ASHLEY COUNTY MEDICAL CENTER

SECURITY POLICY AND PROCEDURE MANUAL

December 1, 2013

Dan Austin

Dan Austin
Security Officer

Phillip K. Gilmore

Phillip Gilmore
CEO

Policy Title: Security Management Process	
Policy Number: SC 01	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose:
The purpose of this policy is to describe the various components of Ashley County Medical Center's security management process.

B. Regulatory Reference:
Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.308(a)(1) of the HIPAA Security rule relating to the security management process.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center follows a documented 'Security Management Process' to implement and ensure the security of the hospital's physical and IT infrastructure. The security management process is defined in the hospital's security policies and procedures. The process is reviewed on a regular basis and is updated to accommodate changes in the physical and IT environments, operations, and applicable state and federal regulations.

III. Scope and Applicability:

This policy is applicable to the overall security management process followed by Ashley County Medical Center.

IV. Definitions:

Workforce Members shall include anyone who has access to protected health information at Ashley County Medical Center or performs any work for Ashley County Medical Center.

V. Responsibility:

Members of the Ashley County Medical Center workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Security Management Process: The Security Management Process (SMP) refers to the overall security plan of the hospital. It includes the security of both the physical and IT infrastructure of the hospital. The security management process is defined in terms of the hospital's security policies and procedures.

The security management process is designed based on the operational needs of various departments, hospital business needs, and to comply with the state and federal security regulations. Design of the security management process involves the following:

1. Risk Analysis
2. Risk Management
3. Security Policies and Procedures

These are described in detail below.

B. Risk Analysis: Risk analysis is a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if the measures were not in place.

The Security Officer and the Security Committee (SART) will perform risk analysis on an on-going basis and determine the best security solution/mechanism for the hospital's needs.

C. Risk Management: Risk management is the process of assessing risk, taking steps to reduce to an acceptable level, and maintaining that level of risk.

The Security Officer and the Security Committee (SART) will be responsible for determining and assessing the potential risks to the security infrastructure of the hospital. Proper security solutions/mechanisms should be implemented to either completely eliminate the risk or reduce the risk substantially and to maintain the risk at that level. Regular audits should be performed to ensure the risk level and whether it is being maintained at acceptable levels.

D. Security Policies & Procedures: The hospital's security management process is defined in the hospital's security policies and procedures. These policies and procedures are drafted, reviewed, and updated in accordance with the policy on 'Security policies and procedures'.

E. Sanctions policy: It is the policy of the hospital to ensure complete privacy and security of protected health information. Disciplinary actions may be taken against a workforce member who violates this policy. These actions will be in accordance with the policy on 'Workforce sanctions for privacy and security violations.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

All Security Policies and Procedures

IX. Related Documents:

None

Policy Title: Security Policy & Procedures	
Policy Number: SC 02	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose:
The purpose of this policy is to outline the procedures for defining and implementing the security policies and procedures of Ashley County Medical Center.

B. Regulatory Reference:
Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.308(a)(1) and 164.316 of the HIPAA Security rule relating to documentation standards (written policies and procedures).

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It's the policy of Ashley County Medical Center to protect and secure all forms of protected health information (PHI) and observe proper security policies and procedures as described in the hospital's "Security Policies and Procedures" manual. The hospital Security Officer is responsible for drafting the Security policies and procedures and to ensure that these meet the State and Federal security requirements.

III. Scope and Applicability:

This policy is applicable to all the security policies and procedures that have been or will be drafted and recommended by the Security officer and approved by the hospital Board.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Security Policies and Procedures Manual: The Security policies and procedures of the hospital are described in the hospital's "Security Policies and Procedures" manual. Each policy is numbered and has a revision, approval and an effective date.

The hospital's Security Officer maintains the master copy of the manual. A copy of the manual is on the hospital's Intranet Site. ~~The location is Policies | Security Manual.~~ There will be a paper copy ~~and an electronic copy~~ of the policies in the ~~safe at the Business Office~~ Security Officer's Office.

The hospital management considers the security of protected health information and hospital infrastructure as very critical and requires that all workforce members follow the proper security policies and procedures.

B. Drafting and Approving the Security Policies and Procedures: The hospital's Security Committee headed by the Security Officer will draft the Security policies and procedures. Any new policy or change in an existing policy must be approved by the hospital CEO. Upon approval the new or modified policy will be added to the "Security Policies and Procedures" manual with the proper version number and effective date.

C. Modifying the Security Policies and Procedures: The policies and procedures may need to be modified from time to time to take care of the changed security requirements due to environmental or operational changes, changes in technology or to comply with the state and federal requirements.

It will be the responsibility of the Security Officer to ensure that the Security policies meet all the requirements of applicable State and Federal regulations, standards and/or implementation specifications. The Security Officer or any member of the Security Committee can propose a new policy or a change in an existing policy.

In addition, any workforce member may propose a change in a Security policy or procedure. All such proposals must be accompanied with detailed reasons for the proposed change. The Security Committee will consider all such requests and establish if a change is required.

After detailed discussions the Committee may recommend a change. ~~For each new policy or change in an existing policy the Committee must prepare an "Impact Analysis Document" that describes the need for the proposed change, the impact of the proposed change on the existing Security environment, the cost and timeline of the proposed change, etc.~~

D. Documentation Requirements: All changes in the Security policies and procedures must be properly documented. All documentation must be maintained, for a period of 7 years from the date of its creation or the date when it last was in effect, whichever is later.

E. Who should follow the Security Policies & Procedures: All workforce members are required to follow the general Security procedures and safeguards to protect and secure patient PHI. The workforce members using computers or handling PHI in electronic format will be required to observe additional security procedures. These will be explained during the Security Training.

F. Enforcement: Each department head is responsible for enforcing the Security policies and procedures in his/her department. The Security Officer will be responsible for the overall enforcement. Any violations of the hospital's Security policies should be immediately reported to the respective department heads, a Security Committee member or the Security Officer.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

All Security Policies and Procedures

IX. Related Documents:

Security Policies and Procedures Manual

Policy Title: Designation of Security Officer and Security Committee	
Policy Number: SC 03	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy to establish the post of the Security Officer and designate the Security Officer as the contact to receive complaints, requests and provide information relating to hospital's security practices.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.308(a)(2) of the HIPAA Security rule relating to designation of Security Officer / IT Security Committee.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center will designate a Security Officer responsible for development and implementation of the hospital's Security policies and procedures and provide information relating to the hospital's Security practices. The Security Officer will head the hospital's Security Committee. The Security Officer will also receive any complaints or requests from an individual, workforce member and other persons related to the Security practices of the hospital.

III. Scope and Applicability:

This policy is applicable to the Security Officer, the Security Committee and the hospital management.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and

department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Designating required personnel: The hospital has designated the Director of Information Management Services as the Security Officer. The Security Officer will be responsible for managing all ongoing activities related to the development, implementation, maintenance of and adherence to the hospital's security policies and procedures in compliance with regulatory accreditation organizations, federal and state laws and the security practices of the hospital.

B. Security Committee: The hospital management realizes that security management and enforcement is a complex task and encompasses several areas of hospital's functions and facilities. To assist the Security Officer in implementing various security requirements and procedures, a Security Committee consisting of the following personnel is constituted:

1. CEO
2. Privacy Officer
3. Compliance Officer
4. CNO

The Security Officer will head the Security Committee. It will be called "Security Advisory and Response Team" (SART).

C. Responsibilities of the Security Officer: The responsibilities of the Security Officer are, but not limited, to the following:

1. Head the Security Committee and provide guidance for its functions.
2. Draft the security policies and procedures for the hospital.
3. Constantly review the security policies and procedures and modify them to take into account changes in technology, environment or operations and to comply with the applicable state and federal regulations.
4. Ensure the security of all computer systems, applications and electronic data.
5. Ensure proper and appropriate security training for the hospital workforce.
6. Ensure that all departments and workforce members comply with the hospital's security policies and procedures.
7. ~~Submit reports as needed and annually to the hospital management regarding hospital's compliance with its security practices.~~

D. Responsibilities of the Security Committee (SART): The responsibilities of the Security Committee are, but not limited, to the following:

1. Serve as an advisory committee on all security policy matters pertaining to hospital's security, including but not limited to security planning, budgeting, maintenance, and access.
2. Assist the Security Officer in enforcing the security policies and procedures.
3. Assist the Security Officer in testing and revising the security practices of the hospital.

E. Reporting to the Management: The Security Officer will submit a report as needed and annually to the hospital management. The report, at a minimum, should provide:
   1. General assessment of hospital's security compliance since the last report.
   2. Number and brief description of security incidents and violations reported. Actions taken to resolve or mitigate the harmful effects of such incidents or violations should also be reported.
   3. Plan for changing an existing security policy or procedure or adding a new one.
   4. Recommended or required changes in security/technology infrastructure.

F. Performance Review: The hospital's management will conduct an annual review of the Security Officer's performance based on the hospital's appraisal parameters and the Security Officer's role and responsibilities

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

None.

IX. Related Documents:

None.

Policy Title: Security Audits – Review and Evaluation	
Policy Number: SC 04	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy is to describe the procedures for on-going reviews of system activity and the periodic reviews and evaluation of hospital's security compliance.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.308(a)(1)(ii)(D) and of the HIPAA Security rule relating to Information System Activity Review.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of Ashley County Medical Center to conduct periodic review and evaluation of its internal security practices and controls. This includes review of records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The hospital workforce members should assist the Security Committee (SART) in conducting the periodic security reviews and evaluations.

III. Scope and Applicability:

This policy covers all computer and communication devices owned or operated by Ashley County Medical Center. This policy also covers any computer and communications device that are present on Ashley County Medical Center premises, but which may not be owned or operated by Ashley County Medical Center.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Types of Security Review: The hospital realizes the importance of conducting security reviews to ensure the efficiency of security practices and controls. The hospital conducts two types of security reviews:

1. On-going reviews: The hospital conducts on-going reviews of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews are generally done on quarterly basis or as and when required.

2. Annual review: The hospital conducts a complete annual review of its security practices, controls, infrastructure, policies and procedures.

B. Security Review Team: The Security Officer conducts the on-going reviews of information system activity. The annual review is conducted by the Security Officer and the Security Committee. External consultants may be engaged for conducting or assisting in the annual security review.

C. Information System Activity Review: The information system activity reviews are conducted on a periodic basis to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Investigate possible security incidents and to ensure conformance to hospital's security policies
3. Monitor physical access control logs
4. Monitor user or system activity where appropriate.

