UNIVERSITY OF ILLINOIS
CHICAGO • SPRINGFIELD • URBANA-CHAMPAIGN

University of Illinois Medical Center at Chicago

Confidentiality Agreement Employee/Volunteer/Student

As an employee/volunteer/student at University of Illinois, you may have access to "Confidential Information". The purpose of this agreement is to help you understand your obligations regarding confidential information.

Confidential information is protected by Federal and State laws, regulations, including HIPAA, the Joint Commission on Accreditation of Healthcare Organizations standards, and strict University policies. The intent of these laws, regulations, standards and policies is to insure that confidential information will remain confidential - that is, that it will be used only as necessary to accomplish the purpose for which it is needed.

As an employee/volunteer/student, you are required to conduct yourself in strict conformance with applicable laws, standards, regulations and University polices governing confidential information. Your principal obligations in this area are explained below. You are required to read and to abide by these rules. Anyone who violates any of these rules will be subject to discipline, which might include, but is not limited to, termination of employment or expulsion from the University. In addition, violation of these rules may lead to civil and criminal penalties under HIPAA and potentially other legal action.

As an employee/volunteer/student, you may have access to confidential information, which includes, but is not limited to, information relating to:

- Medical record information (includes all patient data, conversations, admitting information, demographic information and patient financial information).
- Protected Health Information (PHI) as defined by HIPAA includes, but is not limited to, names, all geographic subdivisions; all elements of dates (except year) for dates directly related to an individual, 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 and serial numbers, web universal resource locators (URLs), internet protocol (IP) address numbers, biometric identifiers, including finger and voice prints, full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.
- Employee information (i.e., social security number, employment records, and disciplinary actions).
- University information (i.e., financial and statistical records, strategic plans, internal reports, memos, contracts, quality and peer review information, and communications).
- Computer programs, client and vendor proprietary information, source code, and proprietary technology.

Employees, who have access to Cerner in accordance with their job responsibilities may access, view and print their own medical record for the duration of their employment or for the duration of the period that they retain the position that provided them access to Cerner. For copies of information not in Cerner, employees are required to contact the HIM Department. The Director of HIM is not responsible for actions taken on information printed and released by Medical Center employees.

NOTE:

Employees with this level of access are not permitted to access the medical records of their children, spouses, relatives or friends. Such access is considered a breach of patient privacy and is subject to disciplinary action. Employees who do not have access to Cerner must contact the HIM Department to request copies of their medical records.

In the event that you do have access to confidential information, you hereby agree as follows:

- You will only use confidential information/data as needed/necessary to perform your duties as an employee/volunteer/student affiliated with the University.
- You will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information/data except as properly authorized within the scope of your professional activities affiliated with the University.
- You will not misuse confidential information/data or be careless with it.
- You will safeguard and will not disclose your computer password or any other authorization that allows you to access confidential information/data. The University reserves the right to monitor access to the network, including your account, if deemed appropriate.
- You accept responsibility for all activities undertaken using your assigned access code and/or any other authorizations.
- You will report activities by any individual or entity that you suspect may compromise the confidentiality of information. The University will make all attempts possible to keep good faith reports confidential. However, absolute confidentiality cannot be guaranteed.
- You understand that your obligations under this Agreement will continue after your affiliation with the University terminates.
- You understand that any of your access privileges to confidential information/data are subject to periodic review, revision, and, if necessary, modification and/or termination.
- You understand that you have no right or ownership interest in any confidential information/data.
- The University may at any time revoke your access code, or any other authorization that allows you to access confidential information/data.
- You will be responsible for your misuse or wrongful disclosure of confidential information and for your failure to safeguard confidential information/data or your password or any other authorization that allows you to access confidential information/data.
- The University may take disciplinary action against you up to and including termination or expulsion from the University in the event you violate this Confidentiality Agreement. In addition, the University may initiate legal action including but not limited to civil litigation or criminal prosecution.
- You understand the University reserves the right to monitor and record all network and application activity including e-mail, with or without notice, and therefore users should have no expectations of privacy in the use of these resources.

"I certify that I have read and understand the Confidentiality Statement printed above and hereby agree to be bound by it."

_____ _____

Signature **Print Name**

_____/_____/_____

Date

Original copy to be retained in Department and a copy to Employee/Volunteer/Student

Revised 02/09