Staff, faculty, students, trainees, and all other individuals (hereafter referred to collectively as "workforce members") under the control of the University of Utah Health Sciences Center ("UUHSC") are required to maintain the confidentiality of patient, clinical, financial, or other sensitive information. UUHSC workforce members will be held personally responsible for safeguarding security log-in processes, passwords and electronic signatures. UUHSC workforce members must strictly adhere to standards that govern authorized access to, use and/or disclosure of sensitive and confidential information. Failure to do so may result in disciplinary action, up to and including termination of employment. (You are required to sign this document as a condition of employment.)

I ACKNOWLEDGE, UNDERSTAND, AND AGREE:

1. **The types and categories of (written, verbal, electronic or printed) considered to be confidential ("CONFIDENTIAL INFORMATION") includes, but is not limited to: (a) hospital medical records; (b) clinic medical records; (c) physician's private patient records; (d) medical records received from other health care providers; (e) correspondence addressed to or from workforce members of the UUHSC concerning a specific, identifiable patient; (f) patient information verbally given to me by the patient or other persons; (g) diagnoses; (h) assessments; (i)medical histories; (j) operative reports; (k) discharge summaries; (l) nursing notes; (m) medications; (n) treatment plans; (o) follow-up care plans; (p) requests for and results of consultations; (q) results of laboratory, radiologic, or other medical tests; (r) demographic data; (s)financial/funding information; and (t) all other types and categories of information to which I know or have reason to know the UUHSC intends or expects confidentiality to be maintained.**

2. Services provided by the UUHSC for its patients and all documents and information related to such services are considered private and CONFIDENTIAL INFORMATION.

3. **Patients furnish information to the UUHSC with the understanding and expectation that it will be kept confidential and used only by authorized persons, within the scope of his/her employment, as necessary, to provide needed services.**

4. CONFIDENTIAL INFORMATION stored in electronic form must be treated with the same medical/legal care as data in the paper chart.

5. **My access to CONFIDENTIAL INFORMATION subjects me to legal guidelines and obligations.**

6. I will comply with all information security policies and procedures in effect at the UUHSC.

7. **I will access data only in accordance with policies and standards.**

8. My security code (logon, password and electronic signature) is equivalent to my legal signature. I will be personally accountable for all access or use performed under these codes.

9. **By reason of my duties or in the course of my employment I may receive or have access to verbal, written or electronic information concerning patients, staff and services performed by the UUHSC. I will not inappropriately access, use, or disclose (verbally, in written form, or by electronic means) to any person, or permit any person to inappropriately access, use, or disclose any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the patients, staff or operations of University of Utah UUHSC at any time, during or after my employment.**

10. If and when my employment or assignment with the UUHSC ends, I will not inappropriately access, use, disclose, retain, or copy any reports or other documents prepared by me, coming into my possession or control, or to which I have access, nor any other information concerning the patients, staff or operations of the University of Utah.

11. I will not destroy or erase any data or information in any form located in or stored in UUHSC computers or files unless it is part of routine computer maintenance.

12. I will use discretion to assure conversations that include CONFIDENTIAL INFORMATION cannot be overheard by persons who do not have a "need to know" when information must be discussed with others in the performance of my duties.

13. I will adhere to UUHSC procedures governing proper handling or disposal of printed material containing individually identifiable information.

14. I will notify my supervisor and the UUHSC Privacy Officer (at 7-9241 or at uuhsc.utah.edu/privacy) immediately, but not later than one business day, of any actual or suspected inappropriate use, access, or disclosure of CONFIDENTIAL INFORMATION, whether by me or anyone else, whether intentional or accidental. There will be NO retaliation for filing a complaint.

15. I will maintain the confidentiality of all information concerning patients, staff, or operations of the University of Utah regardless of the method of retrieval, including information obtained on home-based or off-site personal computers.

16. The inappropriate access, use, or disclosure of information by me may violate state and/or federal laws and may subject me to civil damages and criminal prosecution, and to disciplinary action, up to and including termination.

17. All documents, encoded media, and other tangible items provided to me by the UUHSC or prepared, generated, or created by me in connection with any activity of the UUHSC are the property of the UUHSC.

18. The UUHSC as the holder of data, reserves the right to, and may monitor and audit, all information systems for security purposes.

19. Security codes (logon, password and electronic signature) are the user's way to verifying his/her identity and should be difficult for someone else to guess. Use of names, birth dates, phone numbers, etc. is not allowed. I will choose security codes carefully and not disclose them to anyone.

20. I will not disclose security codes to anyone nor will I attempt to learn another person's security codes. Any misuse of my confidential security code will be a violation of UUHSC policy and will subject me to disciplinary action, up to and including termination.

21. Security codes must not be written on paper that is accessible to anyone but the user and must not be visible around the terminal/workstation.

22. I may access my own health information via an electronic application, pursuant to established policies, but I may not access that of my spouse, children, family members, or co-workers unless I am involved in their direct care.

23. I will not access data on patients or other individuals for whom I have no responsibility or for whom I have no business related "need to know". Audit trails will track unauthorized access.

24. I will immediately contact the ITS Call Center to obtain a new security code if I have reason to believe the confidentiality of my security code has been breached.

25. Regardless of the site of access, information must be treated as confidential. Unauthorized access or release of confidential information will subject me to disciplinary action, up to and including termination.

26. I will take reasonable steps, such as using a screen saver with a password, to keep my workstations and logins as secure as possible to minimize the risk of unauthorized use of either.

27. I will refrain from making unauthorized copies of data or applications. Loading of viruses, unauthorized queries, and other interference with computer resources will subject me to disciplinary action, up to and including termination.

28. If I receive access to information stores such, as the ITS data warehouse, or other databases containing CONFIDENTIAL INFORMATION, I will utilize that access only for the intended and stated purpose and will not provide access to 3rd parties without the explicit written permission of the data steward. I will utilize data obtained from such information stores in conjunction with data use policies.

29. I am required to complete Privacy and Security Training.

30. This signed document will become a part of my permanent personnel and/or volunteer record.

31. Information Technology personnel will never ask for your password. If someone does ask for my password, I will report it immediately to the ITS Information Security Office at 7-9241.