

DHHS Directive Number II-48

Title: Delegation of Authority to the Director, Office of Privacy and Security
Effective Date: October 5, 2010
Revision History: G.S. 143B-10
Authority:

Purpose

To delegate, clarify and specifically confirm certain authorities of the Secretary of the Department of Health and Human Services (DHHS) to the Privacy and Security Office (PSO). These authorities are delegated under the supervision of the Chief Information Security Officer (CISO), and shall be reported to the Secretary through the Chief Information Officer and Assistant Secretary for Finance and Business Operations for the department.

The DHHS Privacy and Security Office supports the mission of the Department of Health and Human Services by providing the department and departmental divisions/offices with; privacy, security, business continuity, and Health Insurance Portability and Accountability Act (HIPAA) oversight; security consulting, monitoring and testing services; Information Technology (IT) Policy and planning services.

Privacy oversight services shall include, but not be limited to, assistance in: (1) privacy policies, standards, procedures, and guidelines research, analysis, and development; (2) privacy compliance monitoring; (3) short and long term privacy goal planning; (4) assistance in privacy incident resolution.

Security oversight services shall include, but not be limited to, assistance in: (1) security policies, standards, procedures, and guidelines research, analysis, and development; (2) security compliance monitoring; (3) short and long term security goal planning; (4) system-wide security and protection against both deliberate and accidental intrusions and disasters; (5) project review for privacy, security, and BCP requirements; (6) risk management implementation and coordination.

Security consulting, monitoring, incident response and testing services shall include, but not be limited to, assistance in: (1) application, network/system, administrative, physical and software security planning; (2) telecommunications and network security design; (3) network security monitoring; (4) application and system security testing and validation; (5) forensic analysis, investigation and incident response assistance.

Business continuity oversight services shall include, but not be limited to, assistance in: (1) BCP and Continuity of Operations Planning (COOP) policies, standards, procedures, and guidelines research, analysis, and development; (2) BCP and COOP compliance monitoring; (3) short and long term BCP and COOP goal planning; (4) technical assistance and consultation in all areas related to business continuity, disaster recovery and the continuity of operations of the department and departmental divisions/offices; (5) development and review of business continuity, disaster recovery and COOP plans; (6) coordinate and delegate BCP, COOP and disaster recover efforts.

HIPAA oversight services shall include, but not be limited to, assistance in: (1) HIPAA policy, standard, procedure, and guideline research, analysis, and development; (2) HIPAA compliance monitoring; (3) short and long term HIPAA goal planning; (4) technical assistance and consultation in all areas related to HIPAA; Privacy, Security, Transaction Code Identifier, and National Provider Identifier (NPI).

IT Policy and planning services shall include, but not be limited to, assistance in: (1) IT policies, standards, procedures, and guidelines research, analysis, and development; (2) coordinate internal and external IT policy review; (3) IT policy compliance monitoring; (4) Statewide IT policy guidance; (5) IT policy deviation approval.

Delegation of Authority

DHHS Chief Information Security Officer

DHHS shall designate a Chief Information Security Officer who will assume the management and leadership role in the administration of the DHHS Privacy and Security Office. The CISO shall serve as both the Security and Privacy Official for the department

For the purpose of creating a transparent and collaborative departmental privacy and security effort all Division/Office Privacy, Security Business Continuity Officials shall have a “dotted-line” reporting relationship to the Chief Information Security Officer.

As provided in G.S. 143B-10(a), the Secretary of the Department of Health and Human Services delegates the following functions concerning departmental security management and administration to the DHHS Privacy and Security Office:

1. The DHHS Privacy and Security Office, in coordination with the Chief Information Security Officer, may employ the use of data capturing tools with the authority to monitor all division networks and employees or those in their charge and to perform application or system security testing or validation to ensure

compliance with applicable policies and standards and to maintain an acceptable level of security posture required to protect departmental, agency and state networks.

