Board of County Commissioners
Leon County, Florida

Policy No. 05–3

Title:	Emergency Medical Services Division HIPAA Privacy and Security Policy (Health Insurance Portability and Accountability Act of 1996)
Date Adopted:	~~January 19, 2010~~ February 23, 2010
Effective Date:	~~January 19, 2010~~ February 23, 2010
Reference:	N/A
Policy Superseded:	Policy No. 03-19, Emergency Medical Services Division HIPAA Privacy Policy, adopted December 18, 2003; Policy No. 05-3, Emergency Medical Services Division HIPAA Privacy Policy, adopted April 12, 2005; Policy No. 05-3, Emergency Medical Services Division HIPAA Privacy Policy, amended January 19, 2010

It shall be the policy of the Board of County Commissioners of Leon County, Florida, that an updated policy entitled "HIPAA Privacy and Security Policy" is hereby adopted, to wit:

It is the policy of the Leon County Emergency Medical Services Division hereinafter "Division" that:

Purpose: The following privacy and security policy is adopted to ensure that the Division complies fully with all federal and state privacy protection laws and regulations. Person's Protected Health Information (PHI) is of paramount importance to Leon County Government.

Effective Date: This policy is in effect as of ~~January 19~~ February 23, 2010.

Expiration Date: This policy remains in effect until superceded or cancelled.

Availability: Documents, including but not limited to: policies, procedures and forms, related to HIPAA compliance shall be made available to all employees whose job function requires compliance with HIPAA policies and procedures. All forms, policies, and procedures will be available on the Leon County Government intranet site, through EMS Representatives or through the Privacy/Information Security Officer.

Definitions:
Administrative Safeguards: Actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and e-PHI and to manage the conduct of staff in relation to the protection of and authorized access to patient information.

4

Business Associate (BA): A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right. Also see Part II, 45 CFR 160.103.

Covered Entity (CE): Under HIPAA, this is a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. Also see Part II, 45 CFR 160.103.

Disclosure: Release or divulgence of information by an entity to persons or organizations outside of that entity. Also see Part II, 45 CFR 164.501.

Electronic PHI (e-PHI): Protected Health Information created, stored and or transmitted in an electronic format.

Health and Human Services (HHS): The federal government department that has overall responsibility for implementing HIPAA.

HIPAA: means the Heath Insurance Portability and Accountability Act of 1996.

Hybrid Entity: A voluntary designation for a single covered entity that performs both covered and non-covered functions. A covered entity may designate itself a hybrid entity to avoid the imposition of the privacy rules on its non-health care related functions.

Office for Civil Rights: The HHS entity responsible for enforcing the HIPAA privacy rules.

Physical Safeguards: physical measures, policies and procedures to protect our electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Plan Sponsor: An entity that sponsors a health plan. This can be an employer, a union, or some other entity. Also see Part II, 45 CFR 164.501.

Privacy/Information Security Officer: The individual who is responsible for maintaining, and revising when necessary, the privacy and security policies and procedures of the covered entity, or covered components of a hybrid entity.

Protected Health Information (PHI): Individually identifiable information, whether it is in electronic, paper or oral form that is created or received by or on behalf of a covered entity or its health care component.

Security Incident: A Security Incident is an attempted entry, unauthorized entry, or an information breach or attack on our electronic information system. It includes unauthorized probing and browsing of the files, a disruption of service from any cause, and incidents where electronic information has been altered or destroyed. Security incidents may include such things as a virus or a worm, or unauthorized use of computer accounts and computer systems. It may also include complaints or reports of improper use of our information system.

Technical Safeguards: The technologies and the policies and procedures for its use that protect PHI and e-PHI and control access.

Workforce: Under HIPAA, this means persons, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not hey are paid by the covered entity. Also see Part II, 45 CFR 160.103.

Workstation: Any electronic computing device, such as a desktop computer, laptop computer, PDA or any other device that performs similar functions and electronic medium is stored in its immediate environment.

1. GENERAL PROVISIONS

1.1 Privacy/Information Security Officer

It is the policy of the Division that the responsibility for designing, implementing, maintaining and revising when necessary procedure to execute this policy lies with the Privacy/Information Security Officer. The Deputy Chief of EMS Administration is hereby designated as the Division Privacy/Information Security Officer.