If a case of unauthorized access or any other form of security breach is detected during the review process, the reviewer will prepare a 'Security Incident Report' and resolve it as per the policy on "Reporting and handling of security incidents".

D. Security Practices Review: The hospital conducts a complete annual review and evaluation of its security practices, controls, infrastructure, policies and procedures. This includes the testing of hospital's Contingency Plans (Disaster Recovery plan and Emergency Mode Operations plan). The review also tests for compliance with applicable State and Federal regulations.

The review is done as per a written plan prepared by the Security Officer and SART. The findings of the tests and reviews performed are recorded.

Based on the findings of the security review, the Security Officer and SART will modify the hospital's security practices. They may also recommend changes in the security infrastructure.

E. Documentation of Security Reviews: The on-going and annual security reviews are performed as per a documented 'Review/Test Plan'. The reviewer, along with his/her recommendations, documents the results of the review. The Security Officer maintains the master copy of all the review reports and presents a summary to the management on an as needed and annual basis. Only ACMC IT Staff and Security Committee can access the Security Reviews.

All security review exercises are recorded in 'Security Review and Evaluation' log.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Reporting and handling of security incidents

IX. Related Documents:

Security Review and Evaluation Log

Policy Title: Workforce Security & Access Authorization Policy	
Policy Number: SC 05	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy is to ensure that all workforce members who work with electronic protected health information are authorized and it is determined that their access is appropriate.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections164.308 (a)(4) of the HIPAA Security rule relating to information access control

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of Ashley County Medical Center to determine that the access of a workforce member to electronic protected health information is appropriate and to authorize and/or supervise those workforce members who work with electronic protected health information.

III. Scope and Applicability:

This policy is applicable to all workforce members who work with electronic protected health information

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Determining clearance for access:

1. Department Heads/Supervisors will review individually the role of each existing and new workforce members to determine whether providing access to electronic protected health information is appropriate or not.

2. Department Heads/Supervisors will also determine the level of clearance to be given to each workforce members based on their functions and requirements to work with electronic protected health information. This is to ensure that workforce members have enough information to do their work but not more than it is necessary.

3. Also, when the role of a workforce member is changed and increased or decreased level of access is required, the Department Head/Supervisor will review the same and determine the appropriate clearance to be given.

4. Workforce members are not allowed access to PHI other than during their shift unless specifically required to attend to job duties.

B. Providing clearance for access:

The Department Head/Supervisor will communicate their clearance level decided by them for a workforce member to the Security Officer by signing the 'Workforce Access Authorization' form for providing access to the workforce member.

The extent to which the workforce members are cleared for access should be detailed, such as the hospital's applications, computer systems and any other areas where electronic protected health information is maintained and areas where physical access is allowed.

C. Authorization for access:

1. Manager Information Systems will issue the workforce member a log-in and password to use when accessing electronic protected health information maintained on the hospital's information systems.

~~2.~~ To physically access areas where electronic protected health information is maintained, the ~~Security Officer will review the clearance for the workforce member and program the IGuard Biometric Fingerprint Scanner, where available, or electronic keypads to enable access to the areas that have been approved~~ department manager must give the workforce member the access code to the keypads in those areas. Areas should be locked at all times with only authorized workforce members having access to the areas. ~~Areas where the IGuard Biometric Fingerprint Scanners are installed are:~~

~~a. Medical Records~~
~~b. Doctor's Dictation~~
~~c. Chargemaster Coordinator (old server room)~~

~~Areas where the IGuard Biometric Fingerprint Scanners are not installed are:~~

~~a. IMS Office and Server Room~~
~~b. Ashley Specialty Clinics~~
~~c. Ashley Health Services~~
~~d. Ashley Women's Services~~
~~e. Business Office~~
~~f. Home Health – stored in file cabinets (locked)~~
~~g. Warehouse~~

3. In case the clearance level of an existing workforce member has to be changed the Security Officer will modify the access authorization accordingly after the department head has filled out another 'Workforce Access Authorization Form'.

D. Restriction of access:
Security Officer will ensure that any access restriction to the hospital's information systems or physical areas are enforced. ~~for example; if a workforce member is not allowed access to the hospital's medical records room or server rooms, then the IGuard Biometric Fingerprint Scanner will not allow that workforce member access to the room.~~ Unauthorized persons, including family members of employees, are prohibited from utilizing any hospital equipment or device for accessing PHI/EHR.

E. Termination of access authorization:
1. Whenever any workforce member's services end or is assigned a new role that does not require access to electronic protected health information, the respective Department Head/Supervisor will immediately inform the Security Officer by filling out a 'Workforce Access Authorization Form'.

2. Security Officer will immediately terminate the workforce member's access by removing and or disabling the assigned log-in name and password.

~~3. The Security Officer will immediately recover from the workforce member any access cards, codes to disable physical access to areas where electronic protected health information is maintained.~~

4. The termination process described above must be completed within 6 hours of the Human Resources Director informing the Security Officer that a workforce member has been terminated or his/her role has been changed.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Facility Access Controls
System Access Control and Emergency Control
Entity Authentication

IX. Related Documents:

Workforce Access Authorization Form

Policy Title: Reporting and Handling of Security Incidents	
Policy Number: SC 06	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy is to describe how security incidents should be reported and how the security committee (SART) should handle them.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Section 164.308(a)(6) of the HIPAA Security rule relating to security incidents.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Workforce members should respond all security incidents to the Security Committee (SART). SART is responsible for investigating, reviewing and responding to any security incident that may jeopardize hospital's computer network and security infrastructure.

III. Scope and Applicability:

This policy applies to reporting of security incidents by the workforce members and responding to the security incidents by SART.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Security Incidents: A security incident refers to a breach in the security infrastructure of the hospital. Ashley County Medical Center classifies the security incidents in the following two categories:

1. Physical Security Incident: A breach in the physical security or physical security system of the hospital facilities is called a 'Physical Security Incident'. Examples of physical security incidents are:
    a. Unauthorized access to an area secured by a Physical Access Control system.
    b. Damage to locks or other Physical Access Control systems installed to secure areas of the hospital facilities.
    c. Presence of an unauthorized person in an area the person is not authorized to be in.
2. IT Security Incident: An 'IT Security Incident' is any IT related activity that violates an explicit or implicit security policy and has a negative security implication. Examples of IT security incidents are:
    a. An attempt to breach authentication or security measures
    b. Any release of a virus or worm
    c. Unauthorized attempt to gain access to any other account, server, host, or network

B. Reporting Security Incidents: Any workforce member who becomes aware of a security incident should immediately report it to the Security Officer, a member of the Security Committee (SART) or the department head or supervisor. The department head or supervisor should then report it to the Security Officer, a member of SART. The security incident may also be reported by sending e-mail to dan.austin@acmconline.org.

The security incident should preferably be reported on "Security Incident Report" form. If an incident is reported verbally or through e-mail to the Security Officer or a member of SART, then they should fill out the "Security Incident Report" form.

C. Responding to Security Incidents: It is the responsibility of the Security Officer and SART to respond to every security incident in a prompt and efficient manner so as to minimize any potential harmful effects. Responding to a security incident involves several steps, as described below:

1. Classifying the incident
2. Investigating the incident
3. Resolving the incident
4. Documentation

These steps are described in detail below.

D. Classifying Security Incidents: Each security incident should be classified as High, Medium or Low risk depending on the severity of the breach and its impact on the security of the hospital facilities and infrastructure. SART will develop criteria to classify the security incidents in these three categories and the response time for each category.

E. Investigating Security Incidents: Each security incident must be thoroughly investigated. The Security Officer may investigate the incident or may assign the responsibility to one or more members of SART. The investigation will include, but not limited to:

1. Person, if any, responsible for the security incident
2. Cause of the security incident
3. Period of the security incident
4. Effect of the security incident

The person/team investigating the security incident will document its findings in an investigation report. The investigation of security incidents should be completed as soon as possible.

F. Resolving Security Incidents: After investigation of a security incident is completed, the Security Officer will try and promptly resolve any issues related to the security incident. These may involve implementing new or updated security mechanisms; revising security procedures; implementing a new or updated IT technology; etc.

If a workforce member is found to have willfully breached the security practices that compromised the privacy and security of protected health information, then appropriate actions will be taken in accordance with "Workforce sanctions for privacy and security violations".

G. Documentation and Management Reporting: The security incidents must be properly documented. A 'Security Incident Log' will be maintained. The log will contain a summary of the incident and its resolution. Each entry in the log will be a security incident and will be linked to the following documents corresponding to that security incident:

1. Security Incident Report form

The Security Officer will present a summary of the security incidents in the as needed and annual management report.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it

is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Workforce Use and Security

IX. Related Documents:

Security Incident Report form
Security Incident Log

Policy Title: Security Awareness Training	
Policy Number: SC 07	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the hospital's requirement of training the workforce members in hospital's security policies & procedures.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Section 164.308(a)(5) of the HIPAA Security rule relating to Security Awareness Training.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of Ashley County Medical Center that all hospital workforce members, including full-time and part-time employees, contract employees, volunteers and medical students, should attend and successfully complete the appropriate course in hospital's Security policies and procedures.

In the event of changes in hospital's Security policies & procedures all or certain workforce members affected by the changes are required to undergo remedial training.

III. Scope and Applicability:

This policy is applicable to all existing workforce members and any new members who join the hospital workforce.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Type of Training Programs: Ashley County Medical Center requires that each workforce member undergo "Security Awareness Training" based on his/her roles and responsibilities. For this purpose, the Security Officer may plan different training programs for different workforce members depending on their responsibilities and the degree of access to confidential healthcare information. There would be at least two separate security training programs:

1. General Security Awareness Training: To be undertaken by 'all' workforce members.
2. ~~IT Security Training: To be undertaken by workforce members who use computers and other IT infrastructure.~~
3. In-depth Security Training: To be undertaken by the Security Officer, the members of the Security Committee (SART) and certain designated persons from the Administration office and other departments.

The Security Officer, in consultation with the appropriate Department heads, will determine the type of training program a workforce member must undergo.

B. Content of the Training Program: The Security Committee (SART) is responsible for developing a security training curriculum for the hospital workforce. External consultants may be used for designing and developing the curriculum.

The 'General Security Awareness Training' program should train all the workforce members in:

1. Brief overview of the federal and state security requirements
2. Basic security safeguards to be observed by all workforce members
3. Physical access control systems
4. Security incident reporting
5. Certain other security policies & procedures

~~The 'IT Security Training' program should train the workforce members who use computers and other IT infrastructure in:~~

1. Proper and secure use of IT infrastructure including proper use of workstations, servers, other media, etc.
2. Importance of monitoring login success/failure, and how to report discrepancies.
3. Virus protection, including training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the

introduction of a virus to a computer system, and what to do if a virus is detected.

