THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Issuing Office(s):
Information Technology Services – Institutional Privacy Office
Responsible University Officer(s):
Chief Privacy Officer

UNIVERSITY STANDARD

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL STANDARD ON HIPAA SANCTIONS

Introduction

PURPOSE

The University of North Carolina at Chapel Hill (The "University" or "UNC-Chapel Hill") has a responsibility to protect the privacy and security of protected health information ("PHI") that it creates, receives, accesses, maintains, uses or transmits. Inappropriate access, use, or disclosure of PHI may cause substantial harm to individuals whose information is used or disclosed, and may cause financial and reputational injury to the University. To protect against such harms and in furtherance of its legal and regulatory obligations, the University is deeply committed to protecting PHI.

Under applicable University Policy, potential privacy violations involving PHI trigger investigation and, where such investigation demonstrates that an individual covered by this Standard violated the University's Policies governing the protection of PHI, the University will take appropriate corrective action. This Standard provides guidance and a framework for such corrective action, which may include discipline for those who improperly access, use, or disclose PHI.

This Standard maps violation levels to applicable discipline structures for University Constituent groups. The intent of this Standard is to provide consistency between Constituent groups for violations of similar severity for management of HIPAA violations.

SCOPE OF APPLICABILITY

This Standard is applicable to all UNC-Chapel Hill faculty, staff, students and other University Constituents with access to UNC Chapel Hill PHI, UNC Healthcare System ("UNCHCS") PHI, or the PHI of any other entity to which they have access stemming from their affiliation with UNC-Chapel Hill.

Standard

In accordance with the UNC-Chapel Hill Privacy of Protected Health Information Policy and related security policies, the University will appropriately sanction Constituents who have access to PHI as a result of their affiliation with UNC-Chapel Hill who fail to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended, applicable HIPAA regulations, and/or the University's privacy or security Policies, Standards and Procedures, or otherwise fail to protect the confidentiality and security of PHI (commit a violation).

Upon receiving notification of a possible HIPAA violation involving a University Constituent, the Chief Privacy Officer (CPO), a Privacy Liaison, or other designate(s) will conduct a confidential investigation of the alleged violation. If the report is received from the HIPAA Privacy Officer of UNCHCS, or of another Covered Entity, and the Chief Privacy Officer deems the information provided to be sufficient, the Chief Privacy Officer may rely upon the report rather than performing an independent investigation.

If the Chief Privacy Officer determines that a violation has occurred, they will document that determination in writing and will recommend sanctions according to this Standard. Disciplinary recommendations and referral to the appropriate governing authority will be made by the CPO, in consultation with other administrative units. This recommendation will be made to the appropriate University authority based upon the affiliation type of the Constituent (faculty, staff, student, or other). If the Constituent has more than one affiliation type, the Privacy Officer will make a determination of the most appropriate course(s) based on the circumstances of the violation and the affiliation that gave rise to the Constituent's access to the relevant PHI.

Violation levels

Sanctions will be recommended based on the severity of the violation. Determination of severity is based upon whether the violation was intentional or unintentional, and other mitigating or aggravating factors.

Mitigating or aggravating factors below may influence both determination of the violation level and sanctions recommendations:

1. Whether the violation indicated a pattern or practice of improper use or disclosure;
2. Whether the violation was reported by the Constituent (the University has a vested interest in encouraging reports of possible breach, and sanctions applied should reflect that self-reporting);
3. Whether that reporting was prior or subsequent to discovery of the violation by others;
4. Whether the Constituent cooperated with the investigation and related processes;
5. Multiple HIPAA violations occurring in concert;
6. Multiple HIPAA violations in the same instance/occurrence;
7. Bad faith, egregiousness, or maliciousness (not otherwise encompassed by "severity" or "intent" generally);
8. Any non-employee's role in the violation;
9. Any disclosure to an outside entity, (which may include non-HIPAA-covered units or non-HIPAA-trained individuals within the University)
10. Damage to the University and/or its reputation;
11. Employee's use or misuse of institution's computing resources;
12. Degree of confidentiality, integrity, and/or availability of systems or data impacted;
13. Degree to which systems, network, or data was at risk subsequent to and as a result of the violation;
14. Number of patients or other individuals affected;
15. Degree to which patients or other individuals were harmed or likely harmed;
16. Individual's training and/or retraining regarding HIPAA requirements;
17. Individual's past related violations and/or discipline, if any;
18. Individual's prior record regarding HIPAA compliance;
19. Individual's reasonable belief that he/she was acting in compliance;
20. Individual's acceptance of personal responsibility and acknowledgement of wrongdoing;
21. Individual's understanding of how to avoid future violation(s);
22. A Student's program (health or non-health, undergraduate, graduate, or professional) expectations as they relate to professionalism, competence, experience, and understanding of their HIPAA-compliance responsibilities;
23. Other relevant factors specific to the situation.

