STUDENT HEALTH SERVICE
CONFIDENTIALITY AND SECURITY AGREEMENT

Purpose: The Health Insurance Portability and Accountability Act (HIPAA) and its regulations, the California Confidentiality of Medical Information Act and other federal and state laws and regulations were established to protect the confidentiality of medical and personal information, and provide, generally, that patient information may not be disclosed except as permitted or required by law or unless authorized by the patient. These medical privacy laws and regulations apply to all members of the University of California, Santa Barbara, Health System (UCSB HS) workforce including faculty, staff, residents, fellows, medical and other students and volunteers. All members of the workforce of the Health System are required to agree to and sign this confidentiality statement.

CONFIDENTIALITY STATEMENT

As a member of the UCSB HS workforce, I understand that I may be working with confidential medical and other sensitive or private information. This information may include, but is not limited to, medical records, personnel information, ledgers, verbal discussions, and electronic communications including e-mail.

I understand and acknowledge that HIPAA requires that I be trained on the requirements of HIPAA and UCSB SH policies, procedures and guidelines relating to protection of confidential patient information, and I agree to obtain all required training before I access, use or disclose any confidential patient information.

I acknowledge that it is my responsibility to respect the privacy and confidentiality of patient and other confidential information. I will not access, use or disclose patient or other confidential information unless I do so in the course and scope of fulfilling my duties as a member of the UCSB HS workforce. I understand that I am required to immediately report any information about unauthorized access, use or disclosure of confidential patient information. Initial reports go to the UCSB HIPAA Compliance Officer. If electronic media is involved, an incident report will be forwarded to the Campus Sensitive Data Incident Coordinator.

I understand and acknowledge that, should I breach any provision of this agreement, I may be subject to civil or criminal liability and/or disciplinary action consistent with applicable University policies, bargaining contracts and University processes.

For more information on UCSB HS HIPAA-related policies, procedures and guidelines please contact your departmental HIPAA representative.
.

Initial _____

INFORMATION SECURITY POLICY

Purpose: The purpose of this policy is to establish requirements which all employees of Student Health (SH) and any other persons with access to SH information systems must follow in order both to prevent the improper disclosure of confidential information and to prevent unauthorized persons from gaining access to confidential information. SH maintains data on the Student Affairs (SA) Network which is supported by Student Information Systems and Technology (SIS&T). The University has a duty to safeguard confidential information which is accessible via this network and to insure that the use of computer workstations is in compliance with federal and state regulations and with University and campus policies.

Privileged Information: Except as provided for by law or policy, any information that contains personally identifiable elements is confidential.

1. All charts, reports, records, and conversations regarding care of patients of SH are kept confidential and are not discussed outside of the department.
2. You are only allowed to access and view confidential information that is necessary for you to do your job. You may not access medical records for any other purpose.
3. You may not discuss confidential information in public places. You may not leave documents displaying visible confidential information in open places. You may not disclose confidential information to any one in any form or by any means without the written consent of the identified person(s) except as provided for by law or policy, or to inform other employees who have a need to know.

Initial _____

Network Password Protocol: Your password is the key that provides access to confidential information. Passwords must be kept secret to assure confidentiality.

1. You must maintain your password as a secret code which you may not communicate to anyone, except as provided by item 7 below. If you reveal your password you are personally responsible for any adverse actions which may occur as a result.
2. You may not write down your password.
3. No employee, including your manager, has the right to request that you reveal your password. Do not reveal it to anyone.
4. You must change your password when it expires.
5. Your password must be at least 8 characters long and must include at least one uppercase letter, one lowercase letter and one number.
6. You may not use your SH password in any other system not supported by SH.
7. Where special circumstances require a shared workstation, the workstation manager is responsible for assigning the password and may only reveal it to individuals who have signed confidentiality agreements.

Initial _____

Workstation Use: There are many ways in which network resources can be breached through an individual workstation.

1. You may not leave your workstation logged on in your absence unless you have secured it from unauthorized access.
2. You should turn your workstation off at the end of your shift unless it is a shared workstation being taken over by another user or you will be making a remote connection to it later in the evening.
3. Willful or malicious introduction of viruses into the SA Network is prohibited and every effort should be made to prevent unknowing introduction of viruses.
4. The departmental Information Technology (IT) representative coordinates regulatory and policy compliance.
5. All software, including freeware, shareware and executable internet downloads, must be approved by your departmental IT representative.
6. You may not allow your computer to be connected to any other system through the use of a modem or any other communications device without the approval of your departmental IT representative.

Initial _____

E-mail:

1. E-mail may not be used for patient correspondence. Use Point and Click Secure Messages instead.
2. E-mail may be used to communicate about patients with other staff members within the SA Network.
3. Computer workstations are University property and should be used to conduct University business. However, incidental personal use of E-mail and web access is permissible where it does not interfere with the employee's work or the work of others.
4. Every E-mail user is responsible for abiding by the UC Electronic Communications Policy and the UCSB Implementation Guidelines, which may be viewed as PDF files at J\Policies\Electronic Communications.

Initial _____

Public Workstations:

Public workstations that are clearly visible to the public may only be used for University business. No personal E-mail or web activity is permitted between 8:30 am and 4:30 pm at these workstations. However, employees may use alternate workstations (in non-public areas) during these hours for incidental personal use so long as it does not interfere with the employee's work or the work of others.

Initial _____

Miscellaneous:

1. Protected Health Information (PHI) is any information related to diagnosis, treatment or payment for healthcare that identifies the patient.
2. PHI that is transmitted over an electronic communications network must be encrypted.
3. PHI on laptops or other portable devices must be encrypted.
4. A fax cover sheet including a Confidentiality Notice must be used with any outgoing fax containing confidential information.
5. Documents containing privileged information shall be disposed of by shredding; magnetic media (diskettes, hard disks, backup tapes, etc.) by degaussing or physical destruction; labeled specimen materials by placement in a sealed bio-hazard bag.

Initial _____

Sanctions: Violation of this policy may result in loss of access to information systems or to civil or criminal liability and/or disciplinary action consistent with applicable University policies, bargaining contracts and University processes. Initial _____

For more information on UCSB HS HIPAA-related policies, procedures and guidelines please contact your departmental HIPAA representative.

EMPLOYEE: Emergency home e-mail address: _____

_____ _____ _____

Signature Printed Name Date

……

SUPERVISOR:

Employee is: ___ Staff ___ Student ___ Intern Copy from: _____
other employee with same setup

Employee needs: ___ MS Office ___ E-mail ___ PnC Folders: _____

I certify that the above named employee has received HIPAA training on the Student Health web site,

_____ _____ _____

Signature Printed Name Date