University of Pittsburgh
School of Health & Rehabilitation Sciences
Department of Health Information Management

STUDENT CONFIDENTIALITY STATEMENT

As a student of the University of Pittsburgh, School of Health and Rehabilitation Sciences, Department of Health Information Management, you may have access to confidential information, also referred to as ***Protected Health Information*** (PHI). The purpose of this agreement is to help you understand your obligations regarding confidential, protected health information.

Confidential, PHI is protected by Federal and State laws and regulations. This includes HIPAA (the federal Health Insurance Portability and Accountability Act), the Joint Commission (a hospital accrediting body), Pennsylvania State Law, and strict University of Pittsburgh policies.

As a student, you are required to conduct yourself in strict conformance with the laws, standards, regulations, and University of Pittsburgh policies that govern confidential, PHI. Your obligations to maintain confidentiality of PHI are explained in this document. You are required to read, understand and abide by these rules. Anyone who violates any of these rules will be subject to discipline, which may include, but is not limited to, dismissal from the Department of Health Information Management within the School of Health and Rehabilitation Sciences at the University of Pittsburgh. In addition, violation of these rules may lead to civil and criminal penalties under HIPAA and the potential for other legal action.

As a student, you may have access to confidential information, which includes, but is not limited to, information relating to:

- Medical record information (includes all patient and patient's family's clinical, social, spiritual, demographic and financial data, and data contained in pictures, scans, collected survey and interview data, videos, and conversations). The patient is defined as all the people who receive service from the healthcare facility.
- PHI as defined by HIPAA includes, but is not limited to, names, all geographic subdivisions, all elements of dates, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers, serial numbers, web URLs, internet protocol (IP) address numbers, biometric identifiers (including finger & voice prints, full face photo images and any comparable images) and any other unique identifying number, characteristic, or code.
- All information concerning the activities or operations of any agency or health care organization and any and all research data, educational materials and data from any agency or health care organization.
- Employee information (i.e. social security number, employment records, salary records and disciplinary actions) and employment status of patients and patients' family members.
- Computer programs, health related applications, client and vendor proprietary information, source code and proprietary technology.

Carefully read the following statements
and sign below, acknowledging that you understand and agree to abide by these rules.

I agree that I will not access patient records (either in paper or electronic form) except when specifically permitted to do so by my preceptor. I understand that under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), my preceptor can only provide me with access to information which is necessary for the purposes of my student experience.

According to the American Health Information Management Association's (AHIMA's) Code of Ethics, it is the duty of all Health Information Management professionals to protect and maintain the confidentiality of all patients' medical information, since we serve as the patients' advocates for confidentiality.

I understand that I have an ethical duty while in the HIM program not to discuss with family, friends, or other acquaintances any confidential information seen or heard during class and lab, while working or volunteering on projects at local agencies and/or health care organizations, working or volunteering in any research projects and any other clinical and internship-related activities.

I will work to cultivate a climate where protection of patient privacy and PHI is always expected, and should I observe where confidentiality is not protected, I will speak up and inform my preceptor about the violation. The patient's privacy always comes FIRST.

I hereby agree that for all classes, labs, projects, research activities or internships/clinical activities:

- ✓ I will protect all confidential information that I may see or hear including, but not limited to:
  - All types of data collected in the research project,
  - Patient records (both paper and computer-based),
  - Guest speakers,
  - Student projects,
  - Class/lab discussions,
  - Conversations during internships and clinical visits (with staff and among staff),
  - Financial information of internship and clinical sites,
  - Any clinical and internship facility legal matters,
  - Clinical and internship facility computer access/usage information,
  - Any clinical facility and internship employee-employer issues or employee-employee issues, and
  - Any other class, lab, research, or internship/clinical facility information.

- ✓ I will act in a professional manner at all times.

- ✓ I will use the information obtained strictly to enhance my educational understanding and research activity.

- ✓ I will access only the information necessary to perform clinical and internship duties or as required for class/lab and project activities; and I will not search for:
    - Celebrity records,
    - Family member's records,
    - Any specific diagnoses, or
    - Records containing sensitive information.

  <u>If they are not needed in this research project.</u>

- ✓ I will maintain the confidentiality of all research data and results used for projects, unless otherwise allowed by the facility (for written and oral reporting, the facility will remain anonymous). I will NOT include patient identifying data in any written paper or poster and oral report, and I will not divulge any sensitive information about any patient, provider, employee or organization in any written paper, poster, or oral report. I will make EVERY ATTEMPT to de-identify patients, providers, employees, and organizations.

By signing this form, I agree to abide by all of the conditions set forth in this statement. I have been advised and understand that any violation of this agreement will result in ***disciplinary and academic actions*** up to and including dismissal from the Department of Health Information Management of the School of Health and Rehabilitation Sciences at the University of Pittsburgh, and I may be subject to criminal and civil liability.

I have read the attached document which provides specific examples of activities that violate patient privacy and have an awareness of unacceptable activities. I will strive to always protect patient privacy and encourage others to do so, and will report violations to my preceptor or academic advisor.

_____	_____	_____
Student Signature	Student Name (print)	Date
_____	_____	_____
Instructor/Advisor Signature	Instructor/Advisor Name (print)	Date

ACTIVITIES THAT VIOLATE PATIENT PRIVACY
BE MINDFUL OF THESE AND OTHER ACTIVITIES THAT CAN PUT YOU IN THE HOT SEAT

It is imperative that we continuously revisit the importance of the need for ALL health professionals to protect the privacy of ALL patients. We must create a climate where everyone is expected to ALWAYS be mindful that patients require the basic right to privacy.

Here is a list of some examples of activities, both obvious and not-so-obvious, that you should NEVER do when you are in the clinical setting working on a project, or participating in clinical education/internship.

Can you think of any other activities that belong on this list?

- Never copy and paste ANYTHING from a patient's record to ANY medium.
- Never name a facility {unless the facility gives you approval to do so}, physician, patient or any other person you are researching (coder, or any other employee) in any report. Assign alias names or numbers.
- Never post the name of a facility {unless the facility gives you approval to do so}, physician, patient or any other person you are researching (coder, or any other employee) on any poster or electronic medium. Assign alias names or numbers.
- Never take a screen shot of any confidential information, including patient name, diagnoses or services, provider name, or facility name.
- Never email any confidential information to yourself or any other individual not involved with the patient's care.
- Never discard confidential information in the trash.
- Never search for the medical record of a family member, friend or acquaintance.
- Never download confidential information onto any personal electronic device.
- Never discuss confidential patient information with a family member, friend or acquaintance, either in person or on the phone.
- Never email private information over the internet on an unsecured device.
- Never step away from a computer that displays confidential patient information without logging off.
- If you are provided a password to access a facility's information systems, NEVER share the password with anyone.
- Never Skype (or use any voice-over IP service) private patient information, pictures, or data.
- Never post private patient information, comments about patients, pictures, or data on Facebook, Twitter, Instagram or any other social media site.