



# HOSPITAL INFORMATION SYSTEMS CODE OF ETHICS

*A nonprofit corporation of*

The Sisters of Charity  
of St. Augustine Health System and **University Hospitals  
HealthSystem**

## SOFTWARE

This code of ethics states the Hospital policy concerning software duplication. Unless otherwise provided in the license, any unauthorized duplication of copyrighted software, except for backup and archival purposes, is a violation of the law and is contrary to the Hospital's policies. The following points are to be followed to comply with software license agreements:

1. Hospital employees/students are not permitted to make unauthorized copies of any software under any circumstances.
2. The Hospital will not tolerate the use of unauthorized copies of software. Any employee/student illegally reproducing software can be subject to civil and criminal penalties, including fines and imprisonment. The Hospital does not condone illegal copying of software under any circumstances.
3. Hospital employees/students are not permitted to give software to any outsiders, including clients, customers and others.
4. All software used by the Hospital on company computers will be properly purchased through appropriate procedures.

## E-MAIL

1.
  - All employees will use the E-mail system in accordance with the E-mail Code of Ethics.
  - E-mail should not be used to relay patient clinical and occurrence information.
  - Use of profanity, racial slurs, sexual innuendoes, and threatening verbiage is prohibited and will not be tolerated.
  - The E-mail system shall not be used for personal communications, such as after-work appointments or gossip. E-mail is Hospital property and must be used for work purposes only. Information contained in the E-mail is Hospital property and may be accessed and disclosed as part of a legal process.
  - Using the system to solicit outside business ventures; to access confidential patient information without authorization or for personal; political; or religious causes is prohibited.
  - It is the sole responsibility of the user to minimize the number of old E-mail messages retained, in order to conserve resources.
2. All E-mail users are required to read and sign the Hospital Information Systems Code of Ethics and return the signed form to Information Services. Any user violating the Code of Ethics may be subject to progressive corrective action.

## PASSWORD ASSIGNMENT

By accepting a Signon/Password on the Hospital System(s), I understand:

1. I have a legal obligation to keep confidential all information concerning patients that I may have access to and will only discuss information with employees/students who have a need to know the information in order to perform their job.
2. I will not intentionally attempt to gain access to areas that are not needed for the performance of my job.
3. The signon/password that is assigned is unique to me and is not transferable.
4. I am solely and fully accountable for any information entered into the system or information accessed by any person under my signon/password. I will notify my supervisor and/or the System Manager (or designee) immediately, if I suspect that someone has gained unauthorized access to my signon/password.
5. I understand that according to the Hospital policy on confidentiality of information, any unauthorized access, release, use or possession of confidential information by an employee/student will result in progressive corrective action up to and including termination of employment.
6. I have read and understand the E-mail Code of Ethics.

MY SIGNATURE BELOW ACKNOWLEDGES THAT I HAVE READ AND UNDERSTOOD THE CODE OF ETHICS FOR MERCY MEDICAL CENTER UNDER WHICH A SIGNON/PASSWORD HAS BEEN ASSIGNED TO ME.

I UNDERSTAND THAT FAILURE TO COMPLY WITH THE ABOVE POLICIES WILL RESULT IN FORMAL DISCIPLINARY ACTION, UP TO AND POSSIBLY INCLUDING TERMINATION FROM THE COMPANY IN THE CASE OF EMPLOYEES AND THE TERMINATION OR CANCELLATION OF AGREEMENTS IN THE CASE OF PHYSICIANS, CONSULTANTS, OR VENDORS.

Employee/Student Signature	Print Name	Date
Manager/Instructor Signature	Print Name	Date

**FORWARD TO SECURITY ADMINISTRATOR, INFORMATION SERVICES DEPARTMENT. THANK YOU.**

# INFORMATION SECURITY AGREEMENT

Computerized information systems are one of the Company's most valuable assets. Our success and the privacy of our patients depend on the protection of this information against theft, destruction or disclosure to outside interests.

Employees, physicians, consultants and vendors may at some time be required to operate computer equipment or have access to software systems as part of their performance or duties for the Company. Those charged with this responsibility must understand information security policies in effect throughout the Company.

Therefore, I agree to the following provisions:

- Not to operate or attempt to operate computer equipment without specific authorization from supervisors.
- Not to demonstrate the operation of computer equipment to anyone without specific authorization.
- To maintain assigned passwords that allow access to computer systems and equipment in strictest confidence and not disclose a password with anyone at any time, for any reason.
- To access only computer systems, equipment and functions as required for the performance of my responsibilities.
- To contact my supervisor or Security Coordinator/Designee immediately and request a new password(s) if mine is (are) accidentally revealed.
- Not to record passwords in any manner, as this increases the possibility of accidental disclosure.
- Not to disclose any portion of the Company's computerized system with any unauthorized individuals. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens and documentation created by the Company employees or outside sources.
- Not to disclose any portion of a patient's record except to a recipient designated by the patient or to recipient authorized by the Company who has a need-to-know in order to provide for the continuing care of the patient or to discharge one's employment or other service obligation to the Company.
- To report activity that is contrary to the provisions of this agreement to my supervisor or Security Coordinator.

I understand that failure to comply with the above policies will result in formal disciplinary action, up to and possibly including termination from the Company in the case of employees and the termination or cancellation of agreements in the case of physicians, consultants, or vendors.

Employee/Physician/Consultant/Vendor Signature	Cost Center	Date
--	-------------	------

\_\_\_\_\_ Print Name