Administrative Manual

UNC HEALTH CARE	Policy Name	**Information Security**
	Policy Number	**ADMIN 0082**
	Date this Version Effective	**September 2013**
	Responsible for Content	**UNC HCS Information Security Council**

I. Description

UNC Healthcare System requirements for protecting confidential information, including but not limited to protected health information (PHI), from inappropriate access or disclosure and/or security breaches.

II. Rationale

UNC Healthcare System (UNC HCS) and its affiliates (collectively referred to in this policy as “UNC HCS”) continue to increase their dependence upon computer systems for storage, processing and transmission of information. As a result, information is now more readily available in all areas of UNC HCS. This availability, along with regulatory changes that define the requirements for protecting information and the penalties for failing to do so in the healthcare environment, has heightened the necessity for careful controls regarding information security.

III. Policy

A. Procedure

1. It is the policy of UNC HCS that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

2. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years per HIPAA regulations, or more for certain documents if required by applicable laws and regulations, after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within UNC HCS.

3. At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

B. Scope

1. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

2. The framework for managing information security in this policy applies to all UNC HCS entities and workers, and other Involved Persons and all Involved Systems throughout UNC HCS as defined below in INFORMATION SECURITY DEFINITIONS.

3. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

C. Risk Management

1. A risk assessment of applicable UNC HCS information networks and systems will be conducted on a periodic basis as required by HIPAA and the PCI Data Security Standard. The risk assessment will document the threats and vulnerabilities to stored and transmitted PHI and Confidential information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic -- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

   From the combination of threats, vulnerabilities, and likely impacts, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk assessment will be determined as follows:

   - Entities accepting credit cards from patrons, and seeking compliance with the Payment Card Industry Data Security Standard, must assess risk to Account Data on an annual basis.

2. Risks to PHI in UNC HCS enterprise systems will be assessed on a schedule determined by the UNC HCS Chief Information Officer. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

D. Information Security Definitions

1. Account Data

Data subject to Payment Card Industry Data Security Standard protection.

a. Primary account number by itself or in combination with card holder name, expiration date or service code.

b. Primary account number in combination with sensitive authentication data such as magnetic stripe data or equivalent on a chip, PINs/PIN blocks, or CAV2/CVC2/CVV2/CID.

2. Affiliated Covered Entities (ACE)

Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA. (See UNC HCS Policy ADMIN 0139, Privacy/Confidentiality of PHI, for a listing of the members of the ACE.)

3. Availability

Data or information is accessible and usable upon demand by an authorized person.

4. Confidentiality

Data or information is not made available or disclosed to unauthorized persons or processes.

5. Encryption

The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

6. HIPAA

Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), as modified by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and its implementing regulations at 45 CFR Parts 160 and 164, as the same may be amended from time to time.

7. **Integrity**

   Data or information has not been altered or destroyed in an unauthorized manner.

8. **Involved Persons**

   Every worker at a UNC HCS entity -- no matter what their status might be. This includes physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

9. **Involved Systems**

   All computer equipment and network systems that are operated within the UNC HCS environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), storage devices (CD-ROMs, diskettes, memory keys, enterprise disk systems, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

   All third party information systems services contracted by the UNC HCS to provide software-as-a-service, hosting service, and/or systems administration service outside the UNC HCS environment in support of processing, transmitting or storing UNC HCS information are covered by this policy.

10. **Identity Theft Protection Act (ITPA)**

    A North Carolina state Law that imposes certain obligations on NC State agencies and NC businesses concerning the collection, use, and dissemination of Social Security Numbers and other personal information. (UNCHCS Policy ADMIN 0088, Identity Theft Policy)

11. **Payment Card Industry Data Security Standard (PCI DSS)**

    Developed by the payment card industry, PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

12. **Protected Health Information (PHI)**

    PHI is health information, including demographic information, created or received by the UNC HCS entities which relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that identifies or can be used to identify the individual.

13. **Risk**

    The probability of a loss of confidentiality, integrity, or availability of information resources.

E. UNCHCS Information Security Responsibilities

1. **Information Security Office**

   The Information Security Office (ISO) for the UNC Health Care System is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of UNC HCS. Specific responsibilities include:

a. Ensuring security policies, procedures, and standards are in place and adhered to by entity.

b. Providing basic security support for all systems and users.

c. Advising owners in the identification and classification of computer resources. (See Section F. Information Classification.)

d. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.

e. Detecting vulnerabilities, qualifying according to risk, notifying technical owners for repair, and escalating as necessary.

f. Detecting unauthorized access to UNC HCS information systems and networks and responding appropriately.

g. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.

h. Providing on-going employee security education.

i. Performing security audits.

j. Reporting dually to the UNC HCS Information Services Oversight Committee and Compliance Steering Committee on entity's status with regard to information security.