1.2 Employee, Contractor and Business Associate Access to PHI

It is the policy of the Division that access to protected health information must be granted to each person, contractor or business associate based on the assigned job junctions of the person, contractor, or business associate. It is also the policy of this organization that such access privileges should not exceed that necessary to accomplish the assigned job function.

1.3 Verification of Identity

It is the policy of the Division that the identity of all persons who request access to protected health information is verified before such access is gained. When transmitting e-PHI, a reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmittal.

1.4 Mitigation

It is the policy of the Division that the effects of any unauthorized use of disclosure of protected health information be mitigated to the extent possible.

1.5 Updates

It is the policy of the Division that the HIPAA policies, procedures, and practices shall be reviewed annually or when technology, laws, and regulations change. This update will include a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information to assure compliance with the HIPAA rules and regulations.

1.6 Business Associates

It is the policy of the Division that business associates must be contractually bound to protect health information to the same degree as set forth in 45 CFR 160 and 164 and in this policy.

1.7 Cooperation with Oversight Authorities

It is the policy of the Division that oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of this organization that all personnel must cooperate fully with all privacy and security compliance reviews and investigations.

1.8 Training

The Privacy/Information Security Officer shall be responsible for developing, maintaining and delivering training on an on-going basis to all employee and managers in order to achieve HIPAA compliance. Training and updates shall be provided to all current and newly hired employees who handle or maintain PHI, including but not limited to all employees of the Division.

1.9 HIPAA Violations

Any employee who fails to comply with the HIPAA policies or procedures shall be subject to disciplinary action as outlined in the Leon County Board of County Commissioners Personnel Policies and Procedures in effect on the date of the violation.

1.10 Emergency Access to e-PHI and PHI

To ensure that access to critical e-PHI is maintained during an emergency situation, the following emergency access procedures are established: If a system contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

2. PRIVACY POLICY AND PROCEDURES

2.1 Uses and Disclosures of Protected Health Information

2.1.1 It is the policy of the Division that protected health information (PHI) may not be used or disclosed except when at least one of the following conditions is true:

- The use or disclosure is for treatment, payment or health care operations;
- The individual who is the subject of the information (i.e. the "subject individual") has authorized or consented to the use or disclosure;
- The disclosure is to a personal representative of subject individual as specified by the subject individual;
- The disclosure is to the subject individual. The Privacy/Information Security Officer may deny access in certain limited instances;
- The disclosure is to the Department of Health and Human Services for compliance-related purposes;
- The use or disclosure is for one of the HIPAA "Public Purposes" (i.e. required by law, etc.).

2.1.2. It is the policy of the Division that PHI will not be used of any employment-related purpose other than those related to treatment, payment or health care operation.

2.1.3. It is the policy of the Division that no person, contractor, or business associate may condition treatment, payment, enrollment, or eligibility for benefits on the provision of an authorization to disclose protected health information.

2.1.4. It is the policy of the Division that privacy and security protections extend to information concerning deceased individuals.

2.1.5. It is the policy of the Division that all disclosures of protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure. It is also the policy of this organization that all requests for protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the request.

2.2. Notice of Privacy Practices

It is the policy of the Division that a notice of privacy practices must be published. This notice and any revisions to it will be provided to all subject individuals at the earliest practicable time, and all uses and disclosures of protected health information will be done in accord with this organization's notice of privacy practices.

2.43 Complaints

If a person believes his or her privacy rights have been violated, the person must submit a complaint in writing to the Privacy/Information Security Officer, either directly or through a Division representative.

The Privacy/Information Security Officer will evaluate the complaint and contact the person in writing within thirty (30) days with a response and suggested resolution of the complaint.

If the concern is not resolved to the person's satisfaction, the person should be advised of his or her right to file a written complaint with the Secretary of the United States Department of Health and Human Services.

It is the Policy of the Division that no person, contractor, or business associate may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations.

