HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Approved by: Office of Clinical and Field Education

History: Effective 9/19/2012 | Reviewed 2/2012, 2013, 2014 and 2015 | Revised: 1-20-16; 2-24-16 | Final: 04/2016 | Revised: 8/2020, 12/2021 and 5/2022

Related Policies, Forms, Procedures and References: Eastern Carolina University HIPAA Sanctions policy 2013; http://www.hhs.gov/hipaa/index.html (http://www.hhs.gov/hipaa/); http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html; http://www.apapracticecentral.org/update/2013/03-14/final-rule.aspx

For Questions Contact: Office of Clinical and Field Education | 651.690.7763

Purpose: St. Catherine University has a duty to protect the privacy of Protected Health Information (PHI). The purpose of this policy is to define the requirements for Health Insurance Portability and Accountability Act (HIPAA) training and documentation, the levels of violations, and sanctions resulting from noncompliance for staff, faculty and students within the HSSH who are participating in clinical/fieldwork education.

I. Definitions

A. Disclosure: The release, transfer, provision of access to, or divulging in any manner of PHI outside of the healthcare organization.

B. Protected Health Information (PHI):

1. Individually identifiable information, that is a subset of health information, including demographic information collected about an individual and is created or received by a health care provider, health plan, employer or health care clearinghouse;
2. Information related 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. This information can be written, verbal, or electronic, including the name, address, social security number, phone number, photograph, zip code, treatment date, employer, names of spouse and children, and any other personally identifiable information that can potentially identify the subject such as rare conditions, or characteristics, etc. PHI can be transmitted or accessed by electronic media, maintained in electronic media and/or transmitted or maintained in any other form or medium.
3. 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

C. Use: The sharing, employment, application, utilization, examination, or analysis of PHI within the healthcare organization.

D. Workforce: University faculty, staff, and students who have access to PHI because of their educational, clinical directed practice, or volunteer experiences which bring them to our healthcare partners. The HIPAA Privacy officers of the Henrietta Schmoll School of Health (HSSH) are:

- Nursing students - Dean of Nursing
- Health science students - Dean for Health Sciences

II. Training and Documentation Required

All Henrietta Schmoll School of Health (HSSH) faculty, staff and students will receive HIPAA training prior to going out for any clinical or field education which includes shadowing and volunteering experiences. This applies if there is any expectation that the individual would have access to PHI. Minimum HIPAA training must be completed annually.

The training must include:

1. Review of the HIPAA policy
2. Review of one or more of the HSSH approved training video(s)
3. Completion of program specific quiz with specified score threshold
4. Documentation that the student, faculty, and staff has completed the training and understands the responsibilities related to HIPAA and maintaining confidentiality of PHI.

Specific departments may have additional requirements as spelled out in their department faculty and student policies.

III. De-identification of PHI Data

Discussion of the clinical experience in the classroom setting is an appropriate and valid learning experience within the academic environment; however it must be done in a manner that protects patient and healthcare agency confidentiality. To protect the PHI consistently the student/faculty shall **de-identify** all discussions, notes, communications, and assignments regarding patients/clients by adhering to the following guidelines:

1. Student feedback about a patient/client, therapist, supervisor, or practice site will be discussed in class in a manner that is constructive and that preserves the confidentiality of all involved and that meets the requirements of HIPAA. To protect patient/client health information, the student will de-identify any patients/clients discussed in class by referring to clients in general terms, e.g., a woman over 60.
2. PHI includes the following patient/client details:
   a. Full name or initials of the patient/client
   b. Birth date
   c. Medical record number
   d. Patient's/client's relatives or patient's employer
   e. Address, including city, county, and zip code
   f. Telephone numbers (home, mobile, work, fax)
   g. Account number including Insurer, Insured Patient ID number, Group Numbers (i.e., insurance)
   h. Health beneficiary
   i. Social security number
   j. Driver's license number
   k. Finger prints, voice prints, retinal ID, or photographs

IV. Causes of HIPAA Incidents

A HIPAA violation occurs with any sharing of patients'/clients' PHI if not part of the assigned care delivery for the student or faculty. Examples can include, but are not limited to: careless handling of patient/client information; unauthorized access to the records of patients/clients for whom the student/faculty is not assigned; disclosure of patient/client information; sharing passwords or enabling others to work under the same user ID; accessing electronic patient/client information without first logging on with one's own unique identification or password; failing to log off, shut off, or otherwise protect computer access; gossiping about a patient's/clients health information; sharing or faxing documents containing patient/client information to an unauthorized or wrong recipient or fax number or unprotected email address; mailing reports or giving patient/client information or documents to the wrong patient/client; leaving printed documents containing patient/client or other confidential information unattended in a public place; having cameras or data storage devices with unencrypted patient/client data or pictures lost or stolen; sharing sensitive patient/client information while visitors are present in the patient's/client's room.

Medical records cannot be removed from a health-care facility. This includes any or all of the medical record in a printed or electronic format including digital copies, photographs/facsimile or transmission of data. Medical records include but are not limited insurance documents, billing items, any related documents or samples of documentation or copies of note writing forms, and actual items from a medical chart that could identify a particular patient/client.

