Huntington Hospital

Confidentiality, Computer Usage and Accountability Agreement

The information systems of Huntington Hospital ("Hospital") contain confidential information pertaining to patients, health care professionals and the organization. This information is a major asset for the organization and we are required by law to protect its confidentiality. Huntington Hospital informs individuals of their responsibilities and secures their agreement to abide by the associated policies and procedures.

I, _____ (print name):

1. will comply with the privacy, policies, and rules governing the use of any information accessible through information systems, mobile devices or any other means and only utilize the information to the minimum extent necessary for the performance of my assigned duties;
2. understand the use of hospital information systems, resources, network services, and issued IT equipment is a privilege rather than a right for the purpose of conducting hospital business and for patient care;
3. understand that the information systems contain sensitive and confidential patient, member, business, financial and employee information which should only be disclosed to those authorized and who have a direct business need or patient care need to receive it;
4. understand that I must follow current hospital procedures and have a specific business or patient care need to access information;
5. understand that patient or hospital information is for the sole use of performing my assigned duties and that I am responsible for protecting patient information from misuse;
6. will not attempt to gain unauthorized access to any information system or go beyond my authorized access. This includes attempting to gain access using another's user ID and password;
7. am the only person who has possession of my unique user ID and password, and will not share this information with others or allow anyone to access information systems using my user ID and password;
8. understand that my user ID and password are the equivalent of my signature and that I am accountable for all data and actions recorded under them; I will make certain to logon using my user ID and password before accessing information systems, including logging off systems currently logged on by another user;
9. understand that I am responsible for logging out of information systems and will not leave unattended a computer or mobile device to which I have logged on. I will make sure that no patient data is displayed on the screen before leaving the computer;
10. understand that I am responsible for the physical security of hospital-issued equipment in my care to minimize theft and loss of equipment; and will report to the Information Security Officer if I lose my equipment.
11. will immediately contact the Information Services Help Desk (626-397-5347) or Physician Informatics (626-397-2500) for physician offices, if I suspect that my user ID and password have been compromised;

12. understand that I will use approved methods for the proper disposal of paper-based documents containing patient information and an approved method of destroying electronic documents.

13. will make certain that data I enter into information systems is complete, accurate and timely, and will not knowingly omit or falsify data;

14. understand that my work product including computer files, patient information, emails, email accounts or other information created or updated by me in the course of my assigned duties is property of the Hospital; and I will only use such work product for the benefit of the Hospital, and I will not make copies except as part of my assigned duties without the written authorization of the Hospital;

15. will not remove any electronic or paper-based records, reports or copies from their storage location except in the performance of my assigned duties;

16. will not attempt to circumvent, disable, or remove any security measures implemented to protect computer systems, applications, mobile devices or the network;

17. will not download, install, operate, or make copies of unlicensed and unauthorized software, which includes commercial, shareware, and freeware from the Internet public domain on Hospital computers or mobile devices without the expressed consent from the Information Security and Information Technology departments;

18. will not seek personal benefit of, or permit others to benefit personally by any Hospital information or use of equipment available through my assigned duties;

19. understand that information systems may not be used for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by Hospital management;

20. will not access or distribute material in any form, that is profane or obscene (pornography); that advocates immoral, unethical, illegal, or dangerous acts; or that advocates violence, or any unlawful conduct or discrimination conducted towards other people;

21. understand that all use of information systems, internet, email, voicemail and mobile device usage may be monitored, logged, and audited for content and appropriateness of use;

22. understand that my access privileges are subject to periodic review, revision, renewal, and termination;

23. will report any violation of confidentiality or computer usage policies by reporting such incidents to the Compliance Officer, through the Compliance Webline (www.hhcompliancewebline.com), or by calling the Compliance Hotline (866-311-4231); and

24. I understand that violation of this agreement may be cause to have my access to information systems suspended or revoked; and may subject me to disciplinary action, up to and including termination of employment or medical staff affiliation; and may subject me to penalties under State and Federal laws and regulations. Violations of this Agreement will result in disciplinary action as outlined in the Affiliation with Schools Agreement and may also result in legal liability.

25. Those who cannot accept these standards of behavior may be denied access to the relevant computer systems and networks.

You will find additional information in the following policies:

- 013 Standards of Business Conduct
- 150 Privacy and Security Program: Governing Principles- HIPAA**
- 402 Access Controls (Computer Information, Access and Usage of)
- 407 Control of Medical Records
- 409 Facsimile Transmission of Protected Health Information (PHI)
- 423 Computers, Appropriate Use
- 432 Information Access Management
- 534 Inspections
- 810.7 E-Mail and Voice Mail Policy
- 840.3 Employee Standards of Conduct

By signing this document, I agree that I have read, understand, and will comply with this Agreement in all respects.

Signature: _____ Date: _____

Printed Name: _____ Phone number: _____

_____ e-mail address: _____

Unit Assigned: _____ Clinical rotation dates: From: to: _____

Instructor Name: _____ Phone number: _____

University/College _____