The following violation levels describe some, but not all, types of violations that may occur:

Level 1: Failure to demonstrate appropriate care and safeguards in handling PHI. These types of violations are usually unintentional with no improper exposure of the information. Level 1 may be an appropriate determination for violations which would otherwise be Level 2 violations but for mitigating factors. Examples of Level 1 violations may include failing to log-off of a system, leaving PHI unattended in a low-traffic area, failing to adhere to guidelines for remote access to information systems containing PHI, or other minor first-time violations.

Level 2: Exposure of PHI within the organization regardless of intent, unauthorized intentional access to PHI, or repeated Level 1 violations. Level 2 may be an appropriate determination for violations which would otherwise be Level 3 violations but for mitigating factors. These violations result in no further improper exposure outside appropriate University units with responsibility for that information. Examples of Level 2 violations may include sharing ID/passwords with other staff (within the University unit with responsibility for that information) that results in internal inappropriate access, accessing or using PHI which the individual has no legitimate job-related reason to access or is unnecessary as part of assigned duties.

Level 3: Disclosure of PHI outside of the organization (University unit with responsibility for that information) regardless of intent, or repeated Level 2 violations. Level 3 may be an appropriate determination for violations which would otherwise be Level 4 violations but for mitigating factors. Examples of Level 3 violations may include providing passwords to unauthorized individuals that result in a disclosure outside of appropriate University units with responsibility for that information, sharing of PHI with unauthorized individuals, or failing to perform the necessary responsible actions that would prevent disclosure of PHI outside of the organization.

Level 4: Intentional Abuse of PHI. Examples of Level 4 violations may include large-scale disclosures of PHI, using PHI for personal gain, or altering, tampering with, or improperly destroying PHI.

Recommended Sanctions

The University shall interpret this Standard and the recommended sanctions below consistently with then-current, other policies and processes governing the University Constituent who committed the violation.

The Chief Privacy Officer will provide a written recommendation to the University administrator or operating unit with authority to consider and, where appropriate, to implement the recommended sanction. Recommended sanctions may reflect mitigating and/or aggravating factors listed above. Any implemented sanction that does not result in dismissal/removal of the Constituent will include a counseling session describing required corrective actions.

The recommended sanctions should serve as a minimum standard. Other individual circumstances unrelated to violations under this Standard (e.g., prior unrelated discipline, other unrelated aggravating factors) may result in a determination by the operating unit with oversight authority for the Constituent (e.g., the Office of Human Resources, Provost, Honor Court) in consultation with the Chief Privacy Officer, to impose greater sanctions than those recommended.

1. **Staff (SHRA Employees):**

   The Chief Privacy Officer, in consultation with UNC Employee & Management Relations (E&MR) regarding then-applicable SHRA discipline policies, should detail in their report the substantive basis for the recommended sanctions in accordance with the Disciplinary Action & Related Separations Policy (SHRA). Depending on the particular circumstances, the Chief Privacy Officer should specify the type of just cause (e.g., Unsatisfactory Job Performance, Unacceptable Personal Conduct, etc.) for disciplinary action under that Policy.

   Note: breach investigation and notification has a serious financial impact upon the University, and the resulting reputational damage affects funding, often very substantially. Regulatory penalties for PHI breach can be extreme. The Chief Privacy Officer shall take such impact into consideration when recommending sanctions in alignment with the SHRA Policy.