2.54 Reasonable Safeguards

Reasonable safeguards must be used to protect the security of written, electronic and oral PHI. To that end, employees should:

- Not leave written PHI in plain view of those who do not need access;
- Not discuss PHI in the presence of those who are not authorized to possess the PHI;
- Store PHI in locked cabinets or other secure areas when not in use;
- All paper, film, or other hard copy media containing PHI shall be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Use cross-cut shredder to destroy PHI when necessary;
- Maintain a secure facsimile location;
- Include a confidentiality statement on email and facsimile communications containing PHI.

2.65 Procedures to Request Access, Inspection and Copying of PHI

If a person desires to access, inspect, or copy his or her PHI, the Emergency Medical Services Division representative or Privacy/Information Security Officer will distribute a request form for a person to complete. Once the person has submitted the request in writing (using the County's form is optional), the Division representative must verify that the person's signature matches the signature on file. Alternatively, the person may sign the request in the presence of the Division representative.

Upon receipt of the verified written request, the Division representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the person's request and respond to the person within thirty (30) days from the date of the request. The Privacy/Information Security Officer can request an additional thirty (30) day extension as long as the request is made to the person in writing with the reason for the delay clearly explained.

The Privacy/Information Security Officer shall agree to all reasonable requests. If access is denied, the Privacy/Information Security Officer must provide the person with a written explanation for the denial as well as a description of the person's right to appeal. When the person has requested to access, inspect, or copy his or her PHI and the request has been accepted, the Privacy/Information Security Officer or other authorized Emergency Medical Services Division representative should accompany the person to a private area to inspect the records. After the person inspects the records, the Privacy/Information Security Officer, or other authorized Division representative, will note in the disclosure accounting log the date and time of the inspection, and whether the person made any requests for amendments or changes to the record.

When the person's request for a copy his or her PHI has been accepted, and the Division representative should copy his or her record within fourteen (14) days. The person shall be responsible for reasonable copy charges, which will be communicated to the person prior to any charges being incurred.

2.~~7~~6 Restriction Requests

It is the policy of the Division that serious consideration must be given to all requests for restrictions on uses and disclosures of protected health information as published in this organization's notice of privacy practices. It is furthermore the policy of this organization that if a particular restriction is agreed to, then this organization is bound by that restriction.

The Division representative or the Privacy/Information Security Officer will provide an original form for a person to complete when a person desires to request a restriction on certain uses and disclosures of his or her PHI.

Once the person has submitted the request in writing (using the County's form is optional), the Division representative must verify that the person's signature matches the signature on file. Alternatively, the person may sign the request in the presence of the Division representative.

Upon receipt of the verified written request, representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the person's request and respond to the person within thirty (30) days from the date of the request. The Privacy/Information Security Officer can request an additional thirty (30)-day extension as long as the request is made to the person in writing with the reason for the delay clearly explained.

The Privacy/Information Security Officer shall agree to all reasonable requests. If the restriction is denied, the Privacy/Information Security Officer must provide the person with a written explanation for the denial as well as a description of the person' s right to appeal.

2.87 Amendment to Protected Health Information

It is the policy of the Division that incorrect PHI maintained by this organization be corrected in a timely fashion. It is also the policy of this organization that notice of such corrections will be given to any organization with which the incorrect information has been shared. There are certain limited instances in which information may not be amended by this organization.

The Division representative or the Privacy/Information Security Officer will provide an original form for a person to complete when a person desires to amend of his or her PHI.

Once the person has submitted the request in writing (using the County's form is optional), the Division representative must verify that the person's signature matches the signature on file. Alternatively, the person may sign the request in the presence of the Division representative. The person must supply a reason to support the request.

Upon receipt of the verified written request, the Division representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the person's request and respond to the person within thirty (30) days from the date of the request. The Privacy/Information Security Officer can request an additional thirty (30)-day extension as long as the request is made to the person in writing with the reason for the delay clearly explained.

If the Privacy/Information Security Officer accepts the amendment request, the PHI correction shall be made and communicated to any parties to which the information was disclosed on or after December 29, 2003. The amendment shall not be communicated to any party to which the disclosure date was greater than six years prior to the amendment acceptance.

If the Privacy/Information Security Officer denies the request, the person may submit a short statement of dispute, which shall be included in any further disclosure of PHI.

2.98 Disclosure Accounting

It is the policy of the Division that an accounting of all disclosures of protected health information, with the exception of disclosures for treatment, payment and the Division operations, be given to subject individuals whenever such an accounting is requested. A person must request an accounting of disclosures in writing.

