Current Status: *Active* **PolicyStat ID:** *7944573*

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*

Sanctions for Violations of Privacy Policies

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 will apply appropriate sanctions against members of its workforce who fail to comply with its privacy and security policies and procedures. Sanctions may vary based on the facts and circumstances of the violation.

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. **Sanctions and Disciplinary Actions*:***

1. **Sanctions applicable to UNC Health workforce**.
    a. **UNC Health Member Facilities Workforce**. Employees who have violated UNC Health privacy policies as substantiated in the sole discretion of the UNC Health Privacy Office (or corresponding Privacy Office of the UNC Health Member Facility) will have the violation documented in the workforce member's personnel file.
    b. **UNC School of Medicine Workforce**. Employees of the UNC School of Medicine, including but not limited to faculty, staff and other individuals affiliated with the UNC School of Medicine ("SOM Personnel") who are found to have violated UNC Health privacy policies as substantiated in the sole discretion of the UNC Health Privacy Office shall be referred to the UNC School of Medicine Human Resources Department for the provision of discipline in accordance with UNC School of Medicine policies.
        i. The UNC Health Privacy Office determination on the appropriate Level of discipline according to the UNC Health Discipline Matrix shall be shared with the UNC SOM Human Resources Department for violations of UNC Health privacy policies committed by SOM Personnel. The UNC SOM Human Resources Department and such other University Offices involved in the disciplinary decision-making process (such as the University's HIPAA Officer) shall take into account the UNC Health determination on the appropriate level of discipline as determined by the UNC Health Privacy Office. The ultimate determination on discipline of any SOM Personnel shall be made by the UNC School of Medicine.
        ii. UNC Health may however take such additional steps it believes necessary to protect its electronic systems containing PHI which may result in the decision to terminate or suspend system access credentials of SOM Personnel to any paper and electronic systems of UNC Health containing PHI. In addition to any of the disciplinary actions mentioned above, any instance of faculty non-compliance may also be referred to the appropriate Hospital staff discipline committee (or similar).
2. **Determining Discipline for UNC Health Privacy Policy Violations**
    a. **Determining the Level of Discipline**. The UNC Health Privacy Office (or the Facility Privacy Officer as the case may be) shall determine the level of discipline for any violation of UNC Health Privacy Policies of UNC Health personnel employed by "owned facilities" in accordance with the Sanctions Matrix set forth in Schedule A to this policy. The UNC Health Privacy Office shall be solely responsible for the determination of the Level of any substantiated violation (Level 1, 2 or 3).
        i. **UNC Health Managed Facilities**: UNC Health Managed facilities shall independently determine whether and to what extent they rely on the Sanctions Matrix and which departments and/or offices is/are responsible for determining the level of any violation.
    b. **Sharing Discipline Determination with HR**. The determination of the appropriate level for discipline will be shared with the UNC Health Department of Human Resources (or the facility's Department of Human Resources at the UNC Health Member Facility where the employee works or the UNC School of Medicine as appropriate) for the final determination on appropriate discipline.
        i. **Flexibility in Discipline**. The discipline offered for each level of a violation is meant to be a floor. As a result, UNC Health Facilities shall have the option to impose greater discipline (but not lesser) than what is recommended in any particular Sanctions Matrix level as a

result of other factors it may wish to consider.

c. **Additional Guidance**. The UNC Health Privacy Office may provide additional guidance on discipline as requested.

3. **UNC Health Privacy Office Consultation for Level 2 and 3 Violations**. It is recommended and encouraged (but not required) that incidents investigated by Facility Privacy Officers at UNC Health Member Facilities that are determined by the facility Privacy Officer to constitute a Level 3 violation be referred to the UNC Health Privacy Office for a consultative review prior to the conclusion of the investigation and prior to the determination of any disciplinary action.

III. Definitions

Workforce – means employees, including temporary agency or contract employees, health care professionals, including faculty, medical students and interns, volunteers, trainees, and other persons whose conduct, in the performance of work for UNC Health is under the direct control of UNC Health, whether or not they are paid by UNC Health.

IV. References

45 C.F.R. §§ 164.314(a)(3), 164.502(e)(1), 164.504(e)

V. Related Policies/Forms

UNC Health Sanctions Matrix (*see attached*)

Attachments

Schedule A - Recommended Sanctions for Violations of UNC Health Privacy Policies by UNC Health Workforce - Including UNC Health Staff and UNC School of Medicine Faculty and Staff

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

SANCTIONS MATRIX:
Recommended Sanctions for Violations of UNC Health Privacy Policies by UNC Health Workforce - Including UNC Health Staff and UNC School of Medicine Faculty and Staff

Key Considerations

- The UNC Health Privacy Office (or UNC Health Member Facility Privacy Office) shall be responsible for determining the Level of Violation for all reported incidents determined by the Privacy Office to constitute violations of the UNC Health HIPAA Privacy Policies.
- This matrix is meant to provide interpretive guidance for illustration purposes. The facts and circumstances of each individual incident are unique in each case. In making a determination of the Level of Violation in which an incident is classified, the UNC Health Privacy Office (or privacy office of the applicable UNC Health facility) shall consider the individual facts and circumstances associated with each incident.