4. Password management – rules to be followed in creating and changing passwords and need to keep them confidential

The 'In-depth Security Training' should train certain designated workforce members who are responsible for maintaining the security of the hospital physical and IT infrastructure in the following:

1. Detailed discussion of hospital's security policies and procedures
2. Detailed discussion of hospital's Disaster Recovery plan
3. Detailed discussion of hospital's Emergency Mode Operation plan

In the event of a change in hospital's security policies and/or related procedure(s), due to change in technology environment or operations, or due to changes in State or Federal regulations, the training program shall be suitably modified, if required.

C. Training Requirements: All workforce members must undergo and successfully complete the appropriate security-training program. An individual who joins the hospital workforce after April 1st, 2005 shall undergo applicable security training as part of the orientation program.

D. Security Reminders: Besides the security training, the workforce members will be kept aware of the security requirements and concerns on an on-going basis through security reminders. The Security Officer will send the security reminders either through e-mail or 'Inter-office Memo'.

E. Record of Training: Carelearning will keep a log of all employees that have taken the training

F. Confidentiality Agreement: Each workforce member must sign a 'Confidentiality Agreement' in accordance with the hospital's policy on 'Confidentiality Agreements with workforce members'.

G. Continuing Education & Training: Each workforce member must undergo security training once every year even if there is no change in the hospital's security policies and procedures. In the event of change in the security policies and/or related procedures the Security Officer will determine which workforce members need to receive training.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it

is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Confidentiality Agreement with workforce members

IX. Related Documents:

None

Policy Title: Contingency plan policy	
Policy Number: SC 08	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy ensures that an appropriate plan is established for responding to a contingency situation that may damage the hospital's information systems that maintain electronic protected health information.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.308(a)(7) of the HIPAA Security rule relating to contingency plans.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center will establish an appropriate plan for responding to an emergency or other occurrence such as fire, vandalism, systems failure or natural disaster that damages the hospital's information systems where electronic protected health information is maintained. This 'Contingency Plan' will be reviewed, tested and updated on a regular basis.

III. Scope and Applicability:

This policy is applicable in case of a contingency situation such as fire, vandalism, systems failure or natural disaster

IV. Definitions:

V. Responsibility:

The Security Officer and the Security Committee will be responsible for drafting and executing the Contingency Plan(s).

VI. Procedure:

A. Contingency situations:
A contingency situation is any emergency or other occurrence such as fire, vandalism, systems failure or natural disaster that damages the hospital's information systems where electronic protected health information is maintained.

Even when an emergency is not on a large scale and life threatening but results in the damage to information systems where critical data is maintained causing loss of electronic protected health information, the situation will be considered a contingency situation.

B. Plans to respond to a contingency situation:
To effectively respond to a contingency the hospital has established the following plans to be put into effect (refer to the individual plans for details):

1. Data contingency/backup plan: The hospital safeguards electronic protected health information by maintaining exact retrievable copies of the data and keeping them in a secure location for restoration of lost data due to a contingency situation.

2. Disaster recovery plan: The hospital will restore the data lost due to a contingency as per the procedures detailed in the hospital's Disaster Recovery Plan.

3. Emergency mode operation plan: The hospital has established procedure detailed in the Emergency Mode Operation Plan to enable continuation of critical business processes such as making protected health information available for providing treatment to individuals.

C. Responding to a contingency situation:
1. Mitigation: The Security Officer along with the management of the hospital will immediately take appropriate steps to mitigate the effects due to a contingency situation and safeguard the electronic protected health information.
2. Damage Assessment: The hospital has formed a Security Advisory and Response Team (SART) that will assess a contingency situation and will activate the appropriate plan to respond to the situation.

D. Documentation: The Security Officer will document the damage caused and any harmful effects due to the contingency situation. The mitigation and corrective measures implemented will also be documented for prevention of future incidents where possible.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Data Backup Policy

IX. Related Documents:

Data Backup Plan
Disaster Recovery Plan
Emergency Mode Operation Plan

Policy Title: Data Backup Policy	
Policy Number: SC09	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy ensures that an appropriate plan is established for creating retrievable exact copies of the electronic protected health information maintained in the hospital's information systems.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.310(d)(1) of the HIPAA Security rule relating to data backup and storage.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center safeguards the loss of electronic protected health information maintained on its information systems by a Data contingency and backup plan established for creating retrievable exact copies (backup).

III. Scope and Applicability:

This policy is applicable to all electronic protected health information maintained in the hospital's information systems.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Creating backup of electronic protected health information:
The ACMC IT Staff will be responsible for maintaining an exact copy of the electronic protected health information maintained in the hospital's information systems including servers and any workstations whether on the hospital's network or not, as per the Data Contingency and Backup Plan.

B. Data Backup log:
The ACMC IT Staff will maintain a log of the backed up data and the backup media such as magnetic tapes or compact discs in the Data Backup log. The data backup log will record details such as the date and time and the person's signatures that took the back up.

C. Data storage:
1. See the policy on "Data Contingency/Backup Plan for information on Data Backup Storage.

2. A log will be maintained of movement of the backed up data into and out of storage. The log will record details such as the date and time and the person's name and signatures that delivered or retrieved the data from storage.

D. Data retrieval:
1. The Security Officer and ACMC IT Staff will be authorized to access and retrieve data from storage. If another person is asked to retrieve the data from the storage then this person will have to be authorized for access and retrieval by the Security Officer.

2. The details of the data and the person retrieving it from storage will be recorded in the log maintained as mentioned above in paragraph VI.C 2.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Contingency Plan Policy

IX. Related Documents:

Data Backup Log
Data Backup Plan

Policy Title: Facility access controls	
Policy Number: SC10	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the safeguards adopted by the hospital to protect the systems that maintain electronic protected health information maintained and buildings and equipment from natural and environmental hazards and unauthorized access.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.310(a)(1) of the HIPAA Security rule relating to facility access controls.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center will protect the electronic protected health information by implementing adequate controls for access to buildings, software and hardware equipment. The hospital will maintain a contingency plan to protect the loss of electronic protected health information from natural and environmental hazards and unauthorized access.

The hospital will also keep records of maintenance activities carried out in the areas where the protected health information is maintained and used.

III. Scope and Applicability:

This policy is applicable to access control mechanisms for physical access to various hospital facilities.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Facility security plan:
The Security Officer will prepare a comprehensive security plan for the hospital including and not limited to the areas where electronic protected health information is maintained.

B. Access controls and validation:
Access to the hospital's systems that keep electronic protected health information and the areas where protected health information is maintained will be only granted after validation and authorization for access as per the Workforce Security Access Authorization policy.

The keypad codes will be changed every 90 days and the new codes will be given to department managers. It is up to the department managers to choose who in their department needs access to the codes.

No ACMC employee, volunteer, or contracted individual, on or off duty, are permitted in any workstation except to perform work-related duties (e.g., an off duty nurse may not visit inside any nurses' station).Violators will be subject to the disciplinary process.

ACMC employees, volunteers, or contracted individuals, on or off duty, who do not require access to secured (keypad accessible) units in order to perform work-related duties, are not permitted to access those units. If access is necessary for non-work related purposes, ACMC employees, volunteers, or contracted individuals must receive permission from a nurse or other person authorized to give permission before entering the unit. Under no circumstances are ACMC employees, volunteers, or contracted individuals, on or off duty, allowed to permit unauthorized individuals to enter secured units without permission. (e.g., Employees may not use the keypad to enter any secure unit or allow any other person to enter a secure unit to visit family, friends, etc. who are patients without permission from the patient's nurse or physician.) Violators will be subject to the disciplinary process.

Workforce members will sign a letter of confidentiality stating that all protected health information will be kept confidential. All visitors in that area will have to sign a log-in sheet upon entering the area. These areas are listed below. Log-in

names and passwords assigned by Manager Information Systems will be used for access to electronic protected health information.

- Health Information Record Room
- ~~Doctor's Dictation Room~~
- ~~Ashley Specialty Clinic Record Room~~
- ~~Ashley Health and Women's Services Record Rooms~~
- ~~Ashley IOP Record Room~~
- ~~Surgical Associates Record Room~~

C. Supervision and authorization of visitors and maintenance/operational personnel:

1. Wherever reasonable and appropriate, the hospital will ensure that the visitors are escorted and personnel are supervised while doing their work, to minimize or eliminate the possibility of unauthorized access to areas mentioned above.
2. Unauthorized individuals will be prohibited from accessing provider only areas at all times unless escorted by hospital personnel.

D. Contingency plan for emergencies:

The hospital's electronic protected health information will be protected from loss due to an emergency resulting from a natural or other hazard by the contingency plan outlined in the Contingency Plan policy. In the event of an emergency the disaster recovery plan and the emergency mode operation guidelines will be followed to safeguard and recover the electronic protected health information.

E. Facility maintenance records:

The hospital's Engineering Manager will obtain the approval of the Security Officer for repair and modification activities of the physical components such as walls, doors, locks hardware etc., of the areas where protected health information is maintained. The Security Officer will designate appropriate personnel to supervise such activities, when required.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Workforce Security/Access Authorization Policy
Contingency plan policy

IX. Related Documents:

None

Policy Title: Device and Media Controls	
Policy Number: SC 11	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy is to describe the procedures to be followed to maintain proper records of all devices and storage media, their re-use and disposal.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Section 164.310(d)(1) of the HIPAA Security rule relating to device and media controls.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of the hospital to maintain proper record and track of all electronic devices and storage media used to store and process protected health information. The workforce members must use prescribed procedures for re-using, disposing and backing up the electronic storage media.

III. Scope and Applicability:

This policy applies to the all electronic devices and media that are used to store or process protected health information.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Maintaining Records / Accountability: Proper records of all the electronic devices and storage media used to store or process protected health information must be maintained by the Security Officer.

No device or media shall be removed from the hospital facilities without the written approval of the Security Officer. All such requests should be first approved by the Department Head and then forwarded to the Security Officer for final approval. These approvals are not required for taking back-up tapes to the off-site storage location. All portable media that contains PHI must be encrypted.

