Origination:	*09/2013*
Effective:	*08/2021*
Last Approved:	*08/2021*
Last Revised:	*08/2021*
Next Review:	*08/2023*
Owner:	*De Ann Young: HCS Exec Dir Info Tech - CISO*
Policy Area:	*ISD*
Policy Tag Groups:	
Applicability:	*UNC Health Care System (all owned and managed entities)*

Information Security

APPLICABILITY:

This policy applies to the following entities (collectively referred to as **"UNC Health"** in this policy):

✓	UNC Health Care System / UNC Medical Center*	✓	Johnston Health
✓	UNC Physicians Network	✓	Lenoir Memorial Hospital
✓	UNC Physicians Network Group Practices / UNC Physicians Group Practices II	✓	Margaret R. Pardee Memorial Hospital
✓	Rex Healthcare / Rex Hospital	✓	Nash Healthcare System/Nash Hospitals
✓	Chatham Hospital	✓	Wayne Memorial Hospital
✓	Caldwell Memorial Hospital		
✓	UNC Rockingham Health Care / UNC Rockingham Hospital		

***UNC Medical Center includes all UNC Hospitals' facilities and the clinical patient care programs of the School of Medicine of UNC-Chapel Hill (including UNC Faculty Physicians).**

This policy also covers UNC Health Southeastern as part of the IT Services agreement. Updates to the APPLICABILITY table will occur when UNC Health Southeastern joins the UNC Health PolicyStat system.

I. Description

This policy contains the UNC Health Care System ("UNC HCS") requirements for protecting mission critical information technology assets and confidential information, including but not limited to Protected Health Information ("PHI"), as defined by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), from inappropriate access or disclosure and/or security breaches.

II. Definitions

- **Authentication**
  A process by which a computer system interacts with a user to confirm the user's identity. Authentication commonly occurs through the use of a login ID/password combination and, in some cases, a key fob, hardware token or cell phone held by the user is involved in the authentication to prevent access by someone who has stolen a password.
- **Cyber Threat**
  Malicious software developed or intrusion techniques carried out by a person intending to damage systems or steal data, and with advanced knowledge of network technologies, computer software, operating systems,

and social engineering.

- **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.
- **External Information Systems**
  Systems to which UNC HCS subscribes or that are owned or leased but not installed in a UNC HCS leased or owned building. Examples include cloud services and software-as-a-service (e.g., LMS, MySupport@UNC and ShareFile.)
- **Internal Information Systems**
  Systems to which UNC HCS subscribes or that are owned or leased and are installed in a UNC HCS leased or owned building. Examples include Epic and Lawson.
- **Information or Network User ("User")**
  Every worker, third party or trainee at a UNC HCS entity who has been given UNC HCS information or access to a UNC HCS network. This includes but is not limited to physicians, researchers, residents, students, employees, vendors, contractors, consultants, temporaries, volunteers, and interns.
- **Minimum Necessary**
  HIPAA rule that requires HIPAA covered entities, when using, disclosing, or requesting PHI, to limit access to PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request.
- **Need To Know**
  The practice of authorizing access to or distributing sensitive information based on what an information the user needs to know to perform an assigned task or job duty he is authorized to perform.
- **Principle of Least Privileged**
  The practice of authorizing access rights for computer and software users and system administrators to the lowest level of functionality that they can have in a system and still do their jobs. The principle of least privilege is typically accomplished through the use of roles, templates or profiles.
- **Privileged Access**
  The ability to change security settings, change configuration settings; turn off a service; create, modify or delete accounts; or escalate permissions in a critical telecommunications network, technical service, or server, or in a database or application that contains or provides access to PHI and confidential information
- **Risk**
  The probability of a loss of confidentiality, integrity, or availability of information resources combined with the impact of the loss.
- **Technology Acquisition**
  Entering into an agreement to own, lease or subscribe to use hardware, software (applications, utilities, tools, middleware, etc.), data, or other content, appliances, Internet of Things (i.e. cameras, facility monitors, specimen freezers and refrigerators, forklifts and other warehouse management equipment that require network connectivity), and medical devices that require network connectivity.
- **Two-factor Authentication (2FA)**
- When the authentication process requires not only a login ID/password entry by an end user, but also involves the use of something held by the user such as a key fob, hardware token or smartphone to successfully complete the process and gain access to a system. 2FA is commonly used to prevent access by an unauthorized person who has acquired stolen passwords.