Once the person has submitted the request in writing, the Division representative must verify that the person's signature matches the signature on file. Alternatively, the person may sign the request in the presence of an Emergency Medical Services Division representative.

Upon receipt of the verified written request, the Division representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the person's request and respond to the person within thirty (30) days from the date of the request. The Privacy/Information Security Officer can request an additional thirty (30)-day extension as long as the request is made to the person in writing with the reason for the delay clearly explained.

A person may request an accounting for disclosures made up to six years before the date of the request but not for disclosures made prior to December 29, 2003. The first accounting request within a twelve-month period will be at no change to the person. Any subsequent request within the twelve-month period shall incur a reasonable charge for provision of the list. The person shall be notified of the charges before any costs are incurred.

2.~~10~~9 Request for Confidential Communications of Protected Health Information (PHI)

It is the policy of the Division that confidential communications channels be used, as requested by subject individuals, to the most reasonable extent possible. A person may request receipt of communication of PHI in a certain time or manner. The request must be in writing and must specify how or where the person requests to be contacted.

Once the person has submitted the request in writing, the Division representative must verify that the person's signature matches the signature on file. Alternatively, the person may sign the request in the presence of the Division representative.

Upon receipt of the verified written request, the Division representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the person's request and respond to the person within thirty (30) days from the date of the request. The Privacy/Information Security Officer can request an additional thirty (30)-day extension as long as the request is made to the person in writing with the reason for the delay clearly explained.

2.~~11~~10 Maintenance of Records of Protected Health Information (PHI)

All PHI shall be maintained for a minimum of six (6) years from the date of its creation or the date when it was last in effect, whichever is later, per HIPAA regulations.

Any statute or law which mandates more stringent records retention rules shall supercede HIPAA with regard to maintaining records.

2.~~12~~11 Disclosure Tracking

The Privacy/Information Security Officer shall be responsible for implementing and maintaining a PHI disclosure tracking mechanism (disclosure accounting log) to provide an accounting of all PHI disclosures. The Privacy/Information Security Officer shall provide instruction to the Division representatives regarding the process of documenting any PHI disclosures.

2.~~13~~12 Consent for Participation in the Big Bend Regional Health Information Organization

Patients who receive emergency medical transportation services from the Division may consent to having their PHI transmitted electronically to the Big Bend Regional Health Information Organization (BBRHIO), a regional health information exchange used for the purposes of diagnosis and treatment. The PHI provided to BBRHIO may be accessed by other health care providers through this system for diagnosis and treatment of the patient.

A Medical Records Release Authorization and Consent Form for participation in the BBRHIO shall be transmitted to each patient who receives emergency medical transportation services. Once the ~~person~~ patient, or parent, spouse, guardian, or other person with authority to consent, has submitted the consent for transmission of their PHI to BBRHIO in writing, the Division representative must verify the authenticity of the consent form.

Upon receipt of the verified written consent, the Division representative should forward the request to the Privacy/Information Security Officer for review.

The Privacy/Information Security Officer must review the request and approve inclusion of the PHI in the next electronic file transmitted to the BBRHIO. An accounting of such transactions shall be maintained by the Division.

3. SECURITY POLICY AND PROCEDURES

3.1 Workforce Clearance, Authorization, and Supervision

The Privacy/Information Security Officer shall review each newly hired, assigned, or reassigned employee's job function and determine if access to e-PHI is appropriate, and if so, the level of access required.

Personnel, including contractors, who have not been authorized to access e-PHI, shall be supervised at all times when working in areas where e-PHI is stored.

3.2 Unique User Identification

To uniquely identify and track one user from all others, for the purpose of access control to all networks, systems, and applications that contain e-PHI, and the monitoring of that access, each user must be provided with a Unique User Identification to be used to access e-PHI.

4

3.3 Security Password Management

3.3.1 To ensure that passwords created and used by the Leon County EMS Division to access any network, system, or application used to access, transmit, receive, or store e-PHI is properly safeguarded the following procedures are established:

- All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.
- Password "aging times" (i.e., the period of time a password may be used before it must be changed) may be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.

