

# County of Santa Clara Santa Clara Valley Health and Hospital System Surveillance Use Policy

## FairWarning Electronic Health Record Privacy Monitoring System

### 1. Purpose

Santa Clara Valley Health and Hospital System (SCVHHS) maintains a Patient Privacy Program to ensure compliance with requirements promulgated in the Health Insurance Portability and Accountability Act (HIPAA), and various other federal and state privacy statutes and regulations. The HIPAA Security Rule requires health care entities to protect patient information that is stored electronically. SCVHHS stores patient information in various electronic health record (EHR) systems, and SCVHHS therefore must comply with the HIPAA Security Rule.

County workforce members may be granted access to EHR systems (“EHR users”) ~~in order to~~ access patient information that is required to perform authorized County duties. ~~In order to~~ To comply with the HIPAA Security Rule, SCVHHS must monitor EHR user access (see, 45 CFR §§ 164.312(b) and 164.308(a)(1)(ii)(D)). ~~This~~ Currently, this is accomplished using “audit trails” that log each time an EHR user accesses a patient’s record. These audit trails are regularly reviewed.

SCVHHS purchased a vendor-supported software solution called FairWarning. The system receives daily reports from multiple databases (e.g., EHR audit trails, PeopleSoft data fields, Active Directory data fields) and ~~then~~ analyzes the data for certain indicators of potential inappropriate EHR access. When these indicators are identified, FairWarning generates “alerts.”

FairWarning ~~can also~~ shall be used to generate customized audit trails and reports of EHR user access.

### 2. Authorized and Prohibited Uses

Use of FairWarning ~~is used~~ shall be limited to ~~monitor~~ monitoring EHR user access and ~~investigate~~ investigating potential privacy-violation incidents. Only authorized staff members shall access ~~information~~ FairWarning data captured by the FairWarning audit trails and other database extracts available in FairWarning. ~~This information may~~ It shall be used by permissible for:

- the Ethics & Compliance Office to use the data to monitor EHR user activity, investigate potential privacy incidents, and report incidents to various local, state, and

federal regulators. ~~The information may also;~~

- HHS management or its written designees to use the data to assist with HIPAA compliance and other authorized purposes, including to assess or investigate behavior or activity that appears to be provided unauthorized, improper, illegal, or in furtherance of illegal activity;
- the Ethics & Compliance Office and HHS management, or their written designees, to provide this data to local authorities, the Sheriff's Office pursuant to a Memorandum of Understanding (MOU) with SCVHHS, SCVHHS Protective Services Office staff, County Counsel, and SCVHHS Department Heads or their written designees for purposes of conducting official county/County business, including assessing and investigating possible HIPAA violations and other wrongdoing.

~~Management may access Protected health information in (PHI) disclosure shall be limited to the extent required by patient privacy laws and regulations.~~

~~All other FairWarning to assist with HIPAA compliance and other authorized purposes. Management may also review access or uses of FairWarning data to assess or investigate unusual, suspicious, or illegal behavior or activities.~~

~~shall be prohibited. FairWarning and its data shall not be used for personal, non-County purposes. All other access to or uses of the data available in FairWarning are prohibited; and shall not be used to harass, intimidate, or discriminate against any individual or group.~~

### **3. Data Collection**

FairWarning receives daily data imports from multiple databases, including EHR audit trails. Limited personnel data is also imported from PeopleSoft and Active Directory in order to validate the identity of EHR users. As a result, FairWarning may contain any or all of the following data elements: (1) the identity of EHR users, including job title, department, date of birth, and home address; (2) the identity of patients whose charts are accessed; (3) date/time of EHR access events, including date/time a particular patient's chart was accessed; (4) type of clinical, demographic or other information accessed; and (5) type of EHR user activity (e.g., read only, write, print, etc.).

### **4. Data Access**

Access to data from FairWarning shall be restricted to only the following and only for County business purposes:

- SCVHHS Ethics & Compliance Office;
- Sheriff's Office personnel pursuant to MOU with SCVHHS;

- Protective Services Office staff (SCVHHS security personnel);
- SCVHHS Department Heads or their written designees;
- the County’s Labor Relations Department and the Office of the County Counsel related to specific administrative, civil, or criminal investigations.

Protected health information (PHI) disclosure shall be limited to the extent required by patient privacy laws and regulations.

Efforts shall be made to keep the total number of designees with access to the data as low as possible within the constraints of this Policy.

//

//

## **5. Data Storage and Protection**

Information generated by FairWarning shall be accessible to only authorized staff and configured to prevent unauthorized modification, duplication, or destruction. In addition to password protection, ~~County information technology policies that apply to County servers protect the FairWarning databases and their data~~ the data shall be protected through secure County servers.

## **6. Data Retention**

~~FairWarning server policies comply with applicable County data retention requirements, and all FairWarning records shall be retained for a minimum of seven years.~~

## 7. PUBLIC ACCESS

FairWarning data shall be retained and destroyed in compliance with applicable County data retention requirements, but the default retention period shall be 10 years due to the SCVHHS record retention policy and the Health Insurance Portability and Accountability Act (HIPAA) at 45 CFR 164.528, subdivisions (a)(1), (a)(3), and (b)(1), which provide that an individual has a right to receive an accounting of certain disclosures of PHI in the six years prior to the date on which the accounting is requested, and the covered entity has a legal obligation to provide certain disclosures that occurred during the six years before the request. If no County data retention requirement or law requires the data to be retained for longer than 10 years, the data shall be destroyed no later than six months following the end of the 10-year retention period.

## 7. Public Access

Public requests for data from FairWarning shall be submitted to the SCVHHS CPRA (California Public Records Act) Coordinator for handling. ~~Data from FairWarning may~~ If a CPRA request, subpoena, or court order is issued for such images, the data shall be made available public or deemed exempt from public disclosure pursuant to the extent required

~~by state or federal law, policy, or County agreements,~~ after ~~consulting~~ consultation with the Office of the County Counsel— as needed

## 8. Third-Party Data Sharing

It shall be permissible for the data from FairWarning ~~may~~ to be provided to only the following third parties without a court order or subpoena: government regulators to the extent required as part of a HIPAA-compliance audit or mandated disclosures; law enforcement representatives outside SCVHHS if the SCVHHS Department Head ~~or~~ with oversight responsibility for this Policy or written designee believes that the data ~~may show suspicious or illegal~~ shows behavior or activity— that appears to be unauthorized, improper, illegal, or in furtherance of illegal activity.

Data may be requested by: - an employee or an employee representative regarding a specific claim, allegation, or action against the employee; or law enforcement; or a third party seeking compliance with a court order or subpoena. In each of those circumstances, the request shall be reviewed by the SCVHHS Department Head or designee, who shall seek assistance as appropriate from the Office of the County Counsel and the Labor Relations Department.

Protected health information (PHI) disclosure shall be limited to the extent required by patient privacy laws and regulations.

## 9. Training

Personnel involved in maintaining and using FairWarning shall be appropriately trained on the use of the system and informed of this Surveillance Use Policy.

## 10. Oversight

SCVHHS Ethics & Compliance Officer or written designee shall oversee compliance with this Surveillance Use Policy.

Any employee found to have violated the Surveillance Use Policy ~~may~~ shall be subject to possible discipline. Alleged violations of the Surveillance Use Policy shall be reviewed by the SCVHHS Department Head and/or their designee(s) with the assistance of the Labor Relations Department and the Office of the County Counsel.

Approved as to Form and Legality

---

Rob Coelho  
Office of the County Counsel