III. Rationale

Information Technology and Analytics are a foundation for quality patient care and many strategic initiatives for the UNC Health Care System (UNC HCS) and its affiliates (collectively referred to in this policy as "UNC HCS"). Technology advancements are being driven throughout UNC HCS and information is now more readily available in all areas. At the same time, health care information and networks are a target by malicious Internet actors (aka Cyber threats) because they present opportunity for financial gain. Cyber threats, along with regulatory changes that define the requirements for protecting information and the penalties for failing to do so in the health care environment, has heightened the necessity for careful controls regarding information security.

IV. Scope

- This policy covers the confidentiality, integrity and availability of UNC HCS electronic information, stored, processed, transmitted and used in both internal and external information systems and networks.
- All UNC HCS Information or Network Users ("User") are responsible for complying with this policy.
- All UNC HCS electronic information of any type (e.g.,. audio, video, pictures, text, structured data) on any form of electronic media (e.g. screen display, removable media, computer hard drives, mobile devices etc.) must be protected in accordance with this policy.

V. Policy

It is the policy of UNC HCS that electronic information, as defined herein, in all its forms-- electronically recorded, transmitted 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

A. Documentation

1. All information security policies, standards and procedures must be documented and made available to individuals responsible for their implementation and compliance. All such documentation must be retained for six years per HIPAA regulations, after initial creation, or after changes are made. Where document review period is not specified in UNC HCS policy or in the document itself, documents must be reviewed every two years.
2. Entity or departmental procedures will be developed supporting the implementation of this policy at entity, department and IT services level. All departmental procedures must be consistent with this policy.
3. Information security activities such as information security risk assessments, corrective action plans, security incidents and audits must be documented and retained for six years.

B. Risk Management

1. Risk assessments of applicable UNC HCS information networks and systems will be conducted on a periodic basis as required by HIPAA and the Payment Card Industry Data Security Standard (“PCI DSS”).
2. The schedule for risk assessments is determined by the UNC HCS Chief Information Security Officer.
3. Risk assessments must include a corrective action plan targeting the highest risks identified in the risk assessment. Progress on corrective actions must be tracked to completion.

C. UNC HCS Information Security Responsibilities

1. **Information Security Office**
   The UNC HCS Information Systems Division (ISD) Information Security Office (ISO) is responsible for:
   a. Assessing information security risks.
   b. Advising Senior Leadership, Custodians (as defined herein) and Users (as defined herein) of imminent cyber threats, risks to information and mission critical systems, and courses of action.
   c. Ensuring security policies and standards are in place and effectively communicated.
   d. Providing information security support to UNC HCS Users.
   e. Advising systems and application owners in the identification and classification of computer resources. (See Section D. Information Classification.)
   f. Advising and educating information Custodians in the implementation of appropriate security controls in all phases of a system or application life cycle.
   g. Detecting information security vulnerabilities, qualifying according to risk, notifying system owners for repair, tracking progress and escalating if necessary.

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

i. Providing on-going security education to UNC HCS Users, and application and information owners.

j. Performing security compliance reviews and evaluations.

k. Reporting UNC HCS entity security posture to entity and health system leadership..

2. **Information Owner**

The Information Owner is a person or entity that can authorize or deny access to the information and is responsible for its accuracy, integrity, and timeliness. An Information Owner is responsible for:

a. Knowing the privacy and security regulatory requirements for 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 confidentiality and to ensure integrity and timeliness of the information.

d. In conjunction with Custodians, establishing access authorization and granting procedures commensurate with the classification of information and compliant with applicable regulations and policies.

