



**Sutter Health / California Pacific Medical Center  
Policy On Workforce Confidentiality/Privacy  
And Appropriate Use of Sutter Property**

## **Policy**

It is the policy of Sutter Health and its affiliates 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 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.

## **Definitions :**

**“Patient”** means any person who has registered and received services at a Sutter Health affiliate without regard to date of services.

**“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.

**“Sanction”** means a disciplinary penalty or measure taken by Sutter Health or a Sutter Health Affiliate.

**“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.

**“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.

## **Workforce Confidentiality/Privacy Agreement**

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.

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).

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

Nothing in this policy is intended to, or 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.



## **Access and Use of Patient and Business Information**

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.

## **Access and Use of Patient and Business Information**

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.



## **Access and Use of Patient and Business Information**

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



## **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.

## Work Areas and Equipment

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.

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.

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.



## Technical Resources

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.

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.