertakes.

- **Business Associates**
  DPH shall develop policies regarding the identification of "Business Associates" and develop Agreements that will limit the Business Associate's uses and disclosures of IIHI to those permitted by the Agreements.

- **Limitations on Information Access**
  DPH shall develop policies that limit access to IIHI 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 IIHI shall be required prior to disclosure of the requested information.

- **Use and Disclosure**
  DPH shall develop policies that specify the conditions necessary before Sections/Units can use or disclose IIHI including policies on required authorizations/authorization content, on instances when authorizations are not required, and on requirements for the use of IIHI for Research, Marketing, or Fundraising purposes.

- **Client Rights**
  DPH shall develop policies that will afford clients appropriate protections and controls over their individually identifying health information maintained by DPH. Such controls shall include notifying clients of the Privacy practices in the Division and the client's right to request access to or amendment of their health information.

- **Documentation of Complaints and Designation of a Contact Person**
  DPH shall develop policies that provide a mechanism for receiving complaints from individuals regarding DHHS Division/Office 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**
  DPH shall develop policies that specify appropriate sanctions against members of its workforce who fail to comply with Division or Department Privacy requirements. Sanctions will be appropriate to the nature of the violation. Such sanctions will not apply to whistleblower activities, or to complaints or investigations.

- **Mitigation**
  DPH shall develop policies that define its mitigation procedures for Use or Disclosure of IIHI that is in violation of Division or Department requirements. Any harmful effect that is known to the Division or Department of a use or disclosure of IIHI that is in violation of its policies will be mitigated in an effort to prevent such future occurrences.

- **Refraining from Intimidating or Retaliatory Actions**
  DPH shall develop policies that prohibit intimidation, threats, coercion, discrimination, or other retaliatory action against individuals who file a Privacy complaint against the Division or Department; testify, or assist in an investigation or review of the Division or Department; or oppose any act or practice thought to be unlawful. The Division 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 DPH Privacy policies will address transition requirements for authorizations or other express legal permissions used by DHHS Divisions/Offices. To the extent permitted by the HIPAA Privacy Rule, Divisions/Offices 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 and DPH Privacy policy requirements.

- **Policy and Procedure Changes**
  DPH shall modify, in a prompt manner, its Privacy policies as necessary and appropriate to comply with changes in the State statutes, the federal HIPAA law and other federal law, program requirements, and ongoing business practices. Changes to policies may be made at any time, provided such changes are documented and implemented according to Division policy requirements. DPH workgroups shall modify in a prompt manner their operations to conform to the revised DPH Privacy policies.

DPH Privacy Policy Development and Approval Process

The process for policy development and is summarized below and is based on the NC DHHS HIPAA Office privacy policy development and approval process:

- The DHHS designated Privacy Officials will become part of a Privacy Official Work Group (POWG). The DPH Privacy Official and representatives from the DPH HIPAA Office will represent the Division on and participate in the POWG.
- The NC DHHS HIPAA Office will draft of each policy within a policy category based on the HIPAA requirements and their review of existing policies submitted by DHHS divisions. The HIPAA Office will solicit input from the POWG members when developing the draft policy
- The policy draft(s) will then be distributed to the entire Privacy Official Work Group for review and comment. The POWG will meet regularly to provide commentary and to review the impact of the proposed policy within their organizations. The DPH HIPAA Office will review with and solicit input from selected DPH workgroups where a proposed policy may have a major operational impact. The DPH HIPAA Office will also review selected policies with the DPH Office of Legal and Regulatory Affairs and DPH Human Resources staff to gain the legal and personnel impact of selected proposed policies. The DPH participants will provide Division comments.
- The HIPAA Office will revise the draft policies based on the review and comments from the POWG members and re-issue the draft to confirm that the requested changes were made.
- After the second POWG policy review, the DHHS HIPAA Coordinators will receive the policy to review.

  Division comments are documented on a worksheet that will accompany the policy draft(s) and will be submitted to the HIPAA Office a single person within the Division, (e.g., Privacy Official or HIPAA Coordinator). The DPH Privacy Office coordinates the review within DPH and provides the consolidated Division comments to the DHHS HIPAA Office.
- Final policy drafts will be sent to the HIPAA Attorney in the Office of the Attorney General for review. The HIPAA Attorney will be asked to review the policy in accordance with HIPAA requirements and to review the findings based upon the preemptive legal analysis. Approval from the HIPAA Attorney must be received before the policy is sent to the HIPAA Oversight Committee.
- After the HIPAA Attorney approval is received, the policy will be sent to the Oversight Committee for its review and approval. DPH management is represented on the HIPAA Oversight Committee. The DPH Privacy Office provides DPH management with final comments policy that is pending approval and the HIPAA Oversight Committee considers these comments.
- After a NC DHHS HIPAA Privacy Policy is reviewed and approved with input from the Division as appropriate, the DPH HIPAA Office develops a tailored version of the policy specific to the Division. The DPH HIPAA Office also develops implementation procedures specific to how the policy will be implemented within the Division as a whole or within the specific DPH workgroups to which the policy applies.

- The DPH HIPAA Office reviews the draft DPH policy and implementation procedure internally, involving representatives from affected DPH workgroups as necessary.
- After internal DPH review comments have been addressed and incorporated, the draft DPH policy is reviewed with DPH HIPAA management, and the Office of Legal and Regulatory Affairs and DPH Human Resources as applicable, for final comments and approval.
- The DPH policy is reviewed with the Division Director, or designee, and approved for publication and implementation.
- The approved policy is incorporated into the DPH Privacy and Security Manual.
- The DPH HIPAA Office works with the affected DPH workgroups to integrate the Privacy policy into their operations as needed.
- The DPH HIPAA Office develops policy-specific training and ensures that the affected staff is trained in the specific Privacy policy.

Reference: **DHHS Directive Number III-11; DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, DPH Privacy and Security Manual, DPH HIPAA Compliance Statement Policy, DPH HIPAA Compliance Statement, DPH Privacy Policy Scope, 42 CFR 164.530, NC General Statutes 130A, 10A NCAC**

For questions or clarification on any of the information contained in this policy, please contact the DPH Privacy Office at HIPAA.DPH@ncmail.net.