Whenever an electronic device or media, defined above, is taken off-site an entry should be made in the 'Hardware/Media Tracking Log'. ~~The Security Officer should review the logs regularly as part of the monthly 'Information System Activity Review'.~~

B. Re-use of media: It is recommended that the electronic storage media used for storing protected health information not be re-used for any other purposes. If a storage media needs to be re-used then the following must be ensured:
    1. Data back up: It must be checked if the data on the storage media needs to be backed up. If yes, then the data must be backed-up before using the media.
    2. Erasing the data: The media being used should be formatted to erase all information stored in it.

C. Disposal: The Security Officer must approve disposing-off of any media~~.~~ Before disposing of any storage media step 1 and 2 in #B above must be followed. Disposal of storage media should be properly documented. Disposal must be performed by ACMC IT Staff. Hard Drives, CD's, DVD's, or Blue Ray Discs will be physically destroyed after being erased and discarded in different trash bins.

D. Data backup and storage: Data must be regularly backed up on designated storage media as per the 'Data Backup' policy. Proper records should be maintained of all data back up media that is taken to off-site storage locations.

E. At any time workforce members, if requested, must turn over portable devices that may contain EHR.

F. USB thumb drives are not authorized to be used at ACMC without the written permission from the Security Officer. If approved, the USB thumb drive must be formatted before and after use. The approved workforce employee is responsible

for getting the thumb drive to the Security Officer for formatting. Under no circumstance should a thumb drive be taken away from ACMC with hospital data on it.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Data Backup Policy

IX. Related Documents:

Hardware/Media Tracking Log

Policy Title: Workstation use and security	
Policy Number: SC12	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the method for using the hospital's workstations that maintain electronic protected health information and securing them from unauthorized access and use.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.310(b) and (c) of the HIPAA Security rule relating to workstation use and security.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center implements appropriate safeguards to maintain the integrity and confidentiality of electronic protected health information stored on the hospital's workstations by ensuring proper use and by securing them from unauthorized use and access.

III. Scope and Applicability:

This policy is applicable to all workforce members who are assigned use of workstations to work with electronic protected health information

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

Workstations include all computers including desktops, laptops, and any workstations or mobile devices that are connected or not connected to the hospital's network.

A. Workstation security:

The hospital will secure all rooms that house workstations that maintain any electronic protected health information from unauthorized access while unattended.

1. Workstations, especially those kept in public areas such as receptions, will be placed in a manner that any unauthorized persons cannot view the screen's contents.

2. The Security Officer will limit the use and access of workstations to those workforce members who are assigned the use of the workstation by means of log-in names and passwords issued to the users.

3. The ACMC IT Staff will keep a record of the laptops assigned to workforce members of the hospital, laptops taken offsite and the workforce members who take them offsite.

B. Workstation use:

1. The Security Officer will instruct workforce members in the proper use and access of workstations as part of 'General Security Awareness Training'.

2. Workforce members will not store any protected health information on their individual workstations where it cannot be protected from unauthorized access by a password. If information is stored on the workstation in applications such as MS Excel, then the file should be password protected. If the information is stored in other applications that cannot be password protected such as a MS Word document, then these should be place inside a folder that should be password protected.

3. While away from the workstation, workforce members ~~will either lock their workstations or enable a password protected screen saver~~ should lock their computers.

~~4.~~ The hospital network will be configured so that a user who has been inactive for 15 minutes will automatically ~~trigger a screensaver on the computer that is password protected~~ be locked.

5. Workforce members will be required to keep the locations of the workstations they use secured by ensuring the doors leading to access are kept closed and locked while unattended.

6. Workforce members will access only those workstations that have been assigned to them for their work. Passwords to the workstations, network and screen savers should be kept secret and workforce members should not be revealed.

   The Security Officer and the Department Heads will perform periodic inspections to ensure that user names and passwords are not written on paper (sticky notes) that are in public view.

7. Virus protection must be enabled on each workstation and all files that are downloaded to or uploaded from a workstation are scanned for any viruses or worms. The ACMC IT Staff must ensure that each workstation has the most updated version of the Virus protection software.

8. Any protected health information stored on a workstation should be backed up on a regular basis in accordance with the hospital's policy on data backups.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Workforce Security/Access Authorization Policy
Data Backup Policy

IX. Related Documents:

None

Policy Title: System access control and emergency access	
Policy Number: SC 13	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes access control by the use of unique identifiers and the method for access in case of an emergency to the hospital's information systems that maintain electronic health information.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.312(a)(1) of the HIPAA Security rule relating to access control.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center uses log-in names as unique identifiers issued to workforce members to access the hospital's information systems that maintain electronic protected health information. The hospital has made provision for access to the hospital's information systems that maintain electronic health information in case of an emergency as detailed in the procedures of this policy.

III. Scope and Applicability:

This policy is applicable to all the hospital's information systems that maintain electronic protected health information.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. System access control:
The hospital will provide access to the hospital's information systems that maintain electronic health information by assigning unique identifiers of individual log-in names for those workforce members who are authorized as per the policy of Workforce security and access authorization.

1. Software application access: Access to the application will be provided by log-in names and passwords assigned by the ACMC IT Staff.

2. Network access: Access to the hospital's network will be provided by log-in names and passwords assigned by the ACMC IT Staff.

3. Server Access: Access to the hospital's servers and any folders containing electronic protected health information will be provided by log-in names and passwords assigned by the ACMC IT Staff to those individuals who are authorized to access the servers and the folders maintained on them.

B. Establishing log-in names and password metrics:
1. The Security Officer will decide on the metrics to be used for log-in names and passwords**.**

2. Here are the metrics for passwords within the hospital:

a. For CPSI:
- **i.** Passwords must be at least 8 characters long
- **ii.** Passwords must contain at least 1 uppercase letter, 1 lowercase letter, and one number.
- ~~**iii.** Passwords cannot be a word based in the dictionary~~
- ~~**iv.** Passwords cannot be part of your name~~
- ~~**v.** Passwords cannot be in numerical or alphabetical order~~
- **vi.** Passwords expire every 90 days

b. For the hospital network:
- **i.** Passwords have to be at least 6 characters long
- **ii.** Passwords cannot contain any part of your user name
- **iii.** Passwords must contain characters from 3 of these 4 groups
  1. English Uppercase letters
  2. English Lowercase letters
  3. Base 10 digits
  4. Non-alphabetic characters.
- **iv.** Passwords expire every 90 days
- **v.** Cannot use the last 5 passwords.

c. For T-System:
- **i.** Passwords must be at least 4 characters long
- **ii.** Passwords must contain characters from 3 of these 4 groups
  - **1.** English Uppercase letters
  - **2.** English Lowercase letters
  - **3.** Non-alphabetic characters
  - **4.** Base 10 digits
- **iii.** Passwords expire every 90 days
- **iv.** Cannot use the last 5 passwords

C. Emergency access:

1. In an emergency condition, for example a situation when normal systems including electrical power have been severely damaged or rendered inoperative due to a normal or man made disaster, access to electronic protected health information will be provided as per the Emergency Mode Operation Guidelines and Disaster Recovery Plan Guidelines.

2. When operating in an emergency mode, the ACMC IT Staff will ensure that access is provided to workforce members who are required to work with electronic protected health information with appropriate authorization by assigning log-in names and passwords to any new or alternative systems to safeguard against unauthorized access.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Workforce Security/ Access Authorization Policy
Workstation Use & Security

IX. Related Documents:

Disaster Recovery Plan
Emergency Mode Operation Plan

Policy Title: Technical security audit controls	
Policy Number: SC14	**Effective Date: 4/1/05**
Review Date: 1/1/2013	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the audit controls to be implemented that will help conduct security audits for examining activities of the hospital's information systems that maintain electronic protected health information.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.312(b) of the HIPAA Security rule relating to technical security audit controls.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center has implemented appropriate controls to monitor and examine access and use of information systems that maintain electronic protected health information and will conduct periodic security audits to ensure integrity, confidentiality and availability of information and investigate any security incidents.

III. Scope and Applicability:

This policy is applicable to the hospital's information systems that maintain electronic protected health information and users of these information systems.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Audit controls: The hospital conducts periodic audits of the information systems as per the policy on Security audits – review and evaluation. In order to perform these audits the Security Officer of the hospital will establish appropriate technical security controls that will enable the hospital to examine and monitor the activities of the users.

B. Establishing technical security audit controls:

1. The ACMC IT Staff will analyze the hospital's information systems to assess the operating systems and applications where technical security audit controls must be implemented to ensure activity in the hospitals information systems can be examined and monitored when required.

2. Access to electronic protected health information using the operating system and various software applications will be provided by individual log-in names issued by the ACMC IT Staff as per the hospital's "Access authorization" policy.

3. The following audit controls will be implemented to log the activity on the hospital network:
   Active Directory – logs when users enter the network
   CPSI – logs were users go in CPSI

4. The following audit controls will be implemented to log the activity in various software applications that store or process protected health information:
   CPSI – internally audited through reports via CPSI
   QUANTIM – internally audited

C. Accounting of unauthorized access, use or disclosure:
If any unauthorized access is detected resulting in unauthorized use or disclosure of electronic protected health information, the hospital is required to account for the disclosure as per the policy on 'Accounting of disclosures'.

D. New software purchase:
When any new software needs to be purchased for working with electronic protected health information, the ACMC IT Staff will examine and ensure that the software is capable of providing user based and role based access to establish appropriate audit controls. It must also be checked that the new software generates appropriate audit reports to show user activity.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Security audits – review and evaluation
Access authorization policy

IX. Related Documents:

None

Policy Title: E-mail and Facsimile Policy	
Policy Number: SC15	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the appropriate safeguards for secure and effective use of the hospital's electronic mail system and facsimile for transmitting protected health information.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the HIPAA Security rule.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

Ashley County Medical Center does allow the use of electronic mail to transmit or receive any electronic protected health information both internally and externally but must safeguard the information from unauthorized access. Use of facsimile is permitted to transmit protected health information with strict adherence to safeguards detailed in the procedure of this policy.

III. Scope and Applicability:

This policy is applicable to all workforce members who use facsimile machines or electronic mail for their work and where the mail either originated from or was received into the hospital's information systems.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this

policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Use of electronic mail:
Electronic mail is an integrated tool of the hospital's processes and is intended to facilitate communications and exchange of information to carry out one's tasks.

Users should use electronic mail appropriately and must be aware that electronic communications can be intercepted, forwarded and printed by others. Therefore, users must exercise discretion and confidentiality safeguards equal to, or exceeding that which are applied to written documents. E-mail accounts and passwords should not be shared or revealed to anyone besides the authorized user(s).

B. Use of disclaimer and confidentiality statement in e-mail:
The hospital requires that all workforce members using e-mail for their work include a standard statement of confidentiality and disclaimer in the e-mail. This will be setup by the ACMC IT Staff at the time the email account is setup.

