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*

Administrative, Physical and Technical 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 administrative safeguards to protect the privacy and security of PHI and prevent 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

A. **General Privacy Safeguards**.

1. **Securing PHI**. All Protected Health Information (PHI) and other restricted data, created, received, maintained, and transmitted by UNC Health in all formats, must be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, tampering, and fraudulent use.
2. **Computer Surveillance**: UNC Health has the capability to track and log access and activities in much of its information and computing environment. All user activity on UNC Health information and computing environments, including, but not limited to, access through personal computing devices, is subject to review.
3. **Role-based Access**. Access to electronic PHI is defined by levels based on users' roles and responsibilities. Access to PHI is limited to personnel who have a need to access such information to perform a function or activity required by their job. Personnel when accessing and using PHI for non-treatment related purposes shall limit their use and disclosure of PHI in accordance with the UNC Health Minimum Necessary Policy.
4. **Workforce**: UNC Health and UNC School of Medicine departments, and clinics must define and justify levels of access to PHI for their workforce members relative to their assigned duties and professional "Need to Know".

B. **Reasonable Safeguards**. Conversations regarding PHI, whether in-person or over the telephone, should be held in locations to avoid being overheard by others, to the extent reasonably possible. See UNC Health Physical Safeguards Policy for physical safeguards which may be considered.

C. **Security Policies**. See UNC Health Information Security Policies for additional details and information for appropriate administrative and technical safeguards.

III. Definitions

Access – for electronic PHI purposes only) means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource.

Administrative safeguards – administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication – the corroboration that a person is the one claimed.

Availability – the property that data or information is accessible and useable upon demand by an authorized person.

Information system – an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity – the property that data or information have not been altered or destroyed in an unauthorized manner.

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.]

Technical safeguards – the technology and the policy and procedures for its use that protect electronic PHI

and control access to it.

IV. References

45 C.F.R. §§ 164.308, 164.530(c)

V. Related Policies/Forms

UNC Health Minimum Necessary Policy

UNC Health Physical Safeguards Policy

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