UNIVERSITY OF COLORADO HOSPITAL

Information Services Department

Computer System Security Statement

1. Any individual who requires use of computer applications will be assigned a unique sign-on code to access the system or application. ***This sign-on is issued to an individual and is equivalent to a LEGAL SIGNATURE; it should not be shared with anyone or made public.***
2. ***A user will safeguard all security codes given to them and will neither attempt to determine, use, nor attempt to use a sign-on code or password other than his/her own sign-on code. A user will change his/her password regularly and will avoid using passwords that are reused or can be easily guessed.***
3. False, misleading or inaccurate data may not be knowingly entered into the computer system. A user will not install software or hardware, or alter the configuration of a computer without permission from Information Services.
4. Patient, employee, and hospital information contained or entered into the computer system will not be accessed or disclosed except as required by the person's normal job duties and only in accordance with hospital policies. This information will remain confidential indefinitely, including after access to the system or employment ends.
5. Equipment that is used to access computer systems will not be moved nor disconnected without the knowledge and authorization of the Information Services Department.
6. Information Services should be contacted immediately in the event of any suspected violation of above policies. It is the responsibility of every user to know and comply with all hospital policies.
7. Internet and e-mail applications are intended for business use. ***University of Colorado Hospital owns all computer information. The user is hereby put on notice that all internet and e-mail is subject to monitoring by the Hospital, and the Hospital can copy, intercept, read or record as needed.***
8. Any information accessed via hospital computer systems will be on a need-to-know basis only. Need-to-know is defined as information needed in order to perform job functions.
9. A user will log out or secure the computer system or applications when unattended or not in use.
10. ***Violations of the above policies will result in disciplinary action, up to and including revoking computer system access, termination of employment, and criminal or civil charges.***

FILL OUT THE INFORMATION BELOW AND FAX TO UCH IS: 720-848-8402

I affirm that I have read, understand, and agree to the provisions and intent of this Computer System Security Statement.

Please print legibly and completely. Fill out **ALL** information requested inside this box.

****Note: UCH Employees and Contract Nurses complete the Security Statement in HealthStream.**

Name: _____
Last Name **First Name** **MI**

Employer (Circle): UCH UCHSC UPI Other: _____

Employee # or Non-emp Badge #: _____

***NON-UCH, UCHSC, UPI Required Info:** *Please Circle: Nursing Volunteer Student Non-Nursing Contract MD

*Estimated Term/End Date: _____ *Last 4 digits SS#: _____ *Gender: M F

Job Title: _____ Dept/Specialty: _____

Signature: _____ Date: _____

Revised on 3/9/2009