California Pacific Medical Center
A Sutter Health Affiliate
With You. For Life.

POLICY AND PROCEDURE

Section: General Administration	Manual: Administration Policy No.: 1.99.09 Approved By: Regional Director Corporate Compliance
Subject: Sutter Health / California Pacific Medical Center Policy On Workforce Confidentiality/Privacy And Appropriate Use of Sutter Property	Effective Date: 5/98 Revision Date: 5/04, 1/05, 5/07 Review Date: 3/07,
Cross References:	

I. Policy.

It is the policy of Sutter Health and its affiliates ("Sutter") that all members of the Sutter Workforce treat patient, personnel, and organizational records as confidential. This includes the protected health information ("PHI") of patients treated in Sutter facilities, employment records (including social security numbers), and information related to Sutter's confidential and proprietary business practices and plans. Sutter and its Workforce are legally and ethically obligated to protect such information. It is the policy of Sutter Health and its affiliates that all members of the Sutter Workforce execute annually a "Workforce Confidentiality/ Privacy Agreement" acknowledging their understanding of this policy and their agreement to abide by the guidelines of this policy.

II. Purpose.

The purpose of the Workforce Confidentiality/Privacy Policy is to protect and ensure the appropriate use of Sutter's property and communication systems. Sutter is committed to fair and ethical business practices and to ensuring the utmost confidentiality of records and information related to all patients, physicians, employees, and business operations.

III. Guidelines.

A. Definitions

(i) "Patient" means any person who has registered and received services at a Sutter Health affiliate without regard to date of services.

(ii) "Protected Health Information" ("PHI") means any information about a patient that has been received, created, or stored by a Sutter Health affiliate and which includes information that may be used to identify the patient. PHI includes any such information whether in oral or recorded form, both electronic and written.

(iii) "Sanction" means a disciplinary penalty or measure taken by Sutter Health or a Sutter Health Affiliate.

(iv) "Violation" occurs when an employee fails to comply with a federal or California law or regulation, or a policy of Sutter Health or a Sutter Health affiliate regarding the protection of PHI.

(v) "Workforce" means employees, volunteers, trainees and other persons under the direct control of Sutter, whether or not paid by Sutter. Workforce also means any independent contractors who interact with PHI and who have not signed a Business Associate Agreement

B. Workforce Confidentiality/Privacy Agreement

(i) All Sutter Workforce members shall be provided with a copy of this policy and required to sign a Workforce Confidentiality/Privacy Agreement when they are hired and annually thereafter. The form of this Agreement is attached hereto as Exhibit A.

(ii) Sutter Health or the pertinent Sutter Health affiliate shall assure that all members of its Workforce annually complete a " Workforce Confidentiality/Privacy Agreement," and shall maintain these agreements appropriately (e.g. for employees, in the employees' personnel file).

(iii) Sutter Health or the pertinent Sutter Health affiliate shall address violations of this policy and apply appropriate Sanctions to remedy the problem.

(iv) Nothing in this policy is intended to, shall be construed to, interfere with or otherwise limit any protected rights that Sutter Health or Sutter Health affiliate employees may have under applicable laws, including Section 7 of the National Labor Relations Act.

C. Access and Use of Patient and Business Information

(i) Workforce members may only access files or programs, whether computerized or otherwise, that are necessary to perform their job functions. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems, or programs, or other property of Sutter or improper use of information obtained by unauthorized means, may be grounds for disciplinary action, up to and including termination.

(ii) If Sutter Health or Sutter Health affiliate has implemented a guest internet wireless service, such service is intended for the use of Sutter Health or Sutter Health affiliate patients or guests and their personal computer property only. When using the computer property of Sutter Health or Sutter Health affiliate, Workforce members may only connect to the Sutter Health network and may not connect to the guest internet wireless service.

(iii) Workforce of Sutter should not have an expectation of privacy in public areas. Sutter reserves the right to conduct video surveillance for public safety and security purposes and for investigatory purposes if Sutter has reason to believe that Workforce members or visitors are engaged in illegal conduct or conduct which violates Sutter rules or regulations

(iv) Workforce members are expected to adhere to the following guidelines in order to maintain security and confidentiality:

- Ensure recipients of confidential information are authorized to receive it. Verify identities of recipients before releasing any information.
- Do not discuss confidential matters where others may overhear conversations.
- Do not leave documents or paper records where unauthorized persons can access or view them. Secure documents in locked cabinets as appropriate to ensure security.
- Follow established procedures when faxing confidential or sensitive information.
- Shred or otherwise confidentially destroy documents that are no longer needed.
- Protect computer screens from view by unauthorized persons, especially the general public.
- Sign-off before leaving computer workstations.
- Do not share computer user codes or passwords (except with supervisors or other appropriate personnel).
- Understand and abide by Sutter Health e-mail policy.
- Report suspected or known breaches of confidentiality to a supervisor or manager.
- If in doubt treat information as confidential and consult a supervisor regarding use and disclosure.

D. Work Areas and Equipment

(i) Desks, storage areas, work areas, lockers, file cabinets, credenzas, computer systems, office telephones, modems, facsimile machines, duplicating machines and vehicles purchased or leased by Sutter are the property of Sutter and must be used only for work purposes, except as provided in this policy.

(ii) Unless specifically authorized, Workforce members may not use their personal locks on storage or work areas owned by Sutter. Keys and locks will be issued to employees at the discretion of Sutter, based upon position held and business need.