Level of Violation (*as solely determined by the Privacy Office*)	**Cause or Motivation**	**Type of Violation**	**Examples of Violations** (will be dependent on individual facts and circumstances)	**Recommended List of Optional Sanctions** (*may choose one or more options within a Level*)
Level I Mistakes or errors in handling PHI, or in maintaining workstation or physical surroundings or failing to take appropriate measures to secure PHI	*Unintentional AND non-malicious AND resulting harm is low* _____ • Lack of training • Inexperience • Poor judgment • Inattention to detail • Performing job functions while distracted • Poor implementation of process or policy compliance	• Clerical Error • Process Error • Technical Error • Judgment Error	• Failure to complete required Privacy Training by deadline • Leaving an active computer screen with access to non-sensitive PHI unattended • Leaving non-sensitive PHI, in any format, unattended in public areas • Disclosing non-sensitive PHI to third party without performing identity verification • Sending non-sensitive PHI via e-mail, fax or mail to wrong person (ex. email auto-populates with wrong name) • Placing non-shredded documents containing non-sensitive PHI in inappropriate waste receptacles	• Retraining • Specialized training • Consultation with Supervisor and/or Privacy Office • Discussion of policy and procedures with supervisor and/or Privacy Office • Verbal counseling/ warning or reprimand (or equivalent) • Written letter of reprimand (or equivalent)

Level II Breach of the UNC Health or UNC Health Member Facility's Confidentiality Statement and/or UNC Health policies concerning access to, the use of and/or disclosure of PHI	*Intentional* *OR* *negligent* *AND* *non-malicious* *AND* *resulting harm is moderate or greater* _____ • Curiosity • Concern • Compassion • Carelessness • Negligence • Compulsiveness	• Un-authorized • Non-job-related • Poor Judgment	• Failure to complete required Privacy Training after deadline and after repeated requests • Discussing PHI in public or other inappropriate areas • Accessing the record of any person, including co-workers, friends, or family, without professional Need-to-Know (that is *determined by Privacy Office to be*: "Low-risk Snooping") • Leaving PHI (which may include sensitive PHI), in any format, unattended in public areas • Sending PHI (which may include sensitive PHI) via e-mail, fax or mail to wrong person • Sharing passwords • Copying/accessing PHI for someone else who is not authorized to access that PHI • Installing (knowingly or unknowingly) unauthorized software or application with potential to harm UNC Health patient care systems • Adding, deleting, or altering electronic information in medical record systems	• Written Letter of Reprimand (or equivalent), requiring written corrective action in response; • ineligible for bonus, transfer or promotion for specified time period (*if available as disciplinary measure*) (ex. 1-6 months) • Suspension of access to patient care systems and/or privileges/access to other information systems containing PHI • Suspension of employment 1-5 days (*if available*) • Subject to reoccurring UNC Health electronic medical record system user access audit verification

Level III Breach of the UNC Health or UNC Health Member Facility's Confidentiality Statement and/or UNC Health policies concerning access to, the use of and/or disclosure of PHI or sensitive PHI for personal gain or to affect harm on another person or acting with disregard to any harm that may result from actions	*Malicious Intent* *OR* *Acts committed were reckless or committed with gross negligence (employee acted with complete disregard to known serious negative consequences of actions)* *AND* *harm caused was significant* _____ • Financial gain • Revenge • Protest • Deceit • Stealth • Poor decision made without consideration of serious negative consequences that would have been apparent to any reasonable employee	• Theft, including identity theft • Malicious actions: i.e., · alteration or deletion of data · making data or systems inaccessible · intent to cause personal or emotional harm • Acting with complete disregard to consequences of actions that may result in a breach of privacy of patient information	• Accessing the record of any person, including co- workers, friends or family, without professional Need- to-Know (that is *determined by Privacy Office to be*: "High-risk Snooping") • Access to and/or unauthorized disclosure of PHI for personal or financial gain or to affect harm on another person • Unauthorized access of PHI of: ○ celebrity ○ national, local, community or other public figure (i.e., police chief) ○ professional or collegiate athlete or coach ○ person reported in news (i.e., accident victim, person charged with crime) ○ VIP • Leaving PHI (which may include sensitive PHI), in any format, unattended in public • Using someone else's computer access credentials to access PHI • Sending PHI (which may include sensitive PHI) via e-mail, fax or mail to wrong person • Malicious alteration, deletion or unauthorized removal of PHI from UNC Health facilities • Unauthorized disclosure, publication, web posting, texting, posting on social media or broadcasting PHI in any medium with personal non-business intent. • Repeated Level I or II violations	• Final written warning (or equivalent) • Ineligible for bonus, transfer or promotion for up to 12 months (if applicable) • Termination or suspension of electronic medical record and/or other information system user privileges • Revocation or suspension of UNC Health Care or facility hospital medical staff privileges • Termination of employment and ineligible for rehire

NOTE: Access of any patient record by an employee (or other individual with access credentials to PHI) to a patient's records with whom they have a relationship (such as family, friends, co-worker, neighbor) or any celebrity, public figure, athlete, etc. . . where such access is determined to be without a professional/business need-to-know will be presumed as "High-risk Snooping" and will be considered a Level III violation by the UNC Health Privacy Office unless additional circumstances or facts indicate that a "Low-risk Snooping" designation (Level II violation) is appropriate.

Examples of additional circumstances that might indicate a "Low-risk Snooping" designation is appropriate include evidence that suggests that the affected patient either approved of the access or would have approved of access or the employee's (or other individual with access credentials to access PHI) intention in accessing the record was for the sole benefit of the patient or at the direction of and wishes of the patient.