2. Information Owner

The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the UNC HCS Information Owner Delegation Form. The owner of information has the responsibility for:

a. Knowing the information for which she/he is responsible.

b. Determining a data retention period for the information.

c. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.

d. Authorizing access and assigning custodianship.

e. Specifying controls and communicating the control requirements to the custodian and users of the information.

f. Reporting promptly to the ISO the loss or misuse of UNC HCS information.

g. Initiating corrective actions when problems are identified.

h. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.

i. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

3. **Custodian**

The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

a. Providing and/or recommending physical safeguards.

b. Providing and/or recommending procedural safeguards.

c. Administering access to information.

d. Releasing information as authorized by the Information Owner and/or the Information Privacy/Security Officer for use and disclosure using procedures that protect the privacy of the information.

e. Evaluating the cost effectiveness of controls.

f. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.

g. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.

h. Reporting promptly to the ISO the loss or misuse of UNC HCS information.

i. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

4. **User Management**

UNC HCS management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

a. Reviewing and approving all requests for their employees’ access authorizations.

b. Initiating security change requests to keep employees' security records current with their positions and job functions.

c. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

d. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

e. Providing employees with the opportunity for training needed to properly use the computer systems.

f. Reporting promptly to the ISO the loss or misuse of UNC HCS information.

g. Initiating corrective actions when problems are identified.

h. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

5. **User**

The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

a. Access information only in support of their authorized job responsibilities.

b. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.

c. Refer all disclosures of PHI (1) outside of UNC HCS and (2) within UNC HCS, other than for treatment, payment, or health care operations, to the applicable entity's health information management department. In certain circumstances, the health information management department policies may specifically delegate the disclosure process to other departments. (For additional information, see UNC HCS Policy ADMIN 0139, Privacy/Confidentiality of PHI.)

d. Keep personal authentication devices (e.g., passwords, SecureCards, PINs, etc.) confidential.

e. Report promptly to the ISO the loss or misuse of UNC HCS information.

f. Initiate corrective actions when problems are identified.

F. Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification, the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

1. Protected Health Information (PHI)

a. PHI is information, whether oral or recorded in any form or medium, that:

i. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and

ii. relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and

iii. includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual.

b. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to UNC HCS and its patients or research interests.

2. Confidential Information

a. Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

Confidential Information also includes Personal Information (PI) defined by the NC Identity Theft Protection Act. Refer to UNC HCS Policy Admin 0008, Identity Theft Policy, for a complete listing of PI. Confidential Information also includes Account Data as defined in the Payment Card Industry Data Security Standard (PCI DSS),

Other examples of Confidential Information may include: personnel information, personal information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

b. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for UNC HCS, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

3. **Internal Information**

a. Internal Information is intended for unrestricted use within UNC HCS, and in some cases within affiliated organizations such as UNC HCS business partners. This type of information is already widely-distributed within UNC HCS, or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories.

b. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.

c. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

4. **Public Information**

a. Public Information has been specifically approved for public release by a designated authority within each entity of UNC HCS. Examples of Public Information may include marketing brochures and material posted to UNC HCS entity internet web pages.

b. System policies and procedures and many electronic mail messages (unless subject to attorney-client, peer review or other privilege) that are considered public records.

c. This information may be disclosed outside of UNC HCS.

G. Computer and Information Control

All involved systems and UNC HCS information are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

1. **Ownership, Installation and Licensing of Software and Digital Content**

All computer software and digital content developed by UNC HCS entity employees or contract personnel on behalf of UNC HCS or licensed for UNC HCS use is the property of the applicable UNC HCS entity. Distribution, installation and use must be in accordance with the UNC HCS entity's license agreement.

All software packages and digital content that reside on computers and networks within UNC HCS must comply with applicable licensing agreements and restrictions and must comply with UNC HCS acquisition of software policies.

2. **Inventory**

Each entity will ensure that an inventory is maintained of its computers and applications. The inventory must minimally include classification of computer (end user workstation, server, printer, etc.), operating system, using department, team responsible for technical support and criticality. The inventory must be accessible by the Information Security Office.