C. Prohibited use of e-mail:
Ashley County Medical Center does allow workforce members to use e-mail to transmit and receive any electronic protected health information both internally and externally. If a workforce member uses email to transmit or receive any electronic protected health information the document has to be password protected. If the hospital is requested for any protected health information to be sent or received via e-mail, the requesting person or entity should be asked to choose an alternate transmission if at all possible.

D. Use of facsimile machines:
Facsimile machines are an important communication tool of the hospital and generally the primary choice for transmitting printed data. Workforce members are required to adhere to the following preventive security measures to safeguard protected health information from unauthorized use and disclosure.
1. Cover sheets: All fax transmissions should contain a cover sheet as the first page. This cover sheet should clearly state the name of the entity the fax is sent to and must state that the matter faxed is confidential.
2. Disclaimer: The cover sheet should contain the disclaimer statement, which should state that if the recipient of the fax is not the entity it was sent to then it should be immediately destroyed.
3. Number confirmation: When faxing to a new entity the person sending the fax must call first and confirm the fax number. The number should be verified before beginning transmission, especially when the number is being dialed from the memory function of the fax machine.

4. Safeguarding transmitted data: Once the matter has been faxed the papers should be immediately removed from the fax machine and secured in their appropriate filing space.

E. Use of Social Media

1. Workforce members are prohibited from referencing patient or similar data on social media sites, blogging or any other similar sites or processes, even if it does not include patient names. The hospital network blocks all social media sites. Disciplinary action may be taken against employees who violate this policy up to and including termination.
2. Employees are prohibited from taking pictures of patients, specimens, or patient families with their personal cell phones. If a patient requests an employee to take a picture of himself/herself with the patient's own camera this is permitted. (no other patients should be in the picture)
3. Workforce members are prohibited from texting PHI or taking pictures of patients with their personal cell phones.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

None

IX. Related Documents:

None

Policy Title: Data Integrity Policy	
Policy Number: SC16	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the method for maintaining the integrity of electronic protected health information data.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.312(c)(1) of the HIPAA Security rule relating to integrity of electronic protected health information.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of Ashley County Medical Center to implement appropriate mechanisms and safeguards to maintain the integrity of electronic protected health information and protect it from unauthorized modification and deletion.

III. Scope and Applicability:

This policy is applicable to all workforce members who work with or come into contact with electronic protected health information.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Providing role based and user based access: Workforce members who work with electronic protected health information should be provided access to the hospital's information systems that maintain electronic protected health information based on their roles. The systems administrator will assign privileges to the applications based on the roles of the users to ensure that the workforce members have limited access to only those features of the application that are required for them to do their job.

B. Disallowing modification and deletion of data: The hospital will implement required rules in the applications to ensure that the workforce members working with electronic protected health information are not able to modify or delete any data by implementing required rules in the applications.

C. Activity Audit: The applications used for storing and processing protected health information should have the capability of recording who logged into the application at what time, who entered new data and who updated it. At a minimum a record of the last update done should be maintained.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

System Access Control and Emergency Access
Technical Security Audit Controls

IX. Related Documents:

None

Policy Title: Entity authentication Policy	
Policy Number: SC 17	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: This policy describes the mechanism for authenticating an entity in order to corroborate that an entity is who it claims to be.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.312(d) of the HIPAA Security rule relating to entity authentication.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of Ashley County Medical Center to implement proper security controls to authenticate an entity accessing information systems externally or internally as well as areas where protected health information is maintained.

III. Scope and Applicability:

This policy is applicable to all entities accessing the hospital's protected health information.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Implementing controls for entity authentication:
The Security Officer of the hospital will be responsible for implementing appropriate controls for ensuring any entity accessing the hospital's information systems internally or externally as well as physical areas where protected health information is maintained can be authenticated.

B. Authentication of internal workforce members:
1. The hospital will authenticate an internal workforce member accessing the hospital's information systems where protected health information is maintained by the unique log-in names issued to individuals.

~~2. The hospital will authenticate an internal workforce member accessing the hospital's physical areas where protected health information is maintained by the workforce member's fingerprint via the IGuard Biometric Fingerprint Scanners where available and by having the internal workforce member sign a confidentiality agreement stating that all records will remain confidential to gain access to areas without the Biometric Fingerprint scanners. No visitors will be allowed in areas with confidential patient information unless they are escorted by a hospital employee that has access to the area and then the visitor must sign a log in the area.~~

C. Authentication of entity accessing from outside:
The hospital will allow external access only over secured connections. The ACMC IT Staff will issue a log-in identity and password for the purpose of authentication to an entity that requires access to the hospital's information systems from outside.

D. Monitoring access:
The ACMC IT Staff will monitor the access both internally and externally to the hospital's information systems where protected health information is maintained to safeguard against unauthorized access.

E. Password expiration:
To safeguard the protected health information the ACMC IT Staff will configure the hospital's information systems where protected health information systems are maintained so that users are required to change their passwords every 90 days. The passwords that have to be changed every 90 days are the Windows Network password and the unique User ID password in CPSI.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it

is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

Workforce Security/Access Authorization
System Access Controls and Emergency Access

IX. Related Documents:

None

Policy Title: Communication Network Controls & Security	
Policy Number: SC 18	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Policy Summary:

A. Purpose: The purpose of this policy is to define the procedures to ensure the security of hospital's internal network and the security of data transmission.

B. Regulatory Reference: Ashley County Medical Center has adopted this policy to ensure compliance with the requirements of Sections 164.312(e)(1) and 164.312(e)(2)(i) of the HIPAA Security rule relating to communication network controls.

C. Violations of this policy may result in corrective action up to and including termination of employment.

D. Ashley County Medical Center intends to honor this policy and the procedures set forth below, but reserves the right to change them at any time, with or without notice, at its sole discretion.

II. Policy:

It is the policy of the hospital to secure the hospital network against unauthorized intrusion by external entities and to ensure secure electronic transmission of protected health information to the authorized entities.

III. Scope and Applicability:

This policy is applicable to hospital's internal and external network. External network refers to connecting to various trading partners for data transmission.

IV. Definitions:

V. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this policy. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this policy. The Privacy, Security, and Compliance Officers will provide assistance to employees and management as needed.

VI. Procedure:

A. Internal Network Security: The hospital uses the Cisco ASA 5510 Firewall to protect its internal network from being accessed by unauthorized external entities.

B. Automatic Log Off: An internal user who has been inactive for more than 15 minutes ~~within the CPSI system will be automatically logged off the hospital network~~ will have their account locked. ~~Automatic logging off will be controlled through the server. Screen savers should be set to come on after a certain period of inactive time as well. These screen savers should be password protected.~~

C. Communication Network Security: The hospital transmits electronic claims (protected health information) to various trading partners. The security of data transmission is ensured by use of dedicated point-to-point connection with each trading partner (dedicated modem and telephone line). A secure connection to the internet is also used to transmit electronic claims.

D. Virus Protection: The hospital network must always be protected against viruses, worms, and other malicious software. Virus protection software must be run as a service on all servers and other computers. The software must be updated on a regular basis. The ACMC IT Staff must perform regular audits to ensure that the hospital network, servers other computers are free from viruses.

ACMC uses AVG Internet Security Business Edition 2012 as their Anti-Virus system. Daily updates are given through the controller and sent out to network devices daily.

E. Internet Access: The internet should only be used for work related issues. The hospital uses an Internet filtering program called iPrism to track all internet users. This program has the ability to deny access to certain sites or let you gain access to certain sites.

F. Remote Access: Certain entities, such as, the vendor of the hospital management system, log on to the hospital server for the purpose of routine maintenance and support. Such entities must log on using a dedicated point-to-point connection (VPN).

~~The Security Officer must approve in writing to allow an external entity to log on to the hospital server(s).~~

- ~~CPSI uses a secure VPN connection to their servers.~~
- ~~Quantim uses a secure VPN connection to their servers.~~
- ~~Ramsoft uses a secure VPN connection to their servers.~~

~~G.~~ Dial-up login (Telecommuting): ACMC does allow telecommuting. The Department Manager must fill out a "Workforce Access Authorization" form to validate the workforce member's access. The Security Officer will then give out a unique username and password for VPN connection. ~~As a rule the hospital does not allow workforce members to telecommute. That is, the workforce members are not allowed to log on to the hospital network from outside. However, if a workforce member needs to access the network from outside, he/she must obtain written approval from the Security Officer.~~

~~i. IT Manager, Network Tech, Clinical Informatics, HR, CEO, PR, Education, Infection Control, Quality Improvement, Accounting, and CNO have laptops that are capable of telecommuting. All home health nurses have Fujitsu tablets to use in patients home.~~

H. Use of Desktop Sharing applications: The hospital, in general, does not allow the use of any 'Desktop Sharing' software applications. If a workforce member needs to use one for a specific purpose, he/she must obtain written approval from the Security Officer. The IT department uses Log Me In to work remotely on hospital computers.

VII. Review:

The Security Officer shall review this policy annually to determine if the policy complies with current HIPAA Security regulations and any other applicable current State or Federal Security regulations that may be stricter than HIPAA. If it is determined that there are significant regulatory changes, the policy will be reviewed and updated as needed.

VIII. Related Policies:

None

IX. Related Documents:

None

Disaster recovery plan guidelines	
Policy Number: SC19	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Plan Summary:

A. Introduction: This document is the disaster recovery plan for Ashley County Medical Center. The information present in this plan guides Ashley County Medical Center management and technical staff in the recovery of computing and network facilities in the event that a disaster destroys all or part of the hospital's facilities where the information systems are maintained.

B. Regulatory Reference: Ashley County Medical Center has adopted this plan to ensure compliance with the requirements of Sections 164.308(a)(7) of the HIPAA Security rule relating to contingency plan.

C. Ashley County Medical Center reserves the right to modify the details and procedures of this plan at any time, with or without notice, at its sole discretion.

II. Definitions:

III. Responsibility:

Members of Ashley County Medical Center's workforce are covered by and responsible for compliance with this plan. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this plan. The Manager Information Systems, Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

IV. Information Systems Disaster Recovery Plan details:

This document is the disaster recovery plan for Ashley County Medical Center that has been devised for efficiently responding to an event that a disaster destroys all or part of the hospital's information systems where electronic protected health information is maintained.

A. Description:
1. The Disaster Recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at Ashley County Medical Center. Each supported computing platform

has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

2. This plan is available with the Security Policy & Procedure Manual to make it readily available. This plan will be updated on a regular basis as changes to the computing and networking systems are made.

