North Carolina Department of Health and Human Services
2001 Mail Service Center • Raleigh, North Carolina 27699-2001
Tel: 919-733-4534 • Fax: 919-715-4645

Michael F. Easley, Governor

Dempsey Benton, Secretary

September 9, 2008

MEMORANDUM

TO: DHHS Division/Office Directors

FROM: Dan Stewart, DHHS Deputy Security

RE: Disk Encryption Deployment Requirements and Status Reports

DHHS has experienced a number of laptop thefts resulting in the loss of confidential information and equipment which is problematic for obvious reasons. In addition, Statewide Information Security Manual, Chapter 3, Section 0801 requires DHHS to comply with the use of whole disk encryption. DIRM has analyzed the various encryption software solutions suggested by ITS and negotiated a very favorable price for the GuardianEdge solution which best meets our needs. Training in the use of GuardianEdge disk encryption was conducted May 28th and 29th. The GuardianEdge Software packages/passwords were released by the Division of Information Resource Management (DIRM) on June 17th.

By November 1, 2008, all laptops within DHHS must have GuardianEdge Disk Encryption installed with active encryption on the hard disk before the laptop system is permitted outside the user's office space. No exceptions will be permitted without written justification and approval by the appropriate division director on a case-by-case basis. Divisions/Offices are required to install the GuardianEdge product on all mobile devices. Laptops and other storage devices which are mission critical and utilize confidential data have first priority installation, followed by desktops in remote office locations that contain confidential information and then all remaining laptops, mobile and storage devices.

The DHHS Privacy and Security Office will be requesting status updates of each division's GuardianEdge deployments for laptops and remote satellite offices. Divisions/Offices should respond with current deployment numbers and estimated completion dates. Regular updates from each Division/Office will be requested until all Divisions/Offices are in full compliance with State Encryption Standards.

Staff should be advised to use due diligence in safeguarding both the information stored on laptops and other mobile storage devices. Locking laptops in secure locations when they are not being used is strongly encouraged. (For example, if an employee assigned a laptop leaves state service or is on vacation, the laptop should be secured.) In autos, laptops should be stored in the trunk of the vehicle or in an inconspicuous location if there is no trunk.

Thanks for assisting us in protecting our assets and confidential information.

cc: Dempsey Benton, Secretary
Karen Tomczak, Chief Information Officer
Pyreddy Reddy, Chief Information Security Office
Division/Office Security Officials