CONFIDENTIALITY OF PATIENT AND HOSPITAL BUSINESS INFORMATION

All employees (which for purposes of this policy include contracted staff) are responsible for upholding hospital privacy, confidentiality, ethics, and information security policies and procedures, including those contained in the notice of privacy practices.

Violation of this policy; any other hospital privacy, confidentiality, or information security policy or procedure; the hospital's notice of privacy practices; or any law with respect to these issues will result in disciplinary action, which may include immediate termination. In addition, employees may be civilly and criminally liable for breach of privacy, confidentiality, or information security laws regarding a patient.

Everyone is expected to treat patient and hospital information in a respectful, professional, and confidential manner. Such information should never be viewed or discussed with another for reasons of personal interest or for reasons outside the employee's responsibilities.

The privacy officer is responsible for the development and implementation of the hospital's policies and procedures regarding privacy and confidentiality of protected health information.

Patient Information

We are required to comply with federal, state, and local laws relating to the confidentiality of patient information, including the Health Insurance Portability and Accountability Act (also known as HIPAA). We are entrusted with protecting confidential patient information, also known as protected health information (PHI). This includes, but is not limited to, any past, present, and future patient-identifiable, clinical, and financial information, in verbal, written, electronic, or other medium (such as that contained on hospital computers, hospital information systems including computing devices, patient charts, and/or other hospital records). The information must be kept completely confidential except where the hospital and/or employees are legally required to disclose certain information.

All employees who come into contact with protected health information must abide by applicable laws for safeguarding and maintaining the confidentiality of such information.

Employees may not use hospital computer or other records to directly obtain information about their own or a family member's patient record. Hospital policy requires all patients to provide completed and signed hospital-designated forms to Health Information Management (and/or other departments, as appropriate) to view or obtain copies of their health records; employees and their family members are subject to the same requirement.

Business Information

All employees are required to maintain the confidentiality of all business information that is not made available to the public by the hospital. This includes but is not limited to personnel information, payroll records, and financial data.

Information Security

Employees shall comply with all hospital information security measures, policies, and procedures to protect the confidentiality of all hospital information, both patient- and business-related. Passwords and other information security measures are set up in the name of each employee for use only by the person to whom they are issued as necessary to perform job functions. Employees are prohibited from sharing passwords and from giving or receiving passwords to or from another user. Any compromised password or other breach of information security measures must be reported immediately to the department director or supervisor.

Although employees may be able to use passwords or codes to restrict access to information left on these systems, it must be remembered that these systems are intended solely for hospital business use. In keeping with this intention, the hospital maintains the ability to access and monitor any information on these systems. Because the hospital reserves the right to obtain access to all voice-mail and computer files including e-mail and internet sites visited for the purposes of appropriate hospital operations and management, employees should not assume that such information is confidential or that access by the hospital or its designated representatives will not occur. Access to these

systems may be conducted before, during, or after working hours, and in the presence or absence of the employee, at the discretion of the hospital.

Complaints, Investigations, and Disciplinary Action

COMPLAINTS

The hospital accepts complaints from any person about any aspect of its privacy, confidentiality, or information security practices as they relate to the protected health information of its patients. The hospital is committed to promptly investigating all such complaints, including those about our vendors (also called business associates) and any entities that they may have engaged.

All patients or other individuals who wish to make a complaint about any aspect of the hospital's privacy, confidentiality, or information security practices should be referred to the hospital's privacy officer for assistance. Employees are encouraged to speak with their supervisor regarding any complaints. If unresolved to the employee's satisfaction after speaking with the supervisor or if the employee is uncomfortable speaking with the supervisor, the employee may make complaints to the privacy officer, Human Resources director, or department director, as he/she deems appropriate. The privacy officer may be contacted by telephone at: **(831) 625-4582**. The employee may also write the privacy officer at:

Community Hospital of the Monterey Peninsula
Privacy Officer
P.O. Box HH
Monterey, CA 93942

Individuals also may complain directly to the secretary of the federal Department of Health & Human Services. Individuals wishing to complain directly to the federal government should be referred to the privacy officer who provides such persons with the contact information they need to file a complaint. The hospital will not retaliate against anyone filing a complaint.