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 information User education and awareness by defining acceptable uses of the information for Users' and their management.

i. Following technology reviews and approval processes for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

3. **Custodian**

The Custodian of information is a person or organization with control over original or a copy of information and/or the security controls that protect and permit access to it. Most often the Custodian is an information technology department such as ISD. However, a User becomes a Custodian when he/she makes a copy of information outside the security controls put in place by ISD, and a third party becomes a Custodian when ISD or a User transfers data to the third party. Responsibilities include:

a. Knowing the security controls applicable to the sensitivity of the information in their custody.

b. Implementing, monitoring and maintaining the appropriate security controls of the information in their custody.

c. In conjunction with Information Owners, establishing access authorization, granting and termination procedures commensurate with the classification of information and compliant with applicable regulations and policies.

d. Administering appropriate access to the information based on authorization.

e. Releasing information as authorized by the Information Owner and in accordance with UNC HCS Privacy and Security policies.

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

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

4. **User Management**

User Management supervises employee and third party Users, overseeing their use of information and information technology resources, including:

a. Reviewing and approving requests for their Users' access.

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

c. Promptly informing ISD of Users' terminations and transfers, in accordance with ISD Identity and Access Management (IAM) procedures.

d. Revoking physical access of terminated Users (i.e. retrieving badge, keys).

e. Reporting promptly to the Information Security Office the loss of control or misuse of UNC HCS information.

f. Initiating corrective actions when problems are identified.

g. Following technology review and approval processes for the selection, budgeting, purchase, and implementation of any new technology to manage information or connect to a UNC HCS network..

5. **User**
   The user is any person who has been authorized to read, enter, or update UNC HCS information or to use a UNC HCS network. A User 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 Information Owner and Custodian.

   c. Refer all requested disclosures of PHI for purposes other than for treatment, payment, or health care operations, to the applicable entity's Health Information Management department or Privacy Office.

   d. Keep personal authentication devices (e.g., passwords, badges, PINs, SmartPhones etc.) confidential and if applicable, physically secured..

   e. Report promptly to the Information Security Office the loss of control or misuse of UNC HCS information.

   f. Initiate corrective actions when problems are identified.

D. Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. The classification assigned and the related controls applied are dependent upon the sensitivity of the information. The following levels are to be used when classifying information:

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

   a. PHI as defined in the UNC HCS Privacy Policy - *PHI and the De-Identification of PHI*, is information (in any format whether electronic, paper or oral) that:

      i. is created or received by a health care provider, health plan, or health care clearinghouse; and

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

      iii. the past, present, or future payment for the provision of health care to an individual.

   b. **AND** there is a reasonable basis to believe the information can be used to identify the individual; **OR**

   c. The information includes one or more of the following nineteen (19) identifiers (of the individual or his or her relatives, household members or even of the individual's employer):

      i. Name

      ii. Geographic subdivisions smaller than a state (i.e., county, town or city, street address, and zip code and equivalent geocode) (note: in some cases, the initial three digits of a zip code may be used)

      iii. All elements of dates (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death, all ages over 89 and dates indicative of age over 89) (note: ages and elements may be aggregated into a single category of age 90 or older)

iv. Phone numbers
v. Fax numbers
vi. Email addresses
vii. Social security number
viii. Medical record number
ix. Health plan beneficiary number
x. Account numbers
xi. Certificate/license numbers
xii. Vehicle identifiers and serial numbers, including license plate numbers
xiii. Device identifiers and serial numbers
xiv. URLs
xv. Internet protocol (IP) address numbers
xvi. Biometric identifiers (e.g., fingerprints)
xvii. Full face photographic and any comparable images
xviii. Any other unique identifying number, characteristic, or code
xix. Any other information about which UNCHCS has actual knowledge that could be used alone or in combination with other information to identify the individual

2. **Confidential Information**
   a. Confidential Information is sensitive material, other than PHI, that may be confidential under applicable law or is otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
   b. Confidential Information includes, but is not limited to: Personal Information (PI), as defined in the UNC HCS Privacy Policy – *Breach Notification*; Account Data as defined in the Payment Card Industry Data Security Standard; sensitive financial information; intellectual property; proprietary business or research information; system passwords; identify verification information; and file encryption keys.
   c. Unauthorized disclosure of Confidential Information to individuals without a need to know may violate laws, regulations and/or internal policies, or may cause significant problems for UNC HCS, its customers, its employees, or its business partners. Decisions about the provision of access to confidential information must always be in compliance with regulations, UNC HCS policies or direction set forth by Information Owner of the confidential information..
3. **Internal Information**
   a. Internal Information is intended for unrestricted use within UNC HCS, and in some cases. with appropriate authorization and agreements as determined by UNC HCS policy or the Information Owner, may be disclosed to UNC HCS business partners.
   b. This type of information may be distributed within the organization without advance permission from the Information Owner.
   c. Internal Information may include personnel directories, conference room schedules, invoice and purchase order information, equipment inventories, etc.
   d. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.
   e. Unauthorized disclosure of Internal information to a third party, although not a reportable data breaches, is a violation of this policy.
4. **Public Information**