Level 1 Violation: Documented performance counseling.

Level 2 Violation: Documented performance counseling or written warning, in accordance with the Disciplinary Action and Related Separations Policy (SHRA).

If the exposure of PHI is the result of a minor lapse or oversight by the employee (e.g. keyboard error); and does not involve a large quantity of PHI or present a significant level of risk to the patient (as determined by the Chief Privacy Officer) then a documented performance counseling session alone is a sufficient penalty for the violation. This counseling session should include at minimum: a full review of the incident; the employee's role; discussions regarding potential mitigation; and the identification of appropriate preventative actions. If a written warning is selected as the appropriate remedy, the manager responsible for the warning will work with the E&MR consultant or follow other E&MR required processes to draft and issue the written warning. Once delivered, the Institutional Privacy Office should be notified. The option of a documented counseling session should not be used when the employee has committed the same offense more than once unless other mitigating factors apply.

Level 3 Violations: Documented performance counseling or written warning or other disciplinary action up to and including dismissal, in accordance with the Disciplinary Action and Related Separations Policy (SHRA).

If the disclosure of PHI is the result of a minor lapse or oversight by the employee (e.g. keyboard error) resulting in release of information external to the University unit responsible for that information; but does not involve a large quantity of PHI or present a significant level of risk to the patient (as determined by the Chief Privacy Officer) then a performance counseling session may be a sufficient penalty for the violation. This coaching/education session shall include at minimum: a full review of the incident; the employee's role; discussions regarding potential mitigation; and the identification of appropriate preventative actions. If a written warning or greater progressive discipline is selected as the appropriate remedy, the manager responsible for such session will work with the E&MR consultant or follow other E&MR required processes to draft and issue the written warning or to take other progressive discipline

action. Once delivered/completed, the Institutional Privacy Office should be notified. The option of a counseling session should not be used when the employee has committed the same offense more than once unless other mitigating factors apply.

Level 4 Violations: Pre-Dismissal Conference (PDC) should be held to evaluate the options of: written warning, suspension, demotion, and termination. The Privacy Officer's report shall include information regarding comparable sanction levels for other University Constituent groups under this Standard in order to support a consistent result across Constituent group populations. If the decision is made to terminate, that can be done under the Disciplinary Action and Related Separations Policy (SHRA). If the employee is not dismissed, appropriate measures shall be taken to prevent the employee from accessing or using PHI as a function of their role at the University.

2. **University Faculty and Employees Exempt from Human Resources Act (EHRA):**

   The Chief Privacy Officer should detail in their report to UNC Human Resources and the Provost the substantive basis for any recommended sanctions. Sanctions recommended shall be in accordance with University policies and procedures for EHRA Non-Faculty Research Staff, Instructional Staff, and Tier II Senior Academic and Administrative Officers of the University of North Carolina at Chapel Hill, the EHRA Non-Faculty Tier I Senior Academic and Administrative Officer Employees of the University of North Carolina at Chapel Hill, or the Faculty Policies, Procedures, and Guidelines.

Level 1 Violations: Documented performance counseling and verbal reprimand.

Level 2 Violations: Documented performance counseling and written reprimand.

Level 3 Violations: Documented performance counseling and written reprimand or other disciplinary actions up to and including dismissal.

Level 4 Violations: Discharge or the highest alternative sanctions applicable under policies governing EHRA employees. If the employee is not discharged, appropriate measures shall be taken to prevent the employee from accessing or using PHI as a function of their role at the University.

3. University Students:

Actions constituting a HIPAA violation would be a failure of a student's responsibilities under the Instrument of Student Judicial governance.