3.3.2. Staff members are responsible for the proper use and protection of their Unique User Identification and password and must adhere to the following guidelines:

- User Identification and passwords are only to be used for legitimate access to networks, systems, or applications.
- Authorized users must ensure that their User Identification and passwords are not documented, written, or otherwise exposed in an insecure manner.
- Staff members seeking access to any network, system, or application must not use another person's user identification and authorization information, nor may staff members allow the use of their User Identification.
- If a staff member or authorized user believes his or her User Identification has been compromised, they must report that security incident to the Privacy/Information Security Officer.
- A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access applications and database systems containing e-PHI.

3.4 Workstation Use and Security

The following procedures are put into place in order to implement physical safeguards for all workstations that access e-PHI and to restrict access to authorized users:

- Employees will only utilize workstations assigned to them for use and only those authorized to access and use the workstation will be permitted use thereto;
- All workstations are set with password protection so that the computer may not be accessed without the proper password;
- All workstations are set up to go "inactive" after a set time period, after the workstation goes inactive, access will not be permitted without the proper password;
- Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible;

- Workstations will be set so that staff members may not change or disable security settings, or access areas of the information system they are not authorized to access;
- Use of any dial up modems and remote access software to access the information system off site must be approved by the Privacy/Information Security Officer and Leon County MIS;
- Multiple network interface cards (NICs) that allow simultaneous network connections shall not be used in individual workstations unless approved by the Privacy/Information Security Officer and Leon County MIS.

3.5 Termination of Access

To ensure that access to the information system and e-PHI is terminated when an authorized person no longer has authorization for access, the following procedure is established:

- Supervisors will notify the Privacy/Information Security Officer when an authorized person no longer requires access to e-PHI so that access to the information system can be disabled.
- Access will be disabled on the effective date of the separation or, if still on the staff, the effective date when authorization for access has ended.
- The person will be removed from all information system access lists and all user accounts and he or she will turn in all keys and / or access cards that allow access to the information system.

This procedure applies to terminations in employment, retirement, resignation, leave of absence, or transfer to an area in the organization where the staff member is no longer authorized to access the information system.

3.6 Facility Access Controls and Security

Access to facilities will be based on the role of the staff person and their need to access a particular area, this access will be reviewed frequently by management and the Privacy/Information Security Officer.

The Privacy/Information Security Officer will maintain a current list of persons with approved access to e-PHI and the electronic information system. This list will include all people with access to e-PHI as well as all access devices, such as keys, issued.

The Privacy/Information Security Officer will be responsible for developing a facility security plan that protects buildings from unauthorized physical access, tampering, and theft. The plan will incorporate hardware, such as keypads or padlocks, to limit access to our buildings to only those persons with proper keys and/or access codes. The Privacy/Information Security Officer will ensure that this hardware allows the capability to alter codes or keys to allow access only to persons on the authorized persons list.

All guests and others with temporary access to the electronic information system that contains e-PHI shall sign or log in to the facility or access point. Access will be granted only upon presentation of verification of identity (such as a driver's license) and authorization to have access to the facility or access point.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to management or the Privacy/Information Security Officer.

Care will be taken to ensure that limitation of access does not hinder our ability to provide essential information needed for treatment and transport of patients, billing for our services, and health care operations.

3.7 Device and Media Controls

Leon County MIS carefully monitors and regulates the receipt, movement, re-use, and disposal of hardware and electronic media that contain e-PHI, PHI and other patient and business information.

3.7.1 Rendering Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

All Protected Health Information shall be served in all data states including data in motion, data at rest, data in use and data disposed. Electronic data containing protected health information in all states shall be secured in such manners as to constitute it unusable, unreadable or indecipherable to unauthorized individuals at all times, consistent with the guidance issued by the Secretary of the Department of Health and Human Services.

All hard disk drives that have been approved by the Privacy/Information Security Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been removed from the drive and shall certified to be free of any PHI by Leon County MIS.

In addition to routine backup, an exact copy of all e-PHI contained in each information system area will be created immediately prior to any movement, sanitizing or disposal.

No software, including computer games, screen savers, and anti-virus and anti-spam programs, may be downloaded without prior authorization from Leon County MIS.