2. The DHHS Privacy and Security Office is authorized to download, install and run security programs or utilities that reveal weaknesses of agency networks and systems or allow for the monitoring of agency employees or those in their charge.
3. The DHHS Privacy and Security Office has the authority to obtain upon request, temporary administrative access to divisional systems and devices as required in the investigation of an incident, the need to monitor activity or in the conducting of any security related testing or validation.
4. When dealing with a suspected incident, the DHHS Privacy and Security Office, in coordination with the Chief Information Security Officer, shall have optional oversight on all incidents pertaining to the department, its divisions/offices and those in their charge. During the course of any incident the DHHS Privacy and Security Office will have the option of conducting the incident investigation. During the conduct of an investigation or in response to an incident, the DHHS Privacy and Security Office have the right to view material that is in direct conflict with DHHS departmental policy.

During the investigative course of a suspected incident the DHHS PSO shall make every effort to contact appropriate division/office management. However; should a division/office representative be unreachable the DHHS PSO shall have the authority to take the action they deem necessary at that time.

5. In coordination with the Chief Information Officer, Assistant Secretary for Finance and Business Operations, and the Secretary, the DHHS Privacy and Security Office shall serve as the department's principle advocate and liaison on matters of privacy and security policy with federal, state, and local agencies. The Chief Information Security Officer shall serve as the principle advisor to the department's executive management team on all privacy, security, BCP and HIPPA issues, and provide appropriate consultation and guidance to all divisions/offices and agencies within the department to ensure compliance with established policies.
6. The Chief Information Security Officer shall assist in and coordinate the development of short and long range strategic privacy, security and business continuity plans for the department and departmental divisions/offices. In coordination with the Chief Information Officer, Assistant Secretary for Finance and Business Operations, and the Secretary, the CISO shall establish requirements for such plans, and shall monitor the implementation of the plans. The requirements for the plans shall address the management of the department's and departmental divisions/offices' data as an organizational resource.

7. The DHHS Privacy and Security Office shall review and approve the privacy, security, and BCP for all department projects and the acquisition of all information resource management (IRM) resources (e.g., computer hardware, software, consulting services, etc.) proposed by all departmental divisions/offices and related agencies, regardless of funding source. The review shall include, but not be limited to, a determination of whether or not the IRM resources proposed to be acquired meet the requirements that have been specified by the purchasing division or agency. The Privacy and Security Office's approval or disapproval shall be consistent with applicable federal, state, or departmental policies, standards, and guidelines. The Privacy and Security Office shall promptly communicate any concerns, problems, or difficulties determined in its review to the appropriate departmental division director in an effort to seek a possible solution. Should a solution not be established, the Privacy and Security Office shall notify the Chief Information Officer, Assistant Secretary for Finance and Business Operations, and the Secretary.
8. The DHHS Privacy and Security Office shall monitor and ensure that departmental system designs and applications are consistent with the State, Federal, departmental regulations, policy, standards and procedures. The Privacy and Security Office shall ensure that consistent technical security standards are developed, maintained, and followed in the design and implementation of the entire department and departmental division IT systems.
9. The Chief Information Security Officer shall serve as the department's principle liaison with the State CIO in information technology security matters.
10. The Chief Information Security Officer shall consult with and keep the Chief Information Officer, Assistant Secretary for Finance and Business Operations, and the Secretary informed on all priority issues related to the privacy and security impact of new technology, the delivery of automation services, and the operation of automated systems within the department.
11. The Privacy and Security Office shall develop an enterprise-wide risk management implementation methodology and shall be responsible for the conduct of risk assessment for the department.
12. The Privacy and Security Office, in coordination with the Chief Information Officer, Assistant Secretary for Finance and Business Operations, and the Secretary, shall assist IT audits conducted by state and federal agencies external to DHHS.
13. The Privacy and Security Office shall develop and implement an enterprise-wide privacy, security, BCP and HIPAA awareness training program and provide training to DHHS divisions and offices.

This delegation of authority shall not deprive the Secretary from performing, in lieu of the Chief Information Security Officer, any of the acts set forth above. This delegation of authority may be amended or withdrawn by the Secretary at any time and without notice. This delegation of authority shall not apply to any action, which by law, state policy, or Governor's Executive Order, may only be executed by the Secretary.

APPROVED

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