Origination: *07/2018*
Effective: *06/2020*
Last Approved: *06/2020*
Last Revised: *06/2020*
Next Review: *06/2023*
Owner: *David Behinfar: HCS Exec Dir Privacy*
Policy Area: *HIPAA - Privacy*
Policy Tag Groups:
Applicability: *UNCHCS - All except Pardee*

Physical Safeguards

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).**

I. Description

UNC Health shall impose reasonable physical safeguards to protect the privacy and security of PHI, and prevent the improper use and disclosure of PHI.

Included within the scope of this policy are the patient care programs of the UNC School of Medicine (UNC SOM). As a result, this policy shall apply to all UNC SOM personnel, including but not limited to faculty, staff, students, trainees, interns and volunteers who may be full-time, part-time, paid or unpaid who create, store, transmit, access or use any patient information in support of clinical purposes for UNC Health or any other healthcare entity.

II. Policy

Workforce members are responsible for protecting PHI with reasonable physical safeguards. It is the responsibility of all Workforce members to secure PHI that they have access to or are using to complete assigned responsibilities. Reasonable physical safeguards are to be used at all times to ensure that PHI is not

disclosed to individuals who are not authorized to receive the information and to minimize incidental disclosures of PHI.

A. **Common Physical Safeguards**. Each Workforce member is responsible to protect the physical security of the PHI he/she is using, accessing or maintaining in his/her work area, including but not limited to:

1. Ensuring that PHI is not readily visible to visitors or to the public;
2. Maintaining charts in designated secure areas and not leaving charts unattended in areas to which the public has access;
3. Locking areas in which there are medical and billing records at the end of the day or when no staff are in the area;
4. Never taking paper PHI records of any kind offsite (i.e. home) unless doing so is approved by the individual's supervisor through a documented and auditable process *See* Transportation of PHI on and Off-Site Policy;
5. Checking that all PHI is removed upon leaving conference rooms and other meeting locations and the unwanted materials are properly disposed (i.e. shredded);
6. Taking reasonable measures (i.e. lower voices, draw curtains) to provide auditory/visual privacy to individuals in areas where interviews or other conversations including PHI are being conducted and have the potential to be overheard. Examples of such situations where privacy protections should be taken when verbal PHI is shared would include:
    a. Conversations among care givers that involve patients;
    b. Using professional judgment when calling out patient names in the waiting room areas;
    c. Discussion of a patient's condition or lab tests with the patient, either in person or over the phone; and/or
    d. Discussing a patient's condition during teaching rounds within UNC Health.
7. Positioning computer screens so that the information is not visible to passersby;
8. Leaving minimal information for patients on answering machines and voice mail;
9. Locating printers and fax machines in secure areas; and
10. Retrieving and distributing faxed PHI in a timely manner.

B. **Securing Paper Records**.

1. Paper documents containing PHI that are not being used should be placed in locations:
    a. that can either be locked or that will be occupied by authorized personnel at all times; and
    b. will be in locations where there are no visitors or third parties who might be able to view access such documents. [Double locking is preferred; i.e., a lockable storage cabinet inside a lockable room.]
2. Paper documents containing PHI that are in use for treatment, payment, or health care operations purposes should be kept in the physical possession or view of an authorized workforce member at all times and should not be placed in areas available to unsupervised members of the general public when left unattended.
3. Documents containing PHI that are ready for to be destroyed/discarded should be discarded immediately upon making that determination or placed in a secure storage area for controlled

shredding/destruction later in accordance with UNC Health Disposal/Destruction of PHI Policy. Documents (or other items such as prescription pill bottles, boxes, or medical waste with stickers or printed PHI) should never be placed in open waste receptacles.

4. Computer printers and fax machines where PHI is expected to be available, printed or received should always be placed in locations that can either be locked or that will be occupied by authorized personnel at all times.

C. **Securing Electronic PHI**

1. To prevent unauthorized use or disclosure, place computers, monitors, and similar data storage and display devices in areas that limit viewing and prevent access by unauthorized persons; position electronic displays away from public view or shield the viewing screen.
2. UNC Health workforce who access PHI at home, in other non-work locations or use mobile devises such as a smartphone, are expected to use appropriate physical safeguards to prevent family members, roommates, friends and others from unauthorized viewing of or accessing any PHI. *See* Transportation of PHI on and Off-Site and the UNC Health Telecommuting Policy.
3. Encrypt all PHI stored on removable electronic storage media (cards, CD's, flash devices, etc.).
4. When no longer needed, physically destroy removable electronic storage media (discs, tapes, CD's, flash devices, etc.) that have been used for storing PHI or place in a locked storage unit for secure controlled destruction later. *See* UNC Health Disposal/Destruction of PHI Policy.
5. Electronically purge data devices used to store PHI before they are discarded or otherwise placed out-of-use.

III. Definitions

Physical Safeguards - are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. [45 CFR 164.304.]

IV. References

45 C.F.R. § 164.310; 45 CFR 164.304

V. Related Policies/Forms

Disposal/Destruction of PHI

Transportation of PHI on and Off-Site

Telecommuting

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
	Jerylyn Williams: Chief Audit & Compliance Ofcr	06/2020
SYSTEM Site Administrator	Emilie Hendee: HCS Attorney Sr	06/2020
	David Behinfar: HCS Exec Dir Privacy	06/2020

Applicability

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