Section V: **Physical Security**
Title: **Off-Site Storage Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **May 16, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To provide guidance on selecting a location for off-site storage of a Division or Office's confidential or critical data such as protected health information (PHI) or electronic protected health information (ePHI).

STANDARD

1.0 Background

To ensure that required functional capability can be maintained during a natural disaster or other significant emergency situation, organizations should consider storing confidential or critical operational data in an off-site location. Stored data must be protected and backed up so that a timely restoration can occur in the event of data loss. Organizations are responsible for ensuring the proper storage of their own data and shall also meet all applicable North Carolina (NC) Department of Health and Human Services (DHHS) policies and standards regarding data and equipment control.

2.0 Geographic Considerations

Organizations should consider both direction and distance when choosing an off-site storage location. The distance between the main site and the remote site should be great enough to minimize the risk of both facilities being affected by the same event (e.g., fire, explosion, hurricane, flood, etc.); however, the distance should not be so great as to hinder the timely recovery of critical data to sustain operations.

3.0 Protections and Controls

Many of the same physical security requirements that apply to an organization's offices will apply to sites chosen for remote data storage. A condition that an organization should consider when choosing an off-site storage location is whether the location has adequate access controls to minimize the risk of data loss or damage. If the agency does not have direct control over the remote location, the agency shall enter into a contract or service level agreement, as appropriate, with the owner of the remote location, which stipulates the specific controls and protections the owner must implement.

A Department-approved encryption method may be considered as one internal security control option to be used to protect confidential data in storage. If this option is selected, care should be taken to ensure through testing that data restoration actually works and that encryption keys are properly stored in a separate location from the data. See NC DHHS Security Standards, Network Security - Encryption Standard.

Below are just a few of the physical security issues to be addressed when choosing a location for off-site storage:

- Perimeter security and physical access controls
- Facility environmental requirements (i.e., fire suppression and detection equipment, HVAC systems, measures to prevent water damage, etc.)
- Secure transportation of media between the organization's offices and the off-site location

4.0 Data Recovery

Once a location or locations are selected, organizations must ensure that business continuity and disaster recovery plans are updated to include the process of data recovery from the designated off-site location(s). These plans should be tested in accordance with the requirements established in the business continuity and disaster recovery policies established by the Department and as required by state and federal regulations. Positive and negative test results should be factored in and used for process improvement to ensure optimal functionality as circumstances and technologies change.

Reference:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 3 - Processing Information and Documents, Section 05: Data Management
    - Standard 030502 - Managing Data Storage
  - Chapter 3 - Processing Information and Documents, Section 06: Backup, Recovery and Archiving
    - Standard 030603 - Managing Backup and Recovery Procedures
  - Chapter 9 - Dealing with Premises Related Considerations, Section 02: Data Stores
    - Standard 090202 - Managing Remote Data Stores
  - Chapter 9 - Dealing with Premises Related Considerations, Section 03: Other Premises Issues
    - Standard 090303 - Disaster Recovery Plan

- NC DHHS Security Standards
  - Network Security Standards
    - Network Security Standards
    - Encryption Standard
  - Physical Security Standards
    - Asset and Inventory Control Standard

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Physical and Environmental Security Policy