3. **Virus Protection**

Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

4. Access Controls

Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by UNC HCS. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

a. Authorization: Access will be granted on a “need to know” basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

   i. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.

   ii. Role-based access: An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

   iii. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

b. Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

   i. At least one of the following authentication methods must be implemented:

      (1) strictly controlled passwords (Attachment 1 – Password Control Standards),

      (2) biometric identification, and/or

      (3) tokens in conjunction with a PIN.

   ii. Password security:

      (1) Users may never share their passwords with another person. Users may never use someone else’s password.

      (2) Users must keep passwords, tokens, PINs, and other authentication mechanisms confidential and/or appropriately secured.

      (3) Information systems must be configured to meet the information security password control standards which address:

         (a) Minimum length and complexity

         (b) Expiration

         (c) Reuse

         (d) Unsuccessful login attempts

         (e) Password protection during user entry, transmission and in storage.

      (4) Procedures must be in place and followed for validating users who request to have their password reset.

iii. An automatic timeout with re-authentication must be required after a certain period of inactivity as approved by the Information Security Office.

iv. The user must log off or secure the system when leaving it.

c. Data Integrity: UNC HCS must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

i. transaction audit

ii. disk redundancy (RAID)

iii. ECC (Error Correcting Memory)

iv. checksums (file integrity)

v. encryption of data in storage

vi. digital signatures

vii. Use of drop down menus, radio buttons, and data validation etc. in lieu of free form text fields in data entry screens.

d. Transmission Security: Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

i. integrity controls and

ii. encryption, where deemed appropriate

Messaging Systems (i.e., email, instant messaging, text messaging): Use of commercial or open source IM, email and text messaging services for transmitting PHI or Confidential information must be protected by an approved encryption mechanism. .

e. Remote Access: Access into UNC HCS network from outside will be granted using UNC HCS approved methods and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, the same level of protections must be maintained for PHI, Confidential and/or Internal Information that is stored or accessed remotely as PHI, Confidential and/or Internal information stored and accessed within the UNC HCS network.

f. Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

The following physical controls must be in place:

i. Information systems deemed “critical” by technical and business owners must be installed in an access-controlled area. The area in and around the computer facility must have appropriate protections against fire, water damage, power and HVAC outages, theft and vandalism.

ii. Information systems containing PHI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

iii. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

(1) Position workstations to minimize unauthorized viewing of protected health information.

(2) Grant workstation access only to those who need it in order to perform their job function.

(3) Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.

(4) Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI.

(5) Use automatic screen savers with passwords to protect unattended machines.

iv. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

(1) Contingency Operations – Documented procedures that allow controlled facility access in support of restoration of lost data, equipment and/or facilities during emergency operations after a disaster.

(2) Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(3) Access Control and Validation – Documented procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(4) Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

g. Emergency Access:

i. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

ii. Procedures must be documented to address:

(1) Authorization,

(2) Implementation, and

(3) Revocation

5. Equipment and Media Controls

The disposal of information must ensure the continued protection of PHI, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

a. Information Disposal / Media Re-Use of:

i. Hard copy (paper and microfilm/fiche)

ii. Magnetic media (floppy disks, hard drives, zip disks, etc.)

iii. CD ROM Disks

iv. Copiers and printers with hard drives.

b. Accountability: Each entity must maintain a record that tracks the custody of hardware and electronic media.

c. Data backup and Storage: When needed, create a retrievable, exact copy of electronic PHI before movement of equipment. Data transmitted outside the facility must be protected by encryption during transmission.

6. Other Media Controls

a. PHI and Confidential Information stored on removable media (diskettes, CD-ROMs, portable storage, memory sticks, etc.) must be protected from unauthorized access in the event the removable media is lost or stolen. PHI and Confidential Information must be protected by encryption if stored on removable media.

b. PHI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

i. Power-on passwords

ii. Auto logoff or screen saver with password

iii. Encryption of transmitted and stored data.

Further, mobile computing devices must never be left unattended in unsecured areas.

c. If PHI or Confidential Information is stored on removable media or mobile computing devices and there is a breach of confidentiality as a result, then the person who stored the PHI or Confidential Information on the media/device will be held personally accountable and is subject to the terms and conditions of UNC HCS and SOM Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with UNC HCS.

