

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

**Badge and Biometric Readers**

This Surveillance Use Policy is for the sole use of the Santa Clara Valley Health and Hospital System (SCVHHS).

**1. Purpose**

SCVHHS maintains and operates infrared badge readers provided through a vendor, Comtel Systems, Inc. at various locations, and biometric readers at the Public Health Department, to create a secure environment for all visitors and staff at SCVHHS facilities. Badge and/or biometric readers shall be used to gain entry to areas having automated access control and entry points. Biometric readers identify the fingerprint as being authorized to enter the designated secure location, but do not identify the individual.

Upon use, badge readers identify the individual identified on the badge. Badge readers collect information such as the date and time an individual enters and exits a building. This information may be provided to local law enforcement authorities, the Sheriff's Office pursuant to a Memorandum of Understanding (MOU) with SCVHHS, SCVHHS Protective Services Office staff, SCVHHS Director of Facilities or designee, and SCVHHS Department Heads or their designees for purposes of conducting official County business or investigating behavior or activity that reasonably appears to be unauthorized, in violation of department or County policy, illegal, or in furtherance of illegal activity.

**2. Authorized and Prohibited Uses**

Infrared badge and biometric readers shall be used for only the County business purposes identified in Section 1 of this Policy, including to control entry into SCVHHS facilities, and to control access to buildings and certain areas within buildings. Consistent with those County business purposes, the following uses shall also be permissible:

- for authorized staff to access employee data captured by badge readers if their administrative or oversight responsibilities necessitate the access based on a legitimate investigative purpose;
- for authorized County management employees to access data obtained by badge readers to assist with the safety of employees, patients, and visitors; and to assess or investigate behavior or activity that reasonably appears to be unauthorized, in violation of department or County policy, illegal, or in furtherance of illegal activity.

Unless authorized in writing by SCVHHS Department Heads or their written designees, SCVHHS employees shall use only their own badges with the badge reader system.

Unauthorized users shall not use the access-card system, the biometric fingerprint system, or the data from the systems. No one shall use those systems to access a part of the building for any purpose other than the performance of their required County job duties. Badge and biometric readers and their data shall not be used for personal, non-County-business purposes. The technologies and their data shall not be used to harass, intimidate, or discriminate against any individual or group.

### **3. Data Collection**

The badge readers shall collect the time and location of every badge, which may be associated with the specific individual badge holder. Biometric readers capture unique physical characteristics of individuals, such as an image of a single fingerprint.

### **4. Data Access**

Access to data from badge and biometric readers shall be restricted to only:

- Sheriff's Office personnel pursuant to a Memorandum of Understanding with SCVHHS;
- Protective Services Office staff (SCVHHS security personnel);
- SCVHHS Director of Facilities or written designee;
- SCVHHS Department Heads or their written designees;
- Other County personnel for County business purposes only, with written approval of the applicable SCVHHS Department Head or written designee.

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 Protection**

All data generated by badge shall be accessible to only authorized staff members and configured to prevent unauthorized modification, duplication, or destruction of the recorded images.

### **6. Data Retention**

The data collected shall be stored for no longer than two years after collection, unless required by law or County policy, or as needed for a specific County business purpose, such as a specific criminal, civil, or administrative investigation or action. Data and records stored shall be subject to County Board Policy 3.57: "Santa Clara County Record Retention and Destruction Policy." See the Countywide Surveillance Use Policy for Facility Access Control Technology.

### **7. Public Access**

Any public requests for data obtained from badge and biometric readers should be submitted to the applicable California Public Records Act (CPRA) Coordinator for handling. If a CPRA request, subpoena, or court order is issued for such data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Office of the County Counsel as needed.

## **8. Third-Party Data-Sharing**

It shall be permissible for data from badge readers to be provided to only the following: law enforcement representatives outside SCVHHS if the SCVHHS Department Head with oversight responsibility for this Policy or written designee reasonably believes that the data shows behavior or activity that appears to be unauthorized, 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; law enforcement; 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.

## **9. Training**


Personnel involved in maintaining and using the badge and biometric readers shall be appropriately trained on the use of the systems and informed of this Surveillance Use Policy.

## **10. Oversight**

SCVHHS Department Heads, security personnel, facilities management, and/or their written designee(s) shall oversee compliance with the Surveillance Use Policy.

Any employee found to have violated this Surveillance Use Policy shall be subject to possible discipline. Violations of this 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

 12/31/19  
\_\_\_\_\_  
Rob Coelho  
Office of the County Counsel