(iii) Sutter reserves the right, at all times, and without prior notice, to inspect and search any and all Sutter property for the purpose of determining whether this policy or any other Sutter policy has been violated, or whether such inspection and investigation is necessary for purposes of promoting safety in the workplace or compliance with State and Federal laws. Such inspections may be conducted during or after business hours and in the presence or absence of the Workforce member.

E. Use of Technical Resources

(i) Sutter computer systems and other technical resources, including voice-mail and e-mail accounts and systems, are provided for use in the pursuit of Sutter's business. Accordingly, Sutter computer systems or other technical resources may be subject to investigation, search and review by Sutter in accordance with this policy. In addition, any electronically stored communications that are sent or received may be retrieved and reviewed by Sutter.

(ii) Sutter recognizes that Workforce members may occasionally find it necessary to use Sutter telephones and computer systems for personal business. Such use must be kept to a

minimum, must not interfere with work, and must not violate any other Sutter policy or procedure applicable to the Workforce members. Workforce members wishing to make personal, long distance telephone calls must use personal cell phones, personal calling cards or public pay telephones. Nevertheless, the Workforce member has no right of privacy as to any information or file maintained in or on Sutter property or transmitted or stored through Sutter computer systems, voice-mail, e-mail accounts and systems, or other technical resources.

(iii) For purposes of inspecting, investigating, or searching Workforce members' computerized files or transmissions, voice-mail, or e-mail accounts and systems, Sutter may override any applicable passwords or codes in accordance with the best interests of Sutter, its employees, or its clients, customers or visitors.

(iv) All bills and other documentation related to the use of Sutter equipment or property are the property of Sutter and may be reviewed and used for purposes that Sutter consider appropriate.

EXHIBIT A

Sutter Health / California Pacific Medical Center

WORKFORCE CONFIDENTIALITY AGREEMENT

I understand that I may have access to information that is confidential and may not be disclosed except as permitted or required by law and by Sutter Health/California Pacific Medical Center (CPMC) policies and procedures. This information includes, but is not limited to, protected health information, personnel information and proprietary business operations information. I understand that I am committed to protect and safeguard from disclosure all confidential information regardless of the type of media on which it is stored (e.g. paper, micro-fiche, voice tape, computer systems). I agree that I will not disclose any confidential information from any record or information system to any unauthorized person.

I understand that:

- I am obligated to hold confidential information in the strictest confidence and not to disclose the information to any person or in any manner that is inconsistent with applicable law or the policies and procedures of Sutter Health/CPMC.

- I acknowledge that I may not use or disclose any confidential records of a friend, relative, staff member, volunteer or any other person, unless I am authorized to do so and am required to do so as part of my official duties. Such use and disclosure must be restricted to that required for essential business purpose(s).

- I will not discuss or allow confidential information of any type to be displayed or overheard in the proximity of any individual who does not have the right or need to know. This includes conversations in public places or private spaces where they may be easily overheard, allowing computer screens to be inappropriately visible, and leaving printed material where it may be openly viewed.

- In order to access certain information, a unique User ID, Security Code, Password, Access Device or Biometric ID may be established that identifies me to Sutter Health/CPMC Information Systems. My authentication codes and devices are for my use only when accessing facilities, systems and information appropriate to my work (although my supervisor or other authorized personnel may have access to such codes). To use anyone else's authentication code or device in order to access any Sutter Health/CPMC system is considered a violation of Sutter Health/CPMC confidentiality and security standards.

- All information obtained from Sutter Health/CPMC systems remains the property of Sutter Health/CPMC regardless of physical location or method of storage, unless otherwise specified by Sutter Health/CPMC in writing.

- If I believe that information confidentiality or security may be compromised in any way, either through the possible disclosure of sign-on information or the direct unauthorized access of information, either intentional or accidental, I shall contact my direct supervisor and/or the Sutter Health Compliance Department as soon as possible.

- User accounts or access to electronic information may be disabled without prior notice by the Chief Data Security Officer, Chief Information Officer or their designee when, in their opinion, they hold a reasonable belief that a user's account may be compromised or is being used for inappropriate access to information.

- I understand that my privileges are subject to periodic review, revision, and if appropriate, renewal. I understand that all access to Sutter Health/CPMC systems is subject to monitoring and review as deemed appropriate by Sutter Health/CPMC.

- If Sutter Health/CPMC has implemented a guest internet wireless service, such service is intended for the use of Sutter Health/CPMC patients or guests and their personal computer property only. When using the computer property of Sutter Health/CPMC, Workforce members may only connect to the Sutter Health network and may not connect to the guest internet wireless service.

- If at any time I feel that the confidentiality of my password(s), sign-on(s) or identification device(s) has been compromised, I will notify the Sutter Health/CPMC Help Desk immediately so that my old code(s)/device(s) can be cancelled and new ones issued.

- My confidentiality obligation continues indefinitely.

- This Agreement does not supercede any other rules or expectations regarding the use or disclosure of confidential information that may be contained in other Sutter Health/CPMC documents. Such documents include, but are not limited to, job descriptions, policies, employee handbooks and department procedures.

- This Agreement is not intended to, and does not, interfere with any protected rights that I may have under applicable laws, including Section 7 of the National Labor Relations Act.

I understand that any access, attempted access, or disclosure of information in violation of law or Sutter Health/CPMC policies will be considered a breach of confidentiality. I understand that if I breach such confidentiality, I may be subject to immediate disciplinary action, up to and including termination.

My signature below acknowledges that I agree to abide by the terms of this agreement.

Printed Name:_____ Dept.: _____

Signature: _____ Date:_____

(NOTE: Employees may view the policy and agreement on HealthStream and acknowledge their agreement electronically.)