DHHS Directive Number III-11

Title:	**Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPPA), Public Law 104-191, Title II-Administrative Simplification**
Effective Date:	**January 12, 2009**
Original Effective Date:	**September 1, 2002**
Revision History:	**August 16, 2005; October 1, 2005**
Authority:	**G.S. 143B-10; 45 CFR Parts 160, 162 and 164**

Purpose

The purpose of this Directive is to declare the North Carolina Department of Health and Human Services (hereinafter referred to as "department" or "DHHS") policy for complying with the United States Department of Health and Human Services (HHS) Administrative Simplification rules in 45 Code of Federal Regulations (CFR) Parts 160, 162 and 164 under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

Background

HIPAA was enacted as a congressional attempt to reform health care. The purpose of the act is to:

- Improve portability and continuity of health insurance coverage in the group and individual markets;
- Combat waste, fraud, and abuse in health insurance and health care delivery;
- Promote the use of medical savings accounts;
- Improve access to long-term care services and coverage;
- Simplify the administration of health insurance; and
- Other purposes.

Title I of the HIPAA law addresses health care access, portability, and renewability with the intention of protecting health insurance coverage for workers and their families when they change or lose their jobs. Title II of the law, also known as "Administrative Simplification," deals with preventing health care fraud and abuse.

The "Administrative Simplification" aspect of that law requires HHS to develop standards and requirements for the maintenance and transmission of health information that identifies an individual. These standards are usually referred to as "HIPAA Rules."

The HIPAA Rules are designed to:

- Improve the efficiency and effectiveness of the health care system by standardizing the interchange of electronic data for specified administrative and financial transactions;
- Protect the security of electronic health information; and
- Protect the confidentiality of health information that identifies an individual.

The requirements outlined by the law and the rules promulgated by HHS are far-reaching. Health care organizations that qualify as health plans, health care clearinghouses, or health care providers who submit standard transactions electronically must comply.

HHS has been and will continue to publish HIPAA Rules to carry out the components of Title II, Administrative Simplification, of the HIPAA law. To comply with HIPAA, the following rules (which have the force of federal law) must be implemented by health plans, health care clearinghouses, and health care providers:

- Electronic Transactions (includes Standard Code Sets)
- Privacy
- Security
- Enforcement
- Unique Health Identifiers
    - National Provider Identifier
    - National Employer Identifier
    - National Health Plan Identifier
    - National Individual Identifier

HIPAA law contains significant penalties for non-compliance. The general penalty for failure to comply is:

- Each violation: $100;
- Maximum penalty for all violations of an identical requirement: may not exceed $25,000;
- Wrongful disclosure of individually identifiable health information offense: $50,000, imprisonment of not more than one year, or both;

- Wrongful disclosure of individually identifiable health information offense under false pretenses: $100,000, imprisonment of not more than 5 years, or both; and
- Wrongful disclosure of individually identifiable health information offense with intent to sell information: $250,000, imprisonment of not more than 10 years, or both.

Each HIPAA Rule has a different required compliance date. After each final rule is adopted, small health plans have 36 months to comply. Others, including health care providers, must comply within 24 months.

Hybrid Entity

The NC Office of the Attorney General has designated DHHS as a "hybrid entity," which is defined as a single legal entity that has health care components that perform functions covered by the HIPAA Rules. As a hybrid entity, the department is responsible for ensuring HIPAA compliance by and oversight of covered health care components within the department. DHHS is not responsible for the compliance with HIPAA requirements by locally managed entities (e.g., local public health authorities, county departments of social services, local managing mental health/developmental disabilities/substance abuse services entities).

Scope for HIPAA Rules: Covered Health Care Components

Based upon assessments of all DHHS divisions and offices, all or portions of several DHHS divisions and offices were determined to be covered health care components that must comply with the HIPAA rules. In addition, other DHHS agencies that perform activities on behalf of the covered components wherein individually identifying health information is exchanged must comply (such entities are hereinafter referred to as "internal business associates"). The official listing of DHHS covered health care components and Internal Business Associates that must comply with the HIPAA Rules is maintained by the DHHS Privacy Officer in the DHHS Office of Privacy and Security.