V. HIPAA Violations

A. Procedure in the Event of a Potential HIPAA Violation

Student breaches of confidentiality are dealt with in the following manner:

1. Faculty will respectfully talk with the person who has made the breach in confidentiality with reminders about the policies of the school, discipline specific code of ethics, and the HIPAA law related to client and consumer rights to confidentiality. A corrective action plan will be developed.
2. Any breach of the HIPAA law must be reported immediately to the director of clinical education and to the relevant program director, who will notify the pertinent clinical site, and will contact the appropriate HIPAA officers [Dean of Nursing (for nursing programs) or Dean of Health Sciences (for all health science programs)].
3. Upon receiving report of a possible HIPAA violation, the HIPAA privacy officer will conduct a confidential investigation of the alleged violation.
4. If appropriate, the HIPAA privacy officer will interview any person who may have knowledge of the alleged violation.
5. The HIPAA privacy officer will determine if a violation has occurred in accordance with the violation levels outlined in Section V.B.
6. If a violation has occurred, the decision will be documented in writing and sanctions will be applied in accordance with Section V.C.
7. Depending on the seriousness of the confidentiality violation, be aware that violations of the HIPAA law may lead to dismissal of the student from the clinical site and/or the University, cancellation of the fieldwork contract (thereby preventing any further students from being placed at the facility), levy of a fine and/or legal action on the University and/or the student.

Faculty breaches of confidentiality are dealt with in the following manner:

1. Any breach of the HIPAA law must be reported immediately to the director of clinical education and to the relevant program director, who will notify the pertinent clinical site, and will contact the appropriate HIPAA privacy officer.
2. Upon receiving report of a possible HIPAA violation, the HIPAA privacy officer will conduct a confidential investigation of the alleged violation.
3. If appropriate, the HIPAA privacy officer will interview any person who may have knowledge of the alleged violation.
4. The HIPAA privacy officer will determine if a violation has occurred in accordance with the violation levels outlined in the Section V.B.
5. If a violation has occurred, the decision will be documented in writing and sanctions will be applied in accordance with Section V.C.
6. Depending on the seriousness of the confidentiality violation, be aware that violations of the HIPAA law may lead to dismissal of the faculty/staff from the clinical site and/or the University, cancellation of the fieldwork contract (thereby preventing any further students from being placed at the facility), levy of a fine and/or legal action on the University and/or the faculty/staff. Human resources will be consulted as needed depending on the violation and next steps.

B. Levels of HIPAA Violation and Regulation-Students

It is the policy of St. Catherine University to have and apply appropriate sanctions against members of its workforce and students who fail to comply with St. Catherine University's privacy regulations and procedures to protect the confidentiality and security of PHI. Sanctions will be imposed based on the severity of the violation, whether it was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure. The following violation levels outline some, but not all, types of violations that may occur:

1. **Level 1:** Failure to demonstrate appropriate care and safeguards in handling PHI. These are usually unintentional with no improper exposure of the information. Examples of Level 1 violations may include failing to log-off of a system, leaving PHI unattended in a non-secure area, or other minor first-time violations of regulations.
2. **Level 2:** Intentional or unintentional exposure of PHI or internal inappropriate access, unauthorized access to PHI, or repeated Level 1 violations. These result in no improper further exposure inside a healthcare organization or no disclosure outside of a healthcare organization or, if applicable, the University setting. Examples of Level 2 violations may include sharing ID/passwords with other staff that result in internal inappropriate access, accessing PHI for which the individual has no responsibility or is not needed as part of assigned duties.
3. **Level 3:** Intentional or unintentional exposure of PHI inside a healthcare organization or disclosure outside of a healthcare organization or, if applicable the University setting. Level 3 violation also includes repeated Level 2 violations. Examples of Level 3 violations may include providing passwords to unauthorized individuals that result in a disclosure outside a healthcare organization, sharing of PHI with unauthorized individuals, and failing to perform the necessary responsible actions that would prevent disclosure of PHI.
4. **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 destroying PHI.

Failure to adhere to these confidentiality guidelines may result in Academic Misconduct being filed against the student.

C. University Faculty and Staff Violations-Follow up actions

1. **Level 1:** Documented performance counseling and warning by the person with immediate supervisory responsibilities.
2. **Level 2:** Documented performance counseling and warning from the program director, department chair, or dean. Further actions may be initiated per University and department policies and procedures for faculty and staff and students.
3. **Level 3**: Referral to the HIPAA officer with supervisory authority for possible initiation of disciplinary actions per University policies and procedures.
4. **Level 4:** Referral to the HIPAA officer with supervisory authority for discharge or suspension per University policies and procedures.

D. University Healthcare Professions Students, Including Students as Volunteers in Healthcare Organizations, Violations:

1. **Level 1**: Documented counseling by the appropriate program director or department chair.
2. **Level 2**: Documented counseling by the HIPAA officers/dean(s). The dean may refer/consult regarding violations with the dean of students for further actions per the student handbook, University policies and regulations.
3. **Level 3**: Referral to the dean(s) and/or dean of students for penalties per the student handbook, University policies and regulations to include possible probation or suspension.
4. **Level 4**: Referral to the dean(s) and dean of students for penalties per the student handbook, University policies and regulations for suspension or expulsion.

VI. Help with this Policy

Students, faculty, and staff should direct all questions regarding this Policy to the Office of Clinical and Field Education: | 651.690.7763

VII. Related Policies or References

Eastern Carolina University HIPAA Sanctions policy 2013