



North Carolina Department of Health and Human Services

2001 Mail Service Center • Raleigh, North Carolina 27699-2001
Tel 919-855-4800 • Fax 919-715-4645

Beverly Eaves Perdue, Governor

Albert A. Delia, Acting Secretary

DHHS Directive Number III-48

Title: Delegation of Authority to the Chief Information Security Officer and Privacy and Security Office
Effective Date: August 21, 2012
Revision History: August 21, 2012; October 5, 2010
Authority: G.S. 143B-10

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's Office through the 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; privacy, security, business continuity and HIPAA policy and planning services.

Privacy oversight services shall include, but not be limited to, assistance in: (1) privacy compliance monitoring; (2) short and long term privacy goal planning; (3) assistance in privacy incident and complaint resolution.

Security oversight services shall include, but not be limited to, assistance in: (1) security compliance monitoring; (2) short and long term security goal planning; (3) system-wide security and protection against both deliberate and accidental intrusions and disasters; (4) project review and approval for privacy, security, and Business Continuity Planning (BCP) requirements; (5) 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) compliance monitoring; (2) short and long term BCP and COOP goal planning; (3) technical assistance and consultation in all areas related to BCP, disaster recovery and COOP of the department and departmental divisions/offices; (4) development and review of BCP, disaster recovery and COOP plans; (5) coordination and delegation of BCP, COOP and disaster recover efforts.

HIPAA oversight services shall include, but not be limited to, assistance in: (1) HIPAA compliance monitoring; (2) short and long term HIPAA goal planning; (3) technical assistance and consultation in all areas related to HIPAA Privacy and Security, Transaction Code Identifier, and National Provider Identifier (NPI); (4) coordination of HIPAA activities with federal, state and local third-party agencies (5) serve as a liaison for HIPAA outreach.

Privacy, security, business continuity and HIPAA policy and planning services shall include, but not be limited to, assistance in: (1) privacy, security, business continuity and HIPAA policies, standards, procedures, and guidelines research, analysis, and development; (2) coordination of internal and external privacy, security, business continuity and HIPAA policy review; (3) privacy, security, business continuity and HIPAA policy compliance monitoring; (4) Statewide privacy, security, business continuity and HIPAA policy guidance; (5) privacy, security, business continuity and HIPAA policies, standards, procedures deviation approval.

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 Official and Privacy Official for the department.

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

Delegation of Authority

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 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 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.

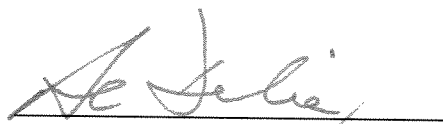
During the investigative course of a suspected incident, the DHHS PSO shall make every effort to contact appropriate division/office management. However; should a division/office representative be unreachable, the DHHS PSO shall have the authority to take the action deemed necessary at that time.

In coordination with the Secretary's Office, the DHHS Privacy and Security Office shall serve as the department's principle advocate and liaison on matters of privacy, security, BCP/COOP, and HIPAA 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.

5. The Chief Information Security Officer shall assist in and coordinate the development of short and long range strategic privacy, security, business continuity, and HIPAA planning for the department and departmental divisions/offices. In coordination with the Secretary's Office, 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.
6. 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 Secretary's Office and other departmental management as required to resolve the IRM issue.
7. 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.
8. The Chief Information Security Officer shall serve as the department's principle liaison with the State Chief Information Officer (SCIO) in information technology matters.
9. The Chief Information Security Officer shall consult with and keep the Secretary and other departmental management required 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.

10. 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.
11. The Privacy and Security Office, in coordination with the Secretary's Office, shall assist and facilitate all IT audits conducted by state, federal, and external third-party agencies.
12. 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.
13. All data exchange agreements between departmental, state, federal or third-party entities must be reviewed and approved by the Privacy and Security Office.
14. The Privacy and Security Office shall conduct, and where necessary, facilitate, the capture, monitoring, e-discovery and public records requests of electronic mail (e-mail).

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.



Al Delia, Secretary

Department of Health and Human Services