The scope of HIPAA impact within the department is subject to change as a result of programmatic or procedural modifications such as changes in billing procedures or development of new health care plans or health care clearinghouses. The DHHS Privacy Officer is responsible for monitoring department change management activities to identify any changes impacting HIPAA scope and notifying the impacted components of the requirements they must follow to achieve HIPAA compliance.

Multiple Functions

Although DHHS, as a hybrid entity, combines the functions and operations of multiple types of health care components (i.e., health care providers, health care plans, and health care clearinghouses) under a single legal entity, each covered health care component must meet the requirements of the HIPAA Rules that apply to that particular type of component.

Compliance Approach

The department shall utilize the compliance approach outlined below in the divisions and offices within the department that are covered by the HIPAA regulations in an effort to achieve in compliance with the HIPAA rules, in accordance with the compliance dates designated in each rule.

1. Understanding HIPAA
   (a) Identify funding and sponsors for the DHHS HIPAA Initiative
   (b) Establish a steering committee to oversee DHHS HIPAA Initiative efforts
   (c) Review HIPAA Rules
   (d) Provide HIPAA awareness training and training on final rules
   (e) Organize a team of people to track and manage HIPAA activities in the department
   (f) Develop a strategic plan for the HIPAA initiative including the mission, goals, and objectives of the effort
   (g) Establish DHHS due diligence documentation methodology and repository
   (h) Develop initiative-level roles and responsibilities
   (i) Develop a project management environment
   (j) Develop detailed work plans and a master plan for the initiative
   (k) Analyze the HIPAA rules against existing organization specific rules, directives, department policies, etc.
   (l) Analyze the HIPAA regulations against potentially preemptive, superceding, or conflicting State and Federal law

2. Baselining the Organization
   (a) Determine components within the DHHS hybrid entity that are performing functions covered under HIPAA

(b) Develop tools for assessing the department
(c) Identify external and internal business associates and electronic trading partners
(d) Document potential impacts (i.e., gaps)

3. Planning Compliance Strategies
   (a) Identify remediation opportunities
   (b) Develop business and technical remediation strategy and guidelines
   (c) Determine what needs to be done to close the gaps
   (d) Organize and/or recruit the staff necessary to close the gaps

4. Remediating the Organization
   (a) Develop/revise department policies and associated procedures
   (b) Determine department-wide remediation approaches
   (c) Implement HIPAA related policies and procedures throughout the department
   (d) Conduct appropriate levels of training for DHHS staff
   (e) Establish/amend formal trading partner agreements and business associate contracts as necessary
   (f) Modify and implement business processes, business application systems, and technical infrastructure as necessary to comply
   (g) Test and/or pilot modifications

5. Validating Compliance
   (a) Develop and deploy self-verification tools and/or techniques to verify compliance with HIPAA requirements
   (b) Determine if independent validation and verification (IV&V) techniques will be used in any of the HIPAA regulation areas
   (c) Solicit external IV&V assistance as necessary

6. Maintaining Compliance
   (a) Develop and implement ongoing compliance training programs for privacy officers, security officers, new employees, etc.
   (b) Develop and implement an audit program to ensure ongoing compliance
   (c) Establish change management processes to identify changes in HIPAA scope and laws

Compliance

DHHS as a hybrid entity is responsible for ensuring that all areas within DHHS that are impacted by HIPAA achieve and maintain compliance with the HIPAA rules. It is the goal of DHHS to achieve compliance by the compliance dates specified in each rule. The Division of Information Resource Management (DIRM) will assume the leadership role in establishing the on-going operations of HIPAA Transactions, Code Sets, Identifiers, Privacy, and Security compliance.

DHHS Privacy Officer

DHHS shall designate a Privacy Officer who will assume the leadership role in the administration of a DHHS Privacy Program that ensures the protection of individually identifiable health information maintained in the department. This shall be accomplished through the development and implementation of privacy policies for the department, by overseeing the development of procedures related to privacy and by monitoring privacy practices for compliance with privacy policies throughout the department.

DHHS Security Officer

DHHS shall designate a Security Officer who will assume the leadership role in the administration of the DHHS Security Program. Responsibility for establishment of security policies and programs for DHHS is delegated to the Director of the Division of Information Resource Management as outlined in DHHS Directive Number II-12 and the DHHS Privacy and Security Policies.

APPROVED

_____

Lanier M. Cansler, Secretary
Department of Health and Human Services