Title:	**DPH Privacy and Security Manual**
Chapter:	**I. DPH HIPAA Privacy Compliance, Policy Statement**
Current Effective Date:	**September 22, 2003**
Original Effective Date:	**April 14, 2003**
Revision History:	**May 14, 2004**

Statement to Comply with HIPAA - Administrative Simplification

This HIPAA Compliance Statement pronounces the North Carolina Department of Health and Human Services (DHHS) Division of Public Health's (hereafter, may be referred to as "Division" or "DPH") policy for complying with the Federal Health Insurance Portability and Accountability Act (HIPAA) - Title II, Administrative Simplification: 45 CFR Parts 160, 162, and 164; Public Law 104-191. Compliance will be performed and maintained as is applicable to Division of Public Health business activities.

Background

In 1996, Congress passed HIPAA into law. The intent of Administrative Simplification (Title II of the Act) is to force the government and private sectors of the health care industry into using a consistent electronic operating environment. The main goals of HIPAA are to decrease costs and improve revenue efficiencies associated with the payment cycle while providing a secure infrastructure that protects the privacy of every citizen's personal health information. Congress also gave the Secretary of the federal Department of Health and Human Services (HHS) the power to change HIPAA Regulations (Rules), providing flexibility to account for needs that will enable successful implementations across the industry.

The Administrative Simplification aspect of HIPAA requires the United States Department of Health and Human Services (HHS) to develop standards and requirements and maintenance of health information that identifies individual patients. These standards are referred to as the HIPAA Regulations (or Rules).

Health care organizations that qualify as health plans and health care clearinghouses, or health care providers who submit standard transactions electronically must comply. A health care organization that must comply is referred to as a Covered Entity.

Each HIPAA Regulation has a different required compliance date depending on when the regulation is finalized. After a regulation is finalized, a covered entity has 24 months to comply.

The HIPAA Regulations and their purpose are as follows:

Electronic Transactions and Code Sets (Primary Compliance date – 10/16/2003):

Purpose is to Standardize Transactions (such as claims, enrollments, payments, etc.) and Code Sets (such as procedure, diagnosis, dental, drug) for individually identifiable health information in electronic form.

Privacy (Primary Compliance date – 4/14/2003):

Purpose is to guarantee individuals new rights and protections against misuse of disclosure of their health records, in any form, by developing and implementing processes for keeping that information Private. Patients have new rights to request access to and amendment of their records and to be provided an accounting of how their information was used, to whom it was disclosed, and for what purposes.

Security and Electronic Signature (Primary Compliance date – 4/21/2005):

Purpose is to safeguard and verify the integrity of electronically transmitted, stored, or maintained health information as it moves over internal systems, networks and Internet by enhancing the Security measures.

Identifiers (Primary Compliance date – Employer ID 7/30/2004):

Purpose is to have one *identifying number* for employers, providers, and health plans. This would eliminate the need to maintain multiple numbers signifying the same single entity thus streamlining this aspect of health information processing. Standards for national Health Plan Identifiers and national Provider Identifiers are pending.

Enforcement and Penalties

Enforcement of HIPAA regulations is the responsibility of the US Office of Civil Rights; however, regulations defining enforcement processes have not yet been published. Current HIPAA regulations specify severe civil and criminal penalties for non-compliance, including:

- Fines of $100 per violation occurrence or up to $25,000 for multiple violations of the same standard in a calendar year. These civil monetary penalties generally refer to violations of electronic transaction format standards.

- Fines up to $250,000 and/or imprisonment for up to 10 years for the intentional misuse of individually identifiable health information. These sanctions constitute criminal penalties for purposely-committed privacy and security violations.

DHHS as a Hybrid Entity and Significance for the Division of Public Health

The State Attorney General's Office has designated the North Carolina Department of Health and Human Services as a "Hybrid Entity". A Hybrid Entity is an organization whose primary function is not health care related, but which performs some health care function(s) that make it a Covered Entity. As a Hybrid Entity, DHHS is responsible for ensuring HIPAA compliance of, and oversight to covered health care components within the Department. In addition, other DHHS Divisions and Offices performing activities on behalf of the covered components wherein individually identifiable health information (IIHI) is exchanged, must comply. The Division of Public Health, while not a covered component at the Division level, has covered health care components within the Division and also has workgroups (business associates) that perform activities on behalf of covered components requiring the exchange and use of IIHI. These covered health care components and business associates must comply fully with the HIPAA Privacy Regulation. Other workgroups within DPH will comply with the general DHHS Privacy Policies as they are applied throughout the Division.

The scope of HIPAA impact within DHHS is subject to change as a result of HHS Rule modifications, and department programmatic or procedural modifications such as changes in billing procedures or development of new health care plans or health care clearinghouses. The Division of Public Health *Privacy and Security Officials* are responsible for monitoring department and Division change management activities to identify any changes impacting HIPAA scope and implement required compliance procedures.

Multiple Covered Functions with DPH

Although DPH is a Division within the NC single DHHS hybrid entity, it combines the functions and operations of multiple types of health care components (healthcare providers and business associate relationships) within a single organization. Each covered healthcare component (or business associate) must meet the requirements of the specific HIPAA regulations that apply to their particular type of healthcare component.

Compliance Approach

DPH will follow the approved NC DHHS compliance approach model within the Division's workgroups that are covered by the HIPAA regulations in an effort to achieve compliance:

- Understanding HIPAA
- Baselining the Organization
- Planning Compliance Strategies
- Remediating the Organization
- Validating Compliance
- Maintaining Compliance.

Refer to http://dirm.state.nc.us/hipaa/hipaa2002/complianceprocess/complianceprocess.html for information about the NC DHHS HIPAA Compliance Model and the detailed activities within each compliance step

Compliance with Electronic Transactions, Code Sets, Identifiers, and Security Regulations

The DHHS Division of Public Health will implement the requirements of these Rules in final form as they apply to business activities determined to be covered under HIPAA.

Compliance with the HIPAA Privacy Regulation:

The federal standards for Privacy of IIHI require changes in the protection of certain IIHI that is created, received, and maintained in any form or medium by DHHS. The DHHS Division of Public Health will implement an operating infrastructure that will protect the privacy of IIHI.

This infrastructure includes the appointment of permanent Division-wide Privacy official who will assume a leadership role in developing and administering the privacy program that ensures the protection of IIHI used, accessed, and maintained within the Division.

The Division will ensure compliance with HIPAA privacy requirements by developing and implementing privacy policies that specify the Division's methods for the protecting the privacy of IIHI. The Division of Public Health will also continue to comply with North Carolina statutes; which will preempt HIPAA when state statutes are more stringent than HIPAA. The Division will continue to adhere to all federal and state laws and regulations and program-specific requirements with respect to the protecting the privacy of health information while fulfilling its Public Health mission. In addition, and as part of its ongoing compliance, the Division will follow DHHS department-level HIPAA policies, procedures, and practices, as applicable.

All employees will follow general Privacy policies, developed by the Division of Public Health. Basic compliance activities will include participating in Privacy Training and signing a new Division Confidentiality Agreement. Additional Privacy policies, procedures, and forms will pertain specifically to covered healthcare components within the Division performing HIPAA covered business functions. These policies are also posted and available on the DPH web site and may be accessed at: http://www.schs.state.nc.us/hipaa/.

Reference: **DHHS Directive Number III-11; DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, 42 CFR Parts 160, 162, 164, 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 mailto:HIPAA.DPH@ncmail.net.