B. Primary FOCUS of the Plan:

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the hospital's information systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

IMPORTANT NOTE!

All disaster recovery plans assume a certain amount of risk, the primary one being how much data is lost in the event of a disaster. Disaster recovery planning is much like the insurance business in many ways. There are compromises between the amount of time, effort, and money spent in the planning and preparation of a disaster and the amount of data loss you can sustain and still remain operational following a disaster. Time enters the equation, too. Many organizations simply cannot function without the computers they need to stay in business. So their recovery efforts may focus on quick recovery, or even zero down time, by duplicating and maintaining their computer systems in separate facilities.

The techniques for backup and recovery used in this plan do *NOT* guarantee zero data loss. The hospital administration is willing to assume the risk of data loss and do without computing for a period of time in a disaster situation. In such a situation alternate hard copies of data such as Medical Records and Admitting forms will be used for continuing operations.

Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup tapes. *Significant* effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point

C. Primary OBJECTIVES of the Plan:

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical information systems capability to the Ashley County Medical Center.
2. Set criteria for making the decision to recover at the JSE Building or repair the affected site.
3. Describe the method for carrying out the plan.

4. Provide information concerning personnel that will be required to carry out the plan.
5. Identify the equipment, procedures, and other items necessary for the recovery.

D. OVERVIEW of the Plan:

This plan uses a "cookbook" approach to recovery from a disaster that destroys or severely cripples information systems at Ashley County Medical Center.

1. Personnel :
   Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

2. Salvage Operations at Disaster Site:
   Early efforts are targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, diskettes) are identified and either protected from the elements or removed to the JSE Building.

3. Designate Recovery Site:
   At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the JSE Building, a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

4. Purchase New Equipment :
   CPSI can provide replacement equipment in the event that some resources cannot be salvaged.

5. Begin Reassembly at Recovery Site :
   Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been kept up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly

phase is complete, the work turns to concentrate on the data recovery procedures.

6. Restore Data from Backups:
   Data recovery relies entirely upon the use of backups stored in locations off-site from the Ashley County Medical Center premises. Backups can take the form of magnetic tape, CDROMs, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup tapes is done. Individual application owners may need to be involved at this point, so teams are assigned for each major application area to ensure that data is restored properly.

7. Restore Applications Data:
   Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, the hospital must have means for restoring each running application database to the point of the disaster. All new data collected since that point should be taken and put into the application databases. When this process is complete, the hospital computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

8. Move Back to Restored Permanent Facility:
   If the recovery process has taken place at the JSE Building, physical restoration of the Ashley County Medical Center premises (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the JSE Building are to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the JSE Building.

E. Disaster Risks and Prevention:
   As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, and steps we should take to minimize risk. The threats covered here are both natural and human-created.

1. FIRE:
   The threat of fire in the hospital can be very real and poses a high risk factor. The hospital is filled with electrical devices and connections that could overheat or short out and cause a fire. Uninterruptible Power Supply batteries can spark and could ignite a fire and explosion.

   The computers within the facility also pose a quick target for arson from anyone wishing to disrupt hospital operations. Wide area fires, such as those common in recent years in California, are also a possibility in dry times.

   Recommendations

   Regular review of the procedures should be conducted to insure that they are up to date. Unannounced drills should be conducted by an impartial administrator and a written evaluation should be produced for the department heads housed in the building.

   Regular inspections of the fire prevention equipment are also mandated. Fire extinguishers should be periodically inspected as a standard policy. Smoke detectors should be periodically inspected and cleaned.

2. FLOOD:
   Rain storms can be threat of flooding causing flood waters to penetrate critical areas and can cause a lot of damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections.

   Recommendations

   Periodic inspections must be conducted to detect water seepage, especially any time there is a heavy downpour. Water drains should also be inspected to make sure that they aren't clogged by debris.

3. TORNADOS AND HIGH WINDS:
   Damage due to high winds or an actual tornado is a very real possibility. A tornado has the potential for causing the most destructive disaster we face.

   Recommendations

   All workforce members of the hospital should know where the strong points of the buildings are and directed to seek shelter in threatening weather.

   Large tarpaulins or plastic sheeting should be available to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage.

4. EARTHQUAKE:
   The threat of an earthquake should not be ignored. Buildings in the area are not built to earthquake resistant standards like they are in quake-prone areas like California. So the hospital could expect light to moderate damage from the predicted quake.

   An earthquake has the potential for being the most disruptive for this disaster recovery plan. If the hospital is damaged, it is highly probable that the JSE Building on campus may also be similarly affected. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do wide-scale building repairs.

   Recommendations
   Large tarpaulins or plastic sheeting should be available to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage.

5. COMPUTER CRIME:
   Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before.

   Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. A well-intentioned employee can make coding errors that affect data integrity (not considered a crime, of course, unless the employee deliberately sabotaged programs and data).

   Recommendations

   Continue to improve security functions on all platforms. Strictly enforce policies and procedures when violations are detected. Regularly let users know the importance of keeping their passwords secret. Let users know how to choose strong passwords that are very difficult to guess.

   Improve network security. Shared wire media, such as Ethernet are susceptible to sniffing activities, which unscrupulous users may use to capture passwords. Implement stronger security mechanisms over the network, such as one-time passwords, and non-shared wire media.

6. TERRORISTIC ACTION AND SABOTAGE:
   The hospital's information systems can be destroyed or sabotaged by terrorist actions.

   Recommendations

   Maintain good building physical security. Doors into areas where information systems that maintain electronic protected health information is maintained should be locked at all times and only authorized personnel provided access. All visitors to these areas should receive prior authorization and log in and out.

F. Disaster Preparation:
   In order to facilitate recovery from a disaster certain preparations should be made in advance. This document describes what should be done to lay the way for a quick and orderly restoration of the hospital's information systems**.**

   The following topics are presented in this document:

   - Disaster Recovery Planning
   - Recovery Facility
   - Replacement Equipment
   - Backups
   - Disaster Lock Boxes

1. Disaster Recovery Planning:
   The first and most obvious thing to do is to have a plan. The hospital should have an overall plan of which this document is a part that Information Systems Department will use in response to a disaster. The extent to which this plan can be effective, however, depends on the overall disaster recovery plan of the hospital.

2. Recovery Facility:

   If an information systems facility is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at CPSI in Mobile, AL.

   There are a number of options for alternate sites, each having a varying degree of up-front costs.

   a) Hot Site
      This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for generally very large organizations. A separate site, possibly even located in a different location, can be built,

complete with servers and other facilities ready to cut in on a moment's notice in the event the primary site goes offline. The two sites must be joined by high speed communications lines so that users at the primary site can continue to have access.

b) Disaster Recovery Company
CPSI has a contract to take care of disaster recovery.

c) Disaster Partnerships
Some organizations will team up with others in a partnership with reciprocal agreements to aid each other in the event of a disaster. These agreements can cover simple manpower sharing all the way up to full use of a computer facility. Often, however, since the assisting partner has to continue its day-to-day operations on its systems, the agreements are limited to providing access for a few key critical applications that the disabled partner must run to stay afloat while its facilities are restored.

The primary drawback to these kinds of partnerships is that it takes continual vigilance on behalf of both parties to communicate the inevitable changes that occur in computer and network systems so that the critical applications can make the necessary upfront changes to remain operational. Learning that you can't run a payroll, for instance, at your partner's site because they no longer use the same computer hardware or operating system that you need is a bitter pill that no one should swallow.

One of the most critical issues involved in the recovery process is the availability of qualified staff to oversee and carry out the tasks involved. This is often where disaster partnerships can have their greatest benefit. Through cooperative agreement, if one partner loses key personnel in the disaster, the other partner can provide skilled workers to carry out recovery and restoration tasks until the disabled partner can hire replacements for its staff. Of course, to be completely fair to all parties involved, the disabled partner should fully compensate the assisting partners for use of their workers unless there has been prior agreement not to do so.

The use of reciprocal disaster agreements of this nature may work well as a low-cost alternative to hiring a disaster recovery company or building a hot site. And they can be used in conjunction with other arrangements, such as the use of a cold recovery site described below. The primary drawback to these agreements is that they usually have no provision for providing computer and network access for anything other than predefined critical applications. So users will be without facilities for a period of time until systems can be returned to operation.

d) Cold Site

A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired. There are varying degrees of "coldness", ranging from an unfinished basement all the way to space where the necessary raised flooring, electrical hookups, and cooling capacity have already been installed, just waiting for the computers to arrive.

Our cold site is the JSE Building. We would have to wait for servers to come from CPSI, but once we received them we could hook them up over there and continue. Depending on the disaster we might not be able to get back up and running for some time. If our routers are destroyed we wouldn't be able to function properly.

3. Replacement Equipment:
This plan should contain a complete inventory of the components of each of the computer and network systems and their software that must be restored after a disaster. The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. Where possible, agreements have been made with vendors to supply replacements on an emergency basis. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long.

The ACMC IT Staff will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

4. Backups:
The data that was stored on the old equipment cannot be bought at any price. It must be restored from a copy that was not affected by the disaster. There are a number of options available to us to help ensure that such a copy of your data survives a disaster at the primary facility. This is the option we use:

a) Off-Site Tape Backup Storage
This option calls for the transportation of backup tapes made at the primary facility to an off-site location. Choice of the location is important. You want to ensure survivability of the backups in a disaster, but you also need quick availability of the backups.

This option has some drawbacks. First, there is a period of exposure from the time that a backup is made to the time it can be physically removed off-site. A disaster striking at the wrong time may result in the loss of all data changes that have occurred from the time of the last off-site backup. There is also the

time, expense, and energy of having to transport the tapes. And there is also the risk that tapes can be physical damaged or lost while transporting them.

Some organizations contract with disaster recovery companies to store their backup tapes in hardened storage facilities. While this certainly provides for more secure data storage, considerable expense is undertaken for regular transportation of the data to the storage facility. Quick access to the data can also be an issue if the storage facility is a long distance away from your recovery facility.

The storage location is:

Monthly tapes are sent to CPSI in Mobile, AL

Monthly tapes are then stored in Fireproof Safe at ~~Alabama Office~~ the Hamburg Clinic

Weekly tapes are stored in Fireproof Safe at ~~JSE Building~~ the Hamburg Clinic.

Daily tapes are stored in Fireproof Safe in Server Room

Disaster Lock Boxes:

To ensure that an up-to-date copy of this plan is available when a disaster occurs, procedures have been established to store a copy of the plan with other important recovery information in the safe at the ~~Alabama Street~~ Hamburg Clinic Location. Paper copies of patient forms and other important documents that will be required for providing healthcare to patients will also be kept in the respective departments.