a. Public Information is intended for a general public audience, and has been approved for public release by a designated authority within each UNC HCS entity.

b. Examples of Public Information may include but is not limited to marketing brochures, way-finding information, news articles, and physician and specialty listings.

c. UNC HCS and the North Carolina Public Records Act:

- The UNC Medical Center is a state entity, but all other UNC HCS entities are not. The UNC Medical Center is subject to the North Carolina Public Records Act and its records are generally considered to be Public Records unless specifically protected by applicable law (such as attorney-client privilege, peer review, privacy laws, or other legal protections). Information covered under the North Carolina Public Records Act for UNC Medical Center, may have been classified as Internal or Confidential information for all other UNC HCS entities (i.e. policies and procedures, business information, compensation.)
- Any Public Records request must be reviewed by the UNC HCS Legal Department for compliance with laws before information is released.

E. Technology Management and Controls

1. **Standards and Acquisition**

a. UNC HCS ISD will maintain security and strategic standards (i.e. application portfolio simplification) for technology.

b. Any new technology proposed for UNC HCS information or network use must be assessed by the ISD Architecture Review Board (ARB) against the security and strategic technology standards. Results of the ARB assessment must be taken into consideration and material issues resolved before proceeding with technology acquisition.

c. Contracts for technology acquisition that will connect to the UNC HCS network must include UNC HCS cyber security language that compels vendors/manufacturers to provide technology that is secure-able. The cyber security contract language will change from time to time to reflect changes in technology and the cyber security industries, and will be maintained by the UNC HCS ISD Information Security Office.

2. **Ownership and Licensing**

a. All software and digital content developed by UNC HCS entity employees or contract personnel on behalf of UNC HCS is the property of the applicable UNC HCS entity.

b. Computer software and digital content for which a UNC HCS entity has purchased a perpetual license is the property of the applicable UNC HCS entity.

c. Distribution, installation and use of acquired software and digital content must comply with applicable licensing agreements and restrictions.

d. All new software products must be approved by UNC HCS ISD before installation on UNC HCS computers and servers. Software installed on a UNC HCS ISD computer or server that has not been approved by ISD may be removed by ISD..

3. **Inventory**

a. UNC HCS ISD will maintain an inventory system for UNC HCS hardware and software. The inventory must have a record of all workstations, servers and appliances that are connected to a UNC HCS network. The inventory of connected workstations, servers and appliances must minimally include:

i. the name of the UNC HCS department or location where the workstation, server or appliance is used or is operated,

ii. the UNC HCS department, and if applicable the vendor, responsible for technical support of the workstation, server or appliance, and

iii. the operating system and version running on the workstation, server or appliance.

b. UNC HCS departments responsible for biomedical engineering or clinical engineering functions will maintain an inventory system for medical devices. The inventory must meet the Device Inventory standards in the Medical and Department Automation Device Technology and Security Standard. See section VI. B. Related UNC HCS Policies and Standards of this policy for a link to the standard.

