Current Status: *Active* **PolicyStat ID:** *7944415*

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 Johnston and Pardee*

Electronic Patient Information Access and Auditing of Access

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

It is the responsibility of UNC Health to ensure that UNC Health employees and others who have authorized access to UNC Health electronic systems containing patient medical information access only the patient medical information necessary to perform their job functions. UNC Health shall have the right to audit accesses into any electronic system, application, database, electronic health record system and any other UNC Health system or application containing patient medical records in electronic format. This policy outlines appropriate behaviors and expectations for access to electronic patient information contained in any UNC Health electronic system.

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. **Protecting Electronic Patient Information**.
Protecting the privacy of patient information is an important consideration for everyone who utilizes the UNC Health electronic systems containing patient information. This policy applies to any individual that is granted electronic access (including remote access) to UNC Health information systems and Electronic Health Record (EHR). UNC Health has a legal and ethical obligation to ensure the confidentiality and security of patient information and individuals granted access to patient information are personally responsible for ensuring that the privacy of our patients is always protected.

B. **Individual Responsibilities to Protect Patient Privacy When Accessing Patient Information in Electronic Systems**.

1. The medical record is the property of UNC Health and is maintained for the benefit of the patient, the Medical Staff, the individual UNC Health Hospital and UNC Health. The information contained within the record, including all forms of electronic patient information, is the property of the patient and cannot be released to individuals not otherwise authorized without the written consent of the patient, a subpoena, court order or pursuant to state or federal law.
2. Only authorized users with a 'Business Need to Know' should access patient records.
3. UNC Health workforce who have been granted access to systems containing UNC Health patient information shall safeguard and are prohibited from disclosing their personal access code or any other access credentials that would permit access by unauthorized individuals to confidential patient information, (e.g., never share personal access codes, passwords or devices with any other person; or allow anyone else to access or alter confidential patient information under their identity).
4. UNC Health workforce who have been granted access to systems containing UNC Health patient information shall accept personal responsibility for all activities undertaken using their assigned access codes / user names and passwords or devices and shall be responsible for any misuse or unauthorized disclosure of confidential patient information made using their assigned access codes / user names and passwords and for the failure to safeguard their assigned access codes / user names and passwords or devices.

C. **Right to Perform Access Audits of UNC Health Electronic Systems**:

1. UNC Health recognizes that auditing is an essential function of safeguarding confidential patient data from inappropriate access or use.
2. Through the use of system tools and technical functionality UNC Health has the right, without prior notice, to conduct audits of any electronic system, including the electronic health record (EHR), database, file folder or application to ensure that any access of patient information was performed in accordance with the appropriate Business Need–to-Know.
3. The UNC Health Privacy Office (and individual Facility Privacy Officers at UNC Health Managed Facilities) shall be responsible for performing access audits of electronic systems containing patient medical information.

D. **Sanctions for Violations.**
Individuals who have been determined to have accessed patient information without an appropriate Business Need to Know shall be subject to discipline in accordance with the UNC Health Sanctions for Violations of Privacy Policies.

III. Definitions

Electronic Health Record – means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Record – any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for UNC Health.

Business Need to Know - Information needed to provide and/or support:

1. patient care treatment activities required by that individual's job or duties;
2. the performance of health care operational activities, as defined by an individual's assigned job duties or at the instruction of an authorized supervisor or other official within UNC Health. Health care operational activities include by way of example, activities in support of compliance, accreditation, licensing, certification and all other administrative activities;
3. the performance of approved educational activities in support of the education of medical residents, students or others or such other professional educational activities in support of UNC Health or the UNC School of Medicine formal educational programs.

IV. References

45 C.F.R. §§ 164.514(h)(1)

V. Related Policies/Forms

UNC Health Sanctions for Violations of Privacy Policies

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, 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