The safe is to remain locked at all times. Keys to the safe are kept by several key people within the hospital, including

- Security Officer
- ACMC IT Staff

In a disaster situation when entry into the safe is needed but the key is not available you can physically break the lock.

G. Backup Procedures:

All CPSI servers are backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes. The off-site storage location used is:

- CPSI in Mobile, AL (monthly)
- Safe at ~~Alabama Street Office~~ the Hamburg Clinic(monthly)
- Safe at ~~JSE Building~~ the Hamburg Clinic(weekly)

- Safe in Server Room (daily)

When a new backup is made, the tapes are sent to the back up site. The procedures for making the backups for each individual computer system differs. In general, media-level or full file system level backups are taken in a given cycle (typically weekly). In some instances, there are additional application-level backups for a system that may be run on a daily basis. Some systems support incremental backups, and these are typically run on a daily basis.

1. CPSI:
   Full Volume backups are taken each day. The tapes are taken off-site each afternoon to the safe in the server room. Also CPSI is backed up hourly to our warm server in the server room. There is also a set of tapes sent to CPSI in Mobile, AL at the end of each month. Full Volume Tape Backups are labeled according to what they are backing up. They have the name of the server written on them.

H. Disaster Notification List:
The disaster notification list for Information Systems Department is shown below. These people are to be notified as soon as possible when disaster threatens or occurs.

CEO –	Phil Gilmore	870-364-4111
Security Officer –	Dan Austin	364-9262 or 500-0078
Privacy Officer –	Kayla Hill	(318) 823-4242
Safety Officer –	Jimmy Stell	(870) 500-1091
CNO -	Emily Bendenelli	(870) 364-4111

I. Disaster Recovery Teams:
To function in an efficient manner and to allow independent tasks to proceed simultaneously, a Recovery Management Team will handle the recovery process. The Recovery Management Team oversees the whole recovery process. The Recovery Manager leads the Recovery Management Team. The Manager has the final authority on decisions that must be made during the recovery. The Recovery Manager is responsible for appointing the other members of the Recovery Management Team.

1. Selecting Personnel for the Recovery Management Team

   The selection of the members of the Recovery Management Team is very important. Since it is almost impossible to document exactly what each of the individual will be required to do (each disaster will have its own special set of circumstances, many of which will be completely unanticipated), each member of the Recovery Management Team must be capable of stepping in with the technical and management skills to make the on-the-spot decisions necessary to complete the task at hand.

The discussion that follows identifies those skills that are needed by members of the Recovery Management Team. If these positions are filled with qualified individuals, then the odds for a timely and successful recovery are very high.

a) Recovery Manager:
This individual needs to be a skilled manager/administrator who is accustomed to dealing with pressure situations. He should have a broad knowledge of the hardware and software in use at the site. He should be a "problem solver" as there will be many problems arise that have not been anticipated in advance. He must be able to delegate responsibility to others. He must also have signature authority to expend funds as a part of the disaster recovery process.
Security Officer – Dan Austin

b) Facilities Coordinator:
This individual needs some of the same skills as the Recovery Manager. However, he also needs to be familiar with the process of getting construction work scheduled and completed on time. He should be able to understand and oversee the setup of the electrical, environmental, and communications requirements of restoring the areas where the information systems are located, primarily the server rooms.
Manager of Engineering – Jimmy Stell

c) Administrative Coordinator:
This individual needs to be skilled in the business operations of the hospital. He should be well acquainted with the day-to-day operations of the hospital's departments. He should also be a "people person" who can deal with employees and their families during hard times. This person must also be familiar with purchasing procedures and contracts.
CEO – Phil Gilmore

d) Security Coordinator:
This individual needs to be skilled in the operations of the hospital and understand the security issues for safeguarding the protected health information of patients. This person must be familiar with the hospital security procedures and have a good knowledge of the hospital's critical areas.
Security Officer – Dan Austin

The following table contains a sample list of the people currently employed who could fill the positions on the Recovery Management Team. Alternates are to be listed, but other qualified individuals who could step in should any of these persons not be available should also be identified.

J. Activating the Disaster Recovery Plan

1. Appointment of Recovery Manager:
   The first order of business is to appoint the Recovery Manager. The person most appropriate for the position is the current Manager Information Systems. If the Manager Information Systems is unavailable, the Administrator should make the appointment. This person must have information systems management experience and must have signature authority for the expenditures necessary during the recovery process.

2. Determine Personnel Status:
   One of the Recovery Manager's important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster will affect any rescues or first aid necessary to people caught in the disaster. However, the Recovery Manager should produce a list of the able-bodied people who will be available to aid in the recovery process.

   If the appointed Recovery Management Team members are unavailable then the Recovery Manager, Administrative Coordinator, Facilities Coordinator and the Security Coordinator should be appointed immediately.

3. Equipment/Media Protection and Salvage:
   A primary goal of the recovery process is to restore information systems without the loss of any data. It is important that the Recovery Manager quickly set about the task of protecting and salvaging any magnetic media on which data may be stored. This includes any magnetic tapes, optical disks, CD-ROMs, and disk drives. The section on Equipment Protection and Salvage contains valuable information on salvaging damaged magnetic media.

4. Establish the Recovery Control Center:
   The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Recovery Manager should designate where the Recovery Control Center is to be established. If a location in the hospital premises is not suitable, the JSE Building has been designated as the off-site location of the center.

5. Activating the Disaster Recovery Plan:
   The Recovery Manager sets the plan into motion. Early steps to take are as follows:

   a) The Recovery Manager should retrieve the safe located in the ~~Alabama Street Office~~ Hamburg Clinic and open it to obtain an up-to-date copy of the Disaster Recovery Plan. This plan is in printed form in the box as well on computer media (diskette or CD-ROM). Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team. The

Recovery Manager is responsible for the remaining contents of the safe, which should probably be relocked if possible.

b) The Recovery Manager is to appoint the remaining members of the Recovery Management Team. This should be done in consultation with surviving members of the management. The Recovery Manager's decision about who sits on the Recovery Management Team is final, however.

c) The Recovery Manager is to call a meeting of the Recovery Management Team at the Recovery Control Center or a designated alternate site. The following agenda is suggested for this meeting:

- Each member of the team is to review the status of their respective areas of responsibility.
- After this review, the Recovery Manager makes the final decision about where to do the recovery. If the JSE building site is to be used, the Recovery Manager is to declare emergency use of the facility and notify the management.
- The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
- Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
- Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
- Each member of the team is to review the makeup of their respective recovery teams. If individual's key to one of the recovery teams is unavailable, the Recovery Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from other area computer centers or vendors.
- The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

d) The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.

e) Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones and/or two-way radios or the satellite phone.

K. Equipment Protection and Salvage:

This document contains information on procedures to be used immediately following an incident to preserve and protect resources in the area damaged.

1. Protection :

It is extremely important that any equipment, magnetic media, paper stocks, and other items at the damaged primary site be protected from the elements to

avoid any further damage. Some of this may be salvageable or repairable and save time in restoring operations.

- Gather all magnetic tape cartridges into a central area and quickly cover with tarpaulins or plastic sheeting to avoid water damage.
- Cover all computer equipment to avoid water damage.
- Cover all undamaged paper stock to avoid water damage.
- Ask the police/security to post security guards at the primary site to prevent looting or scavenging.

2. Salvage Magnetic and Optical Media :
   The magnetic and optical media on which our data is stored is priceless. Although we retain backups of our disk subsystems and primary application systems off-site, magnetic tapes stored in the tape vault and machine room area contain extremely valuable information that would be tough to lose. If the media has been destroyed, such as in a fire, then nothing can be done. However, water and smoke damage can often be reversed, at least good enough to copy the data to undamaged media.

   After protecting the media from further damage, recovery should begin almost immediately to avoid further loss. A number of companies exist with which the hospital can contract for large-scale media recovery services.

3. Salvage Equipment
   As soon as practical, all salvageable equipment and supplies need to be moved to a secure location. If undamaged, transportation should be arranged through the Recovery Manager to move the equipment to the JSE Building, or to another protective area (such as a warehouse) until the JSE Building is ready.

   If the equipment has been damaged, but can be repaired or refurbished, the JSE Building may not be the best location for the equipment, especially if there is water or fire damaged that needs to be repaired. Contractors may recommend an alternate location where equipment can be dried out, repainted, and repaired.

4. Inventory:
   As soon as practical a complete inventory of all salvageable equipment must be taken, along with estimates about when the equipment will be ready for use (in the case that repairs or refurbishment is required). This inventory list should be delivered to the Administrative Coordinator who will use it to determine which items from the disaster recovery hardware and supplies lists must be procured to begin building the recovery systems.

L. Damage Assessment:
   This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. The primary goal is to

determine where the recovery should take place and what hardware must be ordered immediately.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and building network should be conducted. If estimates from this process indicate that recovery at the original site will require more than 14 days, migration to the JSE Building is recommended.

M. Emergency Procurement Procedures:

The success or failure of this plan's ability to ensure a successful and timely recovery of the information systems hinges on our ability to purchase goods and services with lightening speed**.**

There should be a liberal policy for emergency procurement, coupled with extensive Business Interruption Insurance that will provide the Recovery Manager with a sound basis for aggressive recovery actions. Perhaps now is the time for a word of caution. There will always be a day of reckoning following every exciting event, when those actions taken under the stress of the moment will be examined and evaluated in the light of normalcy. You can significantly reduce your anxiety level in the eve of such an accounting by following preset rules and directives - to the extent possible under the circumstances - and most importantly, keeping records and logs of transactions.

The Administrative Coordinator is responsible for all emergency procurement for Information Systems. All Disaster Recovery Team members must submit their requests to the Coordinator.

The Administrative Coordinator is also responsible for tracking all acquisitions to ensure that financial records of the disaster recovery process are maintained and that all acquisition procedures will pass audit review.

The Administrative Coordinator must also be aware of the hospital’s insurance coverage to know what is and is not allowed under our policies. In the event an item to be purchased is disallowed by insurance coverage, or if expenses exceed the dollar limits of the insurance coverage, the Coordinator must consult with the Recovery Manager and other responsible hospital personnel.

M. JSE Building Preparation:

This document focuses on the preparation of the designated JSE Building for the recovery of information systems after a disaster has occurred. If the Recovery

Management Team opts to use the designated JSE Building for recovery after the disaster, some work must be done to convert the space to be able to house the computer systems, network equipment and disaster recovery team personnel.