F. Cyber Security Controls

Appropriate cyber security controls must be deployed to protect against cyber threats. Custodians of systems and networks will develop, maintain and implement standards for implementing and maintaining security controls to thwart reasonably anticipated cyber-**attacks on the systems they support**

1. **Systems Requiring Cyber Security Standards and Controls**
   a. Public (Internet) Facing Computers, Applications and Appliances
   b. End points (desktops, laptops, tablets, smartphones, medical devices, printers)
   c. Email
   d. Servers
   e. Critical Technical Services (domain controllers, DHCP services, load balancers)
   f. Network Equipment (routers, switches, firewalls, access points, etc.)
   g. Telecommunications Equipment
2. **Cyber Security Controls Required to be Addressed**
   a. Inventory
   b. Anti-virus
   c. Event logging
   d. Privileged Administrator account access controls
   e. Patch Management
   f. Advanced threat detection
3. **Additional Cyber Security Controls Required to be Addressed for Public (Internet) Facing Systems**
   a. Device hardening
   b. Two-factor authentication
4. **Response to Cyber Threats to UNC HCS IT Resources and/or Data**
   a. Containment – In order to contain a possible or actual breach the following steps may be warranted.
      i. Network Isolation – The Information Security Office may determine that shutting down parts of the network may be necessary for containment. This could include disconnecting an entire entity from the UNC HCS network if the incident stems from that location.
      ii. Server Disconnect – The Information Security Office may determine that servers need to be disconnected in order to stop the spread of malware or to protect servers from attack. This could potentially affect major UNC HCS enterprise wide systems.
      iii. Restricting access to the Internet and e-mail.
      iv. Disconnecting medical devices.
      v. Disabling all VPN connections.
   b. Eradication - When the breach is contained the Information Security Office will work to find and eliminate the root cause of the breach. This may include the following actions:
      i. Disabling user accounts or resetting passwords.
      ii. Upgrading and patching systems which may cause unplanned downtime.

iii. Re-imaging of servers, workstations and appliances.

iv. Medical devices may need verification checks performed by the vendor.

c. Recovery - Affected systems may be brought back on-line, and any disconnected departments or entities brought back on-line only after confirmation of full eradication by the Information Security Office.

G. Access Controls

The following access controls will be used to control access to UNC HCS networks, PHI, Confidential Information, and Internal Information:

1. **Identification -** Prior to being provided access to a UNC HCS network, new network Users must have an identification record and their affiliation with UNC HCS must be validated. The following information must be provided in order to properly identify and validate new network Users
   a. Name, last 4 digits of SSN (not full SSN), birth month and day but not year (mm/dd),
   b. User's manager or, in the case of third party user, UNC HCS Sponsor,
   c. Affiliation with UNC HCS (i.e. employee, contractor, credentialed provider, etc.
   d. Job title/role, and purpose for the access
2. **Authorization -** Access to a UNC HCS network, PHI or Confidential Information must be authorized by a UNC HCS manager, director or executive. Highly privileged access must include a secondary approval by the Information Owner or the system Custodian where the highly privileged access will be used. Information Owners and Custodians will develop and maintain access authorization and granting procedures that support the "need to know", the HIPAA Minimum Necessary rule and the Principle of Least Privilege. Authorization methods may include:
   a. Online approval by the appropriate authorizer
   b. Role based access whereby a role in the organization is approved for certain accesses and any User who meets the criteria of the role as determined by management, license or credentialing, is granted the accesses assigned to the role
3. **Authentication**
   a. Access to a UNC HCS network and to any application or system that provides access to Confidential or PHI requires unique user authentication.
   b. Passwords and other authentication mechanism intended to be kept secret or secure may not be shared and must be appropriately secured.
   c. Systems and applications must be configured to meet the UNC HCS standards for password strength, expiration, history, account lockout:
      i. Minimum length: 10 characters
      ii. Complexity: at least 1 upper case and 1 lower case letter, and 1 number
      iii. Expiration: 12 months
      iv. History (number of password changes that must occur before a password is re-used): Maximum permitted by the system enforcing password protections
      v. Account lockout for brute force password attack protection - Two-factor authentication largely mitigates brute force attacks on UNC HCS passwords. However, account lockout continues to protect against attacks that have gained access to a UNC HCS internal network. As such, accounts must be locked after:
         1. 10 consecutive unsuccessful login attempts, or
         2. 100 unsuccessful (non-consecutive) login attempts within a 30 minute period
      vi. Locked accounts may be:

1. unlocked by the Service Desk upon verification of the account owner, or
2. unlocked by an authorized self-service password reset platform, or
3. auto unlocked after a period of 30 minutes

d. New technologies or applications purchased or leased by UNC HCS must have the ability to integrate with UNC HCS standard authentication systems. The ISD ARB shall confirm the capability in a product before acquisition.