The Chief Privacy Officer should detail in their report the possible Honor Code violations involved in the Constituent's actions. Depending on the particular circumstances, such Honor Code violations may include but are not limited to:

a. Conduct affecting property (information assets of the University) including
    i. Stealing, destroying, damaging or misusing property belonging to the University or another individual or entity
    ii. Violating University policies regarding use or management of resources including but not limited to electronic resources
    iii. Forging, falsifying, or misusing documents, records, data, or other resources created, maintained, or used by the University
    iv. Trespassing or unauthorized intrusion into electronic records owned or managed by the University or an affiliated organization
b. Assisting or aiding another to engage in acts prohibited by the Instrument of Student Judicial Governance
c. Conduct affecting the integrity of the University including
    i. Knowingly abusing a position of trust or responsibility within the University community
    ii. Knowingly violating officially adopted University policies designed to protect the integrity and welfare of the University and members of the campus community
    iii. Deliberately furnishing false or misleading information to University personnel acting in the exercise of their official duties

Based upon the level of the HIPAA violation, the Chief Privacy Officer's report should recommend appropriate sanctions, consistent with the Instrument of

Student Judicial Governance and subject to determination by the Honor System or specific professional school authority as appropriate. Recommended sanctions are intended to serve as a minimum standard.

Level 1 Violations: Referral to the Office of Student Conduct or to specific professional school authority as appropriate. Recommended sanctions include behavior management or other requirements which may include completion of projects, programs, or requirements designed to help the student manage behavior and understand why it was inappropriate, or otherwise remedy the effects of misconduct such as documented counseling by the appropriate department faculty representative. Loss of use of University facilities or resources including those relating to information technology or computers; and/or failing grades in associated courses or additional education assignments.

Level 2 Violations: Referral to the Office of Student Conduct or to specific professional school authority as appropriate. Recommended Sanctions may include those for Level 1 violations as well as documented counseling by the appropriate Vice Chancellor, Dean, or Director, written warning; and or disciplinary probation. Other academic requirements or conditions designed to assure that academic misconduct is remedied and does not recur in the future.

Level 3 Violations: Referral to the Office of Student Conduct or to specific professional school authority as appropriate. Recommended Sanctions may include those for Level 2 violations as well as failing grade, termination of the affected student's enrollment in the academic program, suspension for a definite or indefinite period, permanent suspension, or expulsion.

Level 4 Violations: Referral to the Office of Student Conduct or to specific professional school authority as appropriate. Recommended Sanctions may include permanent suspension or expulsion.

4. **Other individuals having access to PHI stemming from their affiliation with UNC-Chapel Hill (which may include UNC Contractors, retirees, temporary employees, non-UNC Employees, visiting Researchers or Scholars, and other UNC Visitors/Volunteers):**

The UNC Chief Privacy Officer will determine the most appropriate course of action based upon the circumstances and the individual's affiliation with the University. In this vein, the Chief Privacy Officer will provide a detailed report with recommended sanctions to the department or operating unit with responsibility for the individual who committed the violation. If the individual is also associated with another organization (e.g., another university, UNCHCS, a contractor, a vendor, another healthcare organization) then a report should also be provided to the HIPAA Privacy Officer of that organization (if any) or to another administrator in that organization with authority over that individual.

Depending on the particular circumstances involved and the nature of the individual's relationship with the University, recommended sanctions made may be directed to the University operating unit, or may be informative to the individual's outside organization. The report may provide context, including comparable sanctions that would be applied to a University student or employee in the same circumstances.

Sanctions recommended in the report may include any sanctions listed above as they might be applicable to the individual. In addition, termination of contracts with the University, termination of temporary employment, curtailment of Onyen access or other access to systems or data, or termination of affiliation with the University, or comparable measures may also be recommended. The Chief Privacy Officer will consult with the operating unit and appropriate administrative units as needed to determine what sanctions are feasible and to provide recommended sanctions that are consistent in severity across groups of Constituents.

Report Content

The Chief Privacy Officer will include in their report sufficient information and context to allow the appropriate authorities to determine an appropriate set of sanctions. Without incurring more exposure of PHI and where disclosure of such information is otherwise permissible, the report may include some or all of the following: details of the alleged violation, steps taken to investigate the allegation, a summary of interviews conducted, a discussion of evidence relevant to the allegation, an analysis of applicable laws and University policies, a determination regarding the alleged violation, a description of risk or impact to the University and to individuals whose PHI may have been compromised, and recommended

sanctions. This detail allows the appropriate supervisory authorities or other administrative units to implement sanctions consistently and to understand the risk or impact on the University of the individual's conduct.