7. Data Transfer/Printing

a. Electronic Mass Data Transfers: Downloading and uploading PHI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research purposes that include PHI must be approved through the Institutional Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring PHI to external entities.

b. Other Electronic Data Transfers and Printing: PHI, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PHI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PHI that is downloaded for educational purposes where possible should be de-identified before use.

c. Protecting Data Transfers: PHI and Confidential Information transfers outside of the UNC HCS network must be protected with encryption. The sender must ensure the recipient is authorized to have custody of the PHI and Confidential Information before transfer.

8. **Social Media**

   a. Except as permitted by and in accordance with applicable UNC HCS HIPAA policies and other related policies, communications using Social Media may not divulge PHI, confidential or proprietary information about UNC HCS and may not violate patient privacy and confidentiality policies and laws.

   b. Except as described in 8.a. above, communications using Social Media must never contain any information that directly or indirectly identifies a patient. This may include information that does not directly identify a patient, but would permit someone to identify a patient, either through the identification of a disease or health condition; an event precipitating the patient's health condition, such as an accident or other trauma; the patient's or provider's location within UNC HCS; the names and or specialties of the patient's health care team; the patient's language or country of origin; or any other detail that alone or in combination with other facts in the public or private domain might allow a third party to identify the patient.

   c. Except as described in 8.a. above, communications using Social Media must never contain patient photos, whether such photo directly or indirectly identifies a patient or only includes non-identifiable patient images, such as wounds, diseases, the results of diagnostic tests, or similar images. Unless in the context of providing treatment or educational use, it is never permissible to photograph or disclose any photograph of a patient or his or her anatomy or test results without a signed release, available from the healthcare entity's public relations department.

9. **Audit Controls**

   Hardware, software, and/or procedural mechanisms that record and examine activity by users and systems administrators in information systems that contain or use PHI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

10. **Evaluation**

   UNC HCS requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

11. **Contingency Plan**

   UNC HCS entities must make plans to enable recovery from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

   a. Data Backup Plan

      i. A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

      ii. Backup data must be stored in an off-site location and protected from physical damage.

      iii. Backup data must be afforded the same level of protection as the original data.

b. Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data, system and application software, and equipment in the event of fire, vandalism, natural disaster, or system failure.

c. Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

d. Testing and Revision Procedures: Procedures should be developed and documented and executed to test written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

e. Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

--- ATTACHMENT 1 ---

Password Control Standards

The UNC HCS Information Security Policy requires the use of **strictly** controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See UNC HCS Information Security Policy for definition of these protected classes of information.)

Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for passwords for systems that access PHI, CI, II:

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
3. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
4. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e., children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters is more difficult to guess.

Where possible, system software must be used to enforce the following password safeguards and standards for user passwords. :

1. Passwords routed over any network must be encrypted.
2. Passwords in storage must be encrypted.
3. Passwords must be entered in a non-display field.
4. System software must disable the user identification code when more than five consecutive invalid passwords are given. Lockout time must be set at a minimum of 30 minutes.
5. Passwords must contain at least 1 upper case, 1 lower case and 1 number. A special character may be used in lieu of any of these types of characters; however, this is not recommended due to challenges entering special characters on tablet PCs.
6. Passwords must have a minimum length of 10 characters.
7. Passwords must be forced to change annually. Where specified in laws and regulations, applicable passwords must be set to change more frequently.
8. System software must maintain a history of at least the previous six passwords and prevent their reuse.

--ATTACHMENT 2--

Internet File Sharing and Cloud File Storage

Peer-to-peer:

Peer-to-peer (P2P) file-sharing programs such as Bit Torrent, KaZaA, Gnutella, LimeWire, iMesh, CuteMX, Scour Exchange and FreeNetfile, are prohibited on UNC HCS networks for the following reasons:

1. Ability to locate open computer ports on a firewall to defeat blocking attempts.
2. Designed to enable covert file sharing among anonymous parties for purposes of sharing copyrighted music, videos and games.
3. Enable malicious software to enter the UNC HCS network undetected.

It should be noted that a few products have now become commercially available that are based on P2P file-sharing technologies, but do not share the same risks that are described in this policy. Use of P2P technology for legitimate business purposes and that does not pose undue risk to UNC HCS PHI or Confidential Information may be used upon approval by the entity’s Information Security Officer.

Internet Storage and File Sharing:

Internet storage and file sharing services such as Dropbox, Google Play and Google Docs, Apple iCloud, Microsoft SkyDrive, and Amazon Cloud Drive may not be used for sharing and storing PHI and Confidential Information. PHI and Confidential Information transmitted outside the UNC HCS network must be protected by encryption and may only be shared with authorized recipients.