Informal Investigation

A department director, privacy officer, or Human Resources director may conduct an informal investigation to determine the validity of a complaint or concern that comes to his or her attention. If insufficient evidence is found to determine the validity of the complaint or concern or if the investigating party believes that no violation has occurred, the matter will not be pursued further.

Formal Investigation

To determine if a formal investigation is warranted, the department director, the director of Human Resources, and the privacy officer confer with one another to discuss the actual, suspected, or alleged violation by an employee. If the violation of patient information is at issue, the privacy officer participates in the formal investigation. The involved parties decide who will lead the investigation. If the parties cannot decide, the issue is elevated to Administration for a determination.

The person responsible for the investigation, in conjunction with, as applicable, the privacy officer, the director of Human Resources, and/or department director, investigates the actual, suspected, or alleged violation.

As part of its investigation of complaints regarding its privacy, confidentiality, and information security practices, the hospital seeks to determine if the cause of the complaint was a use or disclosure of protected health information that violated either the hospital's policies and procedures or applicable federal, state, or local law.

Documentation of Investigation

Upon completion of the formal investigation, as determined by the person leading the investigation, in consultation with, as applicable, the privacy officer, the director of Human Resources, and/or the department director, the person leading the investigation prepares a report that documents the scope of the investigation and its conclusions. The person leading the investigation also prepares a recommendation on how the hospital should respond to the results of the investigation with the input of, as applicable, the

privacy officer, the director of Human Resources, and the department director. A copy of the investigation report and recommendation is submitted to Administration.

Determination of Hospital Actions

The decision about the hospital's response, including appropriate disciplinary action in cases involving violation of hospital policies and procedures about privacy, confidentiality, and information security practices is determined by Administration in consultation with the privacy officer, the department director, and the director of Human Resources, as appropriate.

The following disciplinary actions are applied based on the nature of the violation:

1. Unintentional Disclosure

    a. If an employee discloses patient and/or other hospital business information unintentionally due to a human error, the employee receives a verbal counseling for the first incident. Examples may include, but are not limited to, sending a fax to the wrong number or providing a patient's medical information to the wrong patient.

    b. Subsequent human errors of unintentional disclosure may result in further disciplinary action, from verbal warning up to and including termination of employment depending on the severity and/or frequency of the errors. Departments may establish their own policies stating when and what type of disciplinary action is taken for repeat errors of this nature. Department-specific policies must be reviewed and approved by the Human Resources Steering Committee before implementation of the department policy in order to be valid.

2. Violation of Hospital Policy

    Certain incidents of disclosing or accessing patient information or other hospital business information may not violate patient privacy rights (as defined by applicable federal and state privacy regulations) but may be considered violations of hospital policy, particularly when proper procedures have not been followed.

a. A written warning is issued upon the first occurrence of the following or similar events:

- Failing to follow hospital procedures for authorization to view or obtain copies from Health Information Management of (i) an employee's own medical records; (ii) an employee's dependent's medical records; and/or (iii) an employee's spouse's or domestic partner's medical records. In the case of a dependent's medical records, the employee must demonstrate that he/she would have the right to access the dependent's records.

b. Subsequent occurrences of the violation of hospital policies as described above will result in further disciplinary action, up to and including termination of employment.

3. Violation of Patient Privacy Laws

a. If an allegation or suspicion arises that an employee may have violated a patient's privacy rights, the employee is interviewed by the employee's director or supervisor, the privacy officer, and/or a representative from Human Resources.

b. Following the interview, if further investigation is warranted, the employee will be suspended.

c. If the results of the investigation find that the employee violated a patient's privacy rights (including but not limited to disclosing or accessing a patient's PHI for personal reasons), the employee is terminated even if the violation is a first offense.

If the hospital determines that such a violation did occur, and verifies that harmful effects resulted, it will mitigate, to the extent practical, the harmful effects of which it has become aware. The hospital's mitigation efforts may extend to its vendors and other third parties, as appropriate.

Notification

The department director, or such other person designated by Administration, in consultation with Human Resources, notifies any affected employees of any disciplinary action to be taken. Administration determines who should provide notification to any patient or complainant and the scope of such notification.