e. Access to the UNC HCS IT resources on the UNC HCS network requires two-factor authentication when engaged from remote locations.

f. Per Drug Enforcement Administration (DEA) regulations, electronic prescribing of narcotic drugs requires two-factor authentication.

g. Applications and single-signon systems providing access to PHI, must be configured to prompt a User for re-authentication after a certain period of inactivity as approved by the Information Security Office. Inactivity periods vary are based upon physical security afforded to the end point.

h. User's must log off an application or lock a system any time they are leaving the immediate work area of the workstation they are using.

4. **Data Integrity -** UNC HCS must be able to provide corroboration that PHI and financial information that supports any UNC HCS Financial Statement, has not been altered or destroyed in an unauthorized manner. Systems containing PHI used for treatment, payment or operations, and systems that generate financial information used in any UNC HCS Financial Statement, must contain mechanisms that prevent and detect data integrity problems.

5. **Transmission Security -** PHI and Confidential information must be protected by an encryption mechanism approved by the Information Security Office during transmission, including but not limited to::

a. Transmission between web browsers and web servers over internal or external networks

b. Transmission between client applications and servers over external networks

c. Transmission in text and instant messages

d. Transmission outside of UNC HCS via file transfer processes

e. Transmission to an external email address (external is any email address that is not @unchealth.unc.edu)

f. Transmission of an email attachment to either an internal or external email address

6. **Remote Access -** Access to a UNC HCS network and IT resources from a remote location will be granted using UNC HCS approved remote access standard solutions defined by UNC HCS ISD. Non-standard remote access methods are prohibited..

7. **Physical Access -** Physical security controls must be in places where UNC HCS electronic information is used, transmitted, processed or stored to effectively secure against reasonably anticipated unauthorized physical access or damage.

a. Workstations - Controls must be applied to workstations to guard against the following physical breaches:

i. Unauthorized viewing of PHI or confidential information on computer screens,

ii. Physical access to and use of workstations by unauthorized individuals, and

iii. Access to PHI or confidential information in the event of a computer theft.

b. Telecommunications and network equipment and appliances must be installed in secure communications closets or in a UNC HCS data center and access restricted to only authorized personnel.

c. Servers must be installed in a secure UNC HCS data center.

d. UNC HCS data centers must be secured to prevent, detect and minimize damage caused by unauthorized access, as well as weather and environmental hazards such as water, fire, excessive heat, and power fluctuations and outages. UNC HCS ISD will:

i. Regularly review and coordinate testing of the physical security controls listed in the data center physical security plan to ensure they are operating as designed.

ii. Authorize, grant, review and revoke access to the UNC HCS data centers according to documented access procedures. Access management responsibilities may require coordination with Plant/ Facilities Engineering functions at some locations.

iii. Regularly review records of access to the UNC HCS data centers.

iv. Maintain records of UNC HCS data center repairs and maintenance.

v. Ensure the UNC HCS data center emergency access procedures are followed during recovery and operations restoration if normal security controls are deprecated due to a disaster.

H. Disaster Recovery and Contingency Operations

1. **Disaster Recovery Testing** - On an annual basis, UNC HCS ISD will test the recovery of its critical applications and infrastructure to demonstrate recoverability and predictability. The results will be documented and the disaster recovery plan will be updated accordingly.
2. **Business Continuity of Electronic Medical Records**
    a. UNC HCS ISD will maintain business continuity computers in clinics and other patient care areas for contingency patient care operations in the event of a technology outage.
    b. Managers and directors of UNC HCS clinical departments must ensure they practice their patient care business continuity procedures related to EMR system downtime, including use of the business continuity computers, on an annual basis to ensure providers and staff understand how to engage contingency computers during a system outage.