The Privacy/Information Security Officer will establish procedures to ensure that an inventory of all software and hardware containing e-PHI will be developed and maintained:

- Assignment and documentation of identification numbers to hardware and other devices that are part of the electronic information system.
- Any discrepancies in the current inventory of software and hardware in comparison to the last inventory will be reported to management and will be investigated to ensure that there is a proper accounting of all Division software and hardware.

- All original/licensed copies of software, source codes, etc. shall be centrally stored in an area that is secure and environmentally safe so that the software is protected from destruction or damage as best as possible.
- A record shall be kept of all hardware or software that is added, moved, sanitized, reissued, or backed up and stored, including the name and signature of the person undertaking the action as well as the authorizing supervisor.
- The inventory will be conducted on at least an annual basis.

3.8 Maintenance Records

Any repairs or change outs of any security devices will be recorded in a log book maintained by the Facilities Management or the Privacy/Information Security Officer. The repair or maintenance records will contain, at a minimum:

- Name of person completing the maintenance or repair;
- Purpose of the maintenance or repair;
- Name of person authorizing it;
- Date and time the work started and ended;
- Brief description of the work completed and the outcome of it (more work required, alternative procedure to put in place, etc.).

The Privacy/Information Security Officer will periodically review the documentation of maintenance and repairs to determine trends or change in procedures to e-PHI security that should be made.

3.9 Information Activity System Review

Leon County MIS will periodically review records generated by the computer system. This review will be done to determine system functionality, log-in monitoring, detection of unauthorized attempts to gain access to e-PHI and to discover other security incidents.

3.10 Contingency Operations

3.10.1 Preserving Data and Electronically Stored Information, Creating Backups

The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain PHI and other essential business information. All servers, backup drives and other data storing hardware will be located in a secure area, with limited access.

At a minimum, backups must be made at sufficient intervals to ensure that critical data (especially PHI and e-PHI) can be restored and recovered immediately.

There will be verification that the backup was successfully completed at the end of each backup process. Logs will be maintained which contains the following information: 1) whether the backup was successful; 2) date and time the backup began and the date and time it was completed; 3) description of any problems encountered during the backup; 4) verification that a check was made to ensure that the backup was complete.

Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed. Revisions to the procedures shall occur as necessary.

3.10.2 Emergency Mode and Disaster Recovery Plan

A Disaster Recovery Plan will be established to ensure that, in the event of an emergency or disaster, each functional area of the Division can protect systems and information from loss or damage and that critical business processes for the protection and security of e-PHI can be maintained during an emergency. The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the Privacy/Information Security Officer and Leon County MIS. The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

The Disaster Recovery Plan must include:

- A data backup plan including the storage location of backup media.
- Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data.
- Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations.
- Procedures to periodically test data backup and disaster recovery plans.
- Procedures to periodically perform an application and data criticality analysis establishing the specific applications and e-PHI that is necessary to maintain operation in an emergency mode.
- Procedures to log system outages, failures, and data loss to critical systems.
- Procedures to train the appropriate personnel to implement the disaster recovery plan.

3.10.3 Facility Access Under Contingency Plans

Working with management, the Privacy/Information Security Officer will develop a list of persons to be notified when the contingency plan is in operation, as well as those people who have permission to access computer systems and secured areas when these contingency plans are in operation.

3.11 Applications and Data Criticality Analysis

Leon County MIS will assess the relative criticality of specific applications and data within the Division for purposes of developing its Data Backup Plan, its Disaster Recovery Plan, and its Emergency Mode Operation Plan.

The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

3.12 Security Incident Management

All staff members are responsible for immediately reporting a security incident or suspected security incident to the Privacy/Information Security Officer. The Privacy/Information Security Officer will be responsible for notifying Leon County MIS in order to identify and mitigate any damage to information or systems.

Whenever a security incident is suspected or confirmed, remedial action will be taken, including action against any individual staff members when it has been confirmed that they caused or contributed to the incident.

Following a security breach, an analysis shall be made to determine whether the protected health information was secured or unsecured in accordance with section 3.7.1 of this policy. The discovery of a breach of unsecured Protected Health Information shall result in the notification of each individual whose unsecured PHI that has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed during the breach. These notifications shall be made in accordance with applicable rules and regulations.