In an extreme disaster where the JSE Building has also been rendered unusable, an alternate site must be chosen. Those sites may require additional work to prepare for the special power and cooling requirements of equipment.

1. Quick Review of Site Preparation Work:
   The JSE Building may have had only minimal advanced preparations; so much work is to be done in the early stages of the recovery process to make the site ready. The work may involve mainly physical, electrical, networking and air conditioning tasks. Here is a quick review of the facilities and work that must be done.

   - The computer equipment must be relocated to another area within the JSE Building. The JSE Building must be cleared to make the space available for staff and select users to do their work.
   - Adequate power capacity should be made available.
   - The site should have power conditioning equipment, such as an uninterruptible power supply (UPS) or motor generator.
   - The site should preferably have air conditioning equipment installed for equipment.
   - The JSE Building should have security, with doors controlled by a security system. It will be necessary to enter all personnel needing access to the area into the security system.

N. Information Systems Recovery Procedures:
This portion of the plan documents the detailed recovery procedures for each of the computer and network systems to be restored at the recovery facility. Each procedure documents the list of equipment necessary to restore service, power and cooling requirements, cabling and networking requirements, operating system and data restoration procedures, and procedures for placing the system into final form for general use.

1. Mainframe Systems Recovery:

   In the case that the CPSI servers are damaged CPSI will send someone down from their office with replacement equipment and do the work themselves. There should only be a couple of days of downtime in this situation.

2. Applications Recovery Overview: Once the platform system software and subsystems are operating correctly, the task of preparing the remaining end-user applications can begin. Each platform will have a unique recovery road to follow. In some cases, there may be very little to do except for general testing. In other

cases, considerable analysis and data synchronization work will likely be required.

The Recovery Team will be responsible for carrying out this phase of the recovery. Each application area will require a review. This review should be conducted by an analyst familiar with the application while working closely with an application user representative.

Items to be considered should include:

- Review of the Disaster Recovery Plan with special attention to any "interim" procedures that have been required in the time period since the disaster event occurred.
- Review of the application documentation concerning file and database recovery.
- Review the status of files and databases after the general platform recovery processing is complete.
- Identify any changes to bring the application to a ready for production status.
- Identify any areas where the application must be synchronized with other applications and coordinate with those application areas.
- Identify and review application outputs to certify the application ready for production use.

O. Alternate solution for accessing Critical Data:

The hospital's electronic protected health information is critical data that is maintained in the information systems. There would be applications that run and maintain this data and the delay in recovery could cause much hardship on staff, patients and others that depend on it. Other data may also be given very high priority in recovery.

Should a disaster place the hospital in a position where these data cannot be accessed by the normal applications systems, a secondary plan is established.

Proposed Interim Solution:

A set of manual procedures that would be implemented for using hard copies of the protected health information maintained in the hospital's Medical Records Department. Paper copies of patient forms and other documents required for providing services to patients are kept in the Disaster Lock Boxes to be used to follow manual procedures.

V. Review:

A. Basic Maintenance:

The plan will be routinely evaluated once each year by the Manager Information Systems, Security Officer and the Administrator of the hospital. In addition the plan will be tested on a regular basis and any faults will be corrected. The Disaster Recovery Plan coordinator has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and consistent with the rest of the plan.

B. Change-Driven Maintenance:

It is inevitable in the changing environment of the computer industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date. Changes that will likely affect the plan fall into several categories:

1. Hardware changes
2. Software changes
3. Facility changes
4. Procedural changes
5. Personnel changes

As changes occur in any of the areas mentioned above, the Manager Information Systems will determine if changes to the plan are necessary. This decision will require that the manager be familiar with the plan in some detail. After the changes have been made, the Manager Information Systems will incorporate the changes into the body of the plan and distribute as required.

C. Changes Requiring Plan Maintenance:

The following lists some of the types of changes that may require revisions to the disaster recovery plan. Any change that can potentially affect whether the plan can be used to successfully restore the operations of the hospital's information systems should be reflected in the plan.

1. Hardware: Additions, deletions, or upgrades to hardware platforms.

2. Software:

   a) Additions, deletions, or upgrades to system software.
   b) Changes to system configuration.
   c) Changes to applications software affected by the plan.

3. Facilities: Changes that affect the availability/usability of the JSE Building.

4. Personnel:

a) Changes to personnel identified by name in the plan.
b) Changes to organizational structure.

5. Procedural:

a) Changes to off-site backup procedures, locations, etc.
b) Changes to application backups.
c) Changes to vendor lists maintained for acquisition and support purposes.

VI. Related Policies and Plans:

Data contingency and backup plan
Emergency mode operation plan guidelines

VII. Related Documents:

Data contingency/Back up plan	
Serial Number: SC20	**Effective Date: 4/1/05**
Review Date: 1/1/2014	**Revision Date: 1/1/2014**
Approved By: Security Committee	**Approved Date: 3/21/05**

I. Plan Summary:

A. Introduction: Ashley County Medical Center safeguards the electronic protected health information maintained in the hospital's information systems from loss and for future retrieval as per the plan outlined in this policy.

This plan describes the method for creating, storing and retrieving exact copies of the electronic protected health information maintained in the hospital's information systems.

B. Regulatory Reference: Ashley County Medical Center has adopted this plan to ensure compliance with the requirements of Sections 164.308(a)(7) of the HIPAA Security rule relating to contingency plan.

C. Ashley County Medical Center reserves the right to modify the details and procedures of this plan at any time, with or without notice, at its sole discretion.

II. Definitions:

III. Responsibility:

Members of Ashley County Medical Center workforce are covered by and responsible for compliance with this plan. Supervisors, managers and department heads are responsible and accountable for ensuring adherence to this plan. The Manager Information Systems Privacy, Security and Compliance Officers will provide assistance to employees and management as needed.

IV. Data contingency and Backup Plan details:

Ashley County Medical Center has devised the following data backup plan to ensure that critical electronic protected health information is prevented from loss and can be retrieved in the event of a contingency situation.

A. Data criticality assessment:
1. The ACMC IT Staff will be responsible for analyzing the hospital's information systems to identify the hardware and software such as applications, servers and workstations that are connected as well as not

connected to the hospital's network where electronic protected health information is maintained and must be backed up to prevent loss of critical data.

2. This assessment will be an ongoing practice and will identify any new information systems that require data backup.

3. ACMC will have two types of information backed up.

    a) CPSI Information Backed Up on Ultrium 4 Tapes
    b) All other ePHI backed up on a 6TB NAS

4. The following information systems maintain electronic protected health information and will be backed up:

    a. CPSI Linux Server
        a. Backup Daily to Ultrium 4 Tape on 4 week rotation of tapes.
        b. Monthly Tapes are never overwritten.
        c. Synced every hour with Warm Server
    b. EMD Database and Image Server
        a. Backup Daily to NAS
    ~~c. ACMC-Server1~~
        ~~a. Backup every Saturday @ 12:00am~~
    d. Web-Server
        a. Backup Weekly to NAS
    e. Quantim Server
        a. Backup Weekly to NAS
    f. Docuvoice
        a. Backup Weekly to NAS
    g. Call Manager
        a. Backup Weekly to NAS
    h. ACMC-FTP Server
        a. Backup Weekly to NAS
    i. EMD Fax Server
        a. Backup Weekly to NAS
    j. Hmailserver
        a. Backup Weekly to NAS

B. <u>Creating data back up:</u>
    1. <u>Personnel authorized for taking back up:</u> The ACMC IT Staff will have access to backup all data.

    2. <u>Data on the hospital's network:</u> The ACMC IT department will monitor automated backup processes listed in IV.A.3 of this policy.

3. Data stored on individual workstations: Data that is stored on individual workstations will be backed up to a user's network folder at their discretion. With access being only granted to that user and the administrator of the network.

4. Data backup: The data backup will be primarily daily, weekly and monthly and the tapes will be rotated to enable restoration till the point of failure. Data backup should also be taken when installing a new software or software patch to ensure restoration in the event of loss of data while installation.

C. Data Backup log:
   1. The ACMC IT Staff will maintain a log of the data in the Data Backup logs. The data backup logs will record details such as the data and time and the person's signatures that checked the back up.

   2. The ACMC IT Staff will keep the Data Backup logs and access to the log will be provided to designated personnel such as the Security Officer for retrieval of data and restoration of systems in case of an emergency where the ACMC IT Staff is unavailable.

D. Data storage:
   1. The CPSI backup data will be labeled, dated, and stored as follows:

      a. Daily tapes are stored in fireproof safe in ACMC Server Room
      b. Weekly tapes are stored in fireproof safe at the ~~JSE Building~~ Hamburg Clinic.
      c. Monthly tapes are sent to CPSI in Mobile, AL for testing then returned to ACMC. Monthly tapes are then stored in Fireproof Safe at the ~~Business Office~~ Hamburg Clinic never to be overwritten.

   2. The rest of the backed up data will be stored on the ACMC 6TB NAS located in the ACMC Server Room.

   3. A log will be maintained of movement of the backed up data into and out of storage. The log will record details such as the data and time and the person's name and signatures that delivered or retrieved the data from storage.

E. Procedure for contingency situation:
   1. Notification: In the event of a contingency situation where electronic protected health information is lost, the hospital's Security Officer and ACMC IT Staff will be notified immediately.

   2. Assessment of data loss: The ACMC IT Staff will assess and identify the lost data and will restore it from backup maintained by the hospital.

In case of a contingency situation where the ACMC IT Staff is unavailable and the restoration of data is critical, the Security Officer will access the data backup and restore the data with the help of other personnel authorized to access and restore the data.

3. Data retrieval:
   a) The ACMC IT Staff and the Security Officer will be authorized to access and retrieve data from storage. If another person is asked to retrieve the data from the storage then this person will have to be authorized for access and retrieval by the Security Officer.

   b) The details of the data and the person retrieving it from storage will be recorded in the log maintained as mentioned above in paragraph IV.C 2.

4. Data restoration:
   Data will be restored using the daily, weekly and monthly backup tapes or other media if required to enable data being restored to the point of failure.
   Data restoration procedures for each application are provided in the Disaster Recovery Plan guidelines, which will be followed if the ACMC IT Staff is not available in a contingency situation.

V. Plan Review:

The Security Officer shall review this plan annually to determine if the plan addresses the data backup and contingency requirements. The plan will be reviewed and updated as needed.

VI. Related Policies:

Data backup policy
Contingency plan policy
Disaster recovery plan

VII. Related Documents:

Data backup log