ROLES AND RESPONSIBLITIES

Chief Privacy Officer: The individual responsible for

1. Investigation of reported violations of University HIPAA policies or applicable privacy and security laws by any University Constituent, regardless of the location of the violation; provided however, that the Chief Privacy Officer may rely on the investigative effort of the UNCHCS Privacy Office, or another entity's HIPAA Privacy Officer in the case of reported violations involving a University Constituent and PHI of UNCHCS or another entity.
2. The determination of severity level of the violation, and for provision of detailed reports including recommended sanctions to the authorities responsible for each University Constituent type; and
3. Recommendation of sanctions in a consistent manner based on the severity of violation and this Standard, to assist the University in applying sanctions consistently across schools, departments, and Constituent types.

Constituent Oversight Authorities: Responsibility for receiving and acting on reports under this Standard from the Chief Privacy Officer. Application of University procedures related to the discipline of faculty, staff, students, or other Constituents in a consistent and appropriate manner. Authorities should follow sanctions guidance recommended by the Chief Privacy Officer as a method of providing predictability, consistency, and fairness across the University in the application of sanctions to Constituents.

EXCEPTIONS

UNC-Chapel Hill will not apply sanctions against University Constituents (or recommend sanctions against other individuals) in connection with good faith disclosures of unlawful conduct or reporting to law enforcement as victim of a crime, as long as such disclosures meet the requirements of 45 CFR section 164.502(j).

Disclosures by Whistleblowers

If the Chief Privacy Officer determines that:

1. The individual believes in good faith that the University has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by UNC potentially endangers one or more patients, workers, or the public; *and*

   The disclosure is to:

2. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the University or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct; or an attorney retained by or on behalf of the individual for the purpose of determining the legal options of the individual.

   Then the Chief Privacy Officer shall make an appropriate exception to the sanctions that would otherwise be recommended.

Disclosures by Constituents who are Victims of a Crime

If the Chief Privacy Officer determines that:

The PHI disclosed is about the suspected perpetrator of the criminal act; *and*

The PHI disclosed is limited to the purpose of identifying or locating a suspected perpetrator and includes only:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and

h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Then the Chief Privacy Officer shall make an appropriate exception to the sanctions that would otherwise be recommended.

Definitions

University Constituent: UNC-Chapel Hill faculty, staff, students, retirees, contractors, distance learners, visiting scholars and others who require UNC-Chapel Hill resources to work in conjunction with UNC-Chapel Hill.

Disclosure: Disclosure means the release, transfer, provision of access to, or divulging in any manner of PHI to individuals outside of appropriate University offices who do not have a lawful right to receive that information.

Protected Health Information: Individually identifiable information that is a subset of health information, including demographic information collected from an individual, and:

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of a subject; the provision of health care to a subject; or the past, present, or future payment for the provision of health care to a subject; and

a. That identifies the subject; or
b. With respect to which there is reasonable basis to believe the information can be used to identify the individual.

PHI can be:

a. Transmitted by electronic media;
b. Maintained in electronic media; or
c. Transmitted or maintained in any other form or medium.

PHI excludes individually identifiable information that is:

a. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20. U.S.C. 1232g;
b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
c. In employment records held by a covered entity in its role as employer; and
d. Regarding a person who has been deceased for more than 50 years.

Use: Use means the access, exposure, release, transfer, provision of access to, or divulging in any manner of PHI.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

45 CFR 164 Subpart E: Privacy of Individually Identifiable Health Information

"Modification to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," 78 Federal Register 17 (25 January 2013), pp. 5566-5702.

UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES

Employee Policies

Faculty governance

Student Conduct

Privacy of Protected Health Information Policy

Contact Information

PRIMARY CONTACT(S)

Policy	ITS Policy Office	919-962-HELP	Its_policy@unc.edu

OTHER CONTACTS

Institutional Privacy Office: privacy@unc.edu, privacy.unc.edu, 919-962-HELP

Important Dates

- Effective Date and title of Approver: September 6, 2017, Chief Privacy Officer
- Revision and Review Dates, Change notes, title of Reviewer or Approver: N/A

Approved by:

/S/

Micki Jernigan
Chief Privacy Officer

Date: September 6, 2017