POLIC / ID# 2005-016
CLEARED BY: DBlair
DATE: 12-20-05

STATE OF ALABAMA DEPARTMENT OF
PUBLIC HEALTH

Donald E. Williamson, MD
State Health Officer

December 12, 2005

MEMORANDUM

TO: Office, Bureau, Division, and Branch Directors
Area Health Officers
Local Health Officers
Area Administrators and Assistant Area Administrators
Staff Assistants

FROM: Donald E. Williamson, M.D
State Health Officer

RE: Security Policy

Attached is the Department's Security Policy specifying the guidelines and procedures to be followed for safeguarding electronic Protected Health Information (e-PHI) and other sensitive information in accordance with the guidelines of the Health Information Portability and Accountability Act of 1996 (HIPAA).

This policy must be circulated to all employees. The Security Manual must be kept at each bureau/office/county. Supervisors are responsible for ensuring that current employees review the policy. Documentation showing the policy was circulated to all employees must be kept at the work site for audit purposes. All new employees must receive this policy as part of their orientation. The policy should be added to the "Employee Orientation Checklist" in the back of the Employee Handbook, and new employees must acknowledge review of the policy by initialing and dating the checklist.

Additional copies of the policy may be made from the attachment or obtained from the Alabama Department of Public Health's web site, (www.adph.org). This policy and the Security Manual can be found in the Document Library.

cap/
Attachment

POLIC / ID# 2005-016
CLEARED BY: D Blair
DATE: 12-20-05

ALABAMA DEPARTMENT OF PUBLIC HEALTH
SECURITY POLICY

POLICY

It is the policy of the Alabama Department of Public Health to safeguard e-PHI (electronic Protected Health Information) and other sensitive information in accordance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The ADPH policies and procedures to comply with all HIPAA requirements in detail are attached in the Security Manual.

GUIDELINES

The attached Security Manual provides detailed policies and procedures for each aspect of HIPAA compliance. Administrative Procedures, Physical Safeguards, Technical Security Services, and Technical Security Mechanisms are addressed very specifically. Most of the policies and procedures are technical in nature and will be implemented by Computer Systems Center technical staff. The specific guidelines, which apply to every employee, are as follows.

Personal computers, laptops, PDA and other electronic equipment are provided by the Department for business use and may contain information which must be protected from unauthorized access. User security rules include:

1. Only use Department furnished equipment and software. (Security Manual, III.C. Workstation and State Electronic Equipment Use Policy)
2. CSC/Tech Support will purchase and install all network-connected devices. (Security Manual, III.C. Workstation and State Electronic Equipment Use Policy)
3. All personal computers and laptops will have password protection and will have an automatic screensaver, which will activate after 15 minutes or less of unattended use. (Security Manual, III.C. Workstation and State Electronic Equipment Use Policy)
4. CSC/Tech Support will install software updates for security and antivirus weekly on personal computers. (Security Manual, II.F.2 Protection from Malicious Software)
5. Users will connect laptops to the network at least once a month, log into the master database, and receive updates for security and antivirus software. (Security Manual, III.D. Workstation Security Policy)
6. Users will back up critical data or e-PHI stored on their personal computer or laptop to their assigned folder on the server. Users do not need to back up data created and stored in an enterprise information system such as PHALCON, McKesson, or ACORN, because CSC/Tech Support automatically performs backups of these systems. (Security Manual, III.E.4. Data Backup and Storage)

7. The Department will require password changes every sixty days. Users will create a new password when prompted and will keep passwords secured. (Security Manual, II.F.4. Password Management)
8. Users will not use equipment for unlawful activities, distributing pornography, gambling, offensive/harassing messages and images. Supervisors will be responsible for monitoring employees' usage through observation and will handle violations in accordance with Department disciplinary procedures. (Security Manual, III.C. Workstation and State Electronic Equipment Use Policy)
9. Users should report suspected security violations, virus attacks, cyber criminal attacks, or physical compromises to CSC Support Desk immediately. (II.G.1 Security Incident Response and Reporting)
10. When an employee begins work and requires a computer and access to information systems, the bureau/office/local administrator will notify the CSC Support Desk. (Security Manual, II.E.2. Access Authorization)
11. When an employee leaves the Department or transfers to a new office, the bureau/office/local administrator will notify the CSC Support Desk and complete a Computer Access Removal Form. (Security Manual, II.E.2. Access Authorization)
12. When salvaging or transferring computer/electronic equipment, the Department must remove all sensitive or e-PHI from the device. To do that, the office/bureau will salvage the item using the Department equipment salvage procedures. CSC will properly destroy the memory storage components in the equipment. (Security Manual, II.E.1. Device and Media Disposal and III.E.2. Media Re-use)
13. ADPH facilities must be limited to authorized users and safeguarded from unauthorized access, tampering, and theft. Each office/bureau will have procedures for physical security to include locking, key control, electronic device and media protection, employee identification badges, and visitor logs. (III.B.2. Facility Security Plan and Security Manual, III.B.3. Physical Access Control and Validation Procedures)
14. Employees will wear ADPH identification badges. (Security Manual, III.B.3. Physical Access Control and Validation Procedures)

If additional information is needed, please contact the Computer Systems Center Support Desk at 334-206-5268.