I. Electronic Storage and Media Controls

1. **Data Protection -** PHI and Confidential Information must be protected by an encryption mechanism approved by the Information Security Office when stored on removable media (CDs, DVDs, zip drives, thumb drives, memory sticks, removable USB storage devices, magnetic tape, etc.) and mobile devices (i.e. laptops, smartphones, and tablets).
2. **Media Disposal -** Storage media, including removable media and hard drives of storage systems, servers, workstations, printers, copiers, and multi-function peripherals, must be securely destroyed per methods approved by the Information Security Office.
3. **Re-purposing Computers -** Re-purposing computer equipment to third parties must be authorized by UNC HCS ISD. Hard drives of UNC HCS computers that are authorized to be re-purposed to a third party must be securely wiped of UNC HCS data using methods approved by the Information Security Office, before transferring the computers.
4. **User Responsibilities:**
    a. Users may not copy and store PHI and Confidential Information on removable media without approval from the Information Security Office. The Information Security Office will assist users with an alternate and more secure solution, or will ensure the PHI and Confidential Information stored on the removable media will be properly secured.
    b. Users must return computers and peripherals to ISD when no longer in use. User's may not store, transfer or attempt to destroy unused computers and peripherals.
    c. Users must dispose of removable media as follows:
        i. Removable media containing no metals (i.e. CDs, DVDs) may be placed in secure confidential shredder bins.
        ii. Removable media containing metals (i.e. media with a USB cable or plug), must be given to ISD for secure destruction that meets Information Security Standards.

J. Data Extracts and Transfers

1. When PHI or Confidential Information is extracted from UNCHCS databases and stored in unstructured data files, they shed the security controls designed into applications and database management systems. As such, PHI and Confidential Information may only be extracted from UNC HCS databases by Users who have been trained in secure storage and handling of unstructured data files.
2. Before transferring PHI or Confidential Information, the sender of the information must ensure the recipient is authorized to have the data. In the case of third party recipients, the UNC HCS Sponsor of the third party receiving the data must also ensure appropriate contracts and agreements are in place prior to PHI or Confidential Information transfer. Contact UNC HCS Purchasing Shared Services or the Information Security Office for requirements.
3. PHI and Confidential Information must be protected by encryption when transferring to a third party.

K. Audit Controls

1. Applications containing PHI must be configured to record user activity with patient records to support pro-active patient privacy audits and privacy complaint investigations.
2. Security events in critical servers and infrastructure systems must be logged for retrospective review or incident investigations. Critical security events must be identified and, in addition to being logged, must be either actively monitored or configured to alert the system administrator or the Information Security Office.
3. Evaluation - Periodic security evaluations must be performed by the Information Security Office in response to material technical, environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

VI. References

A. Laws and Regulations

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Section 261-264, Public Law 104-191, 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.
2. North Carolina Public Records Act N.C.G.S. § 132.
3. 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.
4. 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.

B. Related UNC HCS Policies and Standards

The policies below are published on the UNC Health PolicyStat site. The Security Standards provide specifications to assist IT asset and data custodians, and users in carrying out information security policy and must be implemented where applicable and feasible. When applicable but infeasible, an exception should be registered with the UNC Health Information Security Office.

Polices	Security Standards
Bring Your Own Device Policy	AD Accounts Standard
Email Policy	Electronic Data Destruction Standard
HIPAA Privacy Policies	Incident Management Plan and Procedures
Breach Notification	Information Security Risk Assessment Standard and Process
Internet Connectivity and Use Policy	Medical and Department Automation Device Technology and Security

Polices	Security Standards
Mobile Computing Device Policy	Payment Card Security Standard
PHI and The De-identification of PHI	Perimeter Security Standard
Payment Card Security Policy	Physical Security For Protection of Electronic Information
	Privileged Administrator Access Controls Standard
	Security Event Logging Standard
	Remote and Third Party Access Standard
	Wireless Networks Security Standard
	Workstation Security Standard

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
	Tracy Parham: System Chief Info Officer	08/2021
SYSTEM Site Administrator	Emilie Hendee: HCS Attorney Sr	08/2021
	De ann Young: HCS Exec Dir Info Tech - CISO	08/2021

Applicability

Caldwell Memorial Hospital, Chatham Hospital, Johnston Health, Nash UNC Health Care, Pardee Hospital, UNC Health Care System, UNC Lenoir Health Care, UNC Medical Center, UNC Physicians Network, UNC Rex Healthcare, UNC Rockingham Health Care, Wayne Memorial Hospital