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 badge ~~and biometric~~ readers provided through a vendor, Comtel Systems, Inc. at various locations ~~for payroll purposes and~~, and biometric reads at the Public Health Department, to create a secure environment for all visitors and staff at SCVHHS facilities. Badge and/or biometric readers ~~are~~shall be used to gain entry to areas having automated access control and entry points. ~~Upon use, badge and biometric~~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. ~~Sensitive areas within buildings, including laboratory and pharmacy locations, may be accessible via a combination of electronic access card and biometric fingerprint reader. This adds an additional level of security and ensures that access is granted to only an individual to whom an access card is issued. Information obtained by these readers,~~Badge readers collect information such as 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 ~~potentially unusual, suspicious, or illegal activities~~behavior or activity that appears to be unauthorized, improper, illegal, or in furtherance of illegal activity.

2. Authorized and Prohibited Uses

Badge and biometric readers ~~are generally~~shall be used for only the County business purposes identified in Section 1 of this Policy, including to control entry into SCVHHS facilities, ~~to document employee time and attendance at work for payroll purposes,~~ and to control access to buildings and certain areas within buildings. ~~Authorized~~ Consistent with those County business purposes, the following uses shall also be permissible:

- for authorized staff ~~may~~to access ~~all~~ employee ~~information~~data captured by badge ~~and biometric~~ readers~~. SCVHHS employees may~~ if their administrative or

oversight responsibilities necessitate that access ~~their individual badge reader transactions via the Kronos Employee Self-Service (ESS) online system, the time and attendance system used by SCVHHS.~~ ;

- for authorized County management employees ~~with authorization may~~ to access ~~information~~data obtained by badge ~~and biometric~~ readers to assist with the safety of employees, patients, and visitors; and to assess or investigate ~~unusual, suspicious, or illegal~~ behavior or ~~activities~~activity that appears to be unauthorized, improper, illegal, or in furtherance of illegal activity.

Unless authorized in writing by SCVHHS Department Heads or their written designees, ~~an SCVHHS employee~~SCVHHS employees shall use only their own badges with the badge reader system. Unauthorized users shall not use ~~another employee's badge~~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 technology and its data shall not be used to harass, intimidate, or discriminate against any individual or group.

3. Data Collection

The badge ~~and biometric~~ readers shall collect ~~information about individuals, including~~ the time and location of every badge ~~and biometric fingerprint transaction.~~, 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 ~~of an employee's right index finger. Certain badge readers capture information that is stored using Kronos, SCVHHS' time and attendance collection system that is interfaced to a County payroll application.~~.

4. Data Access

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

- Sheriff's Office personnel pursuant to ~~MOU~~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;
- ~~SCVHHS Employees (information on their individual badge reader transactions for payroll purposes via Kronos only);~~
- Other County personnel for County business purposes only, with written approval of the applicable SCVHHS Department Head or written designee.

~~5. DATA STORAGE AND PROTECTION~~
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 ~~information~~data generated by badge ~~and biometric readers~~ shall be accessible to only authorized staff members and configured to prevent unauthorized modification, duplication, or destruction of the recorded images. ~~SCVHHS employees may access their individual badge reader transactions for payroll purposes via Kronos.~~

~~5.~~6. Data Retention

See the Countywide Surveillance Use Policy for Facility Access Control Technology. ~~As of April 2017, no information in the Kronos system has been deleted or destroyed.~~

~~6.~~7. Public Access

Any public requests for data obtained from badge and biometric readers should be submitted to the applicable CPRA Coordinator for handling. ~~Data may~~If a California Public Records Act (CPRA) request, subpoena, or court order is issued for such data, 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 agreement,~~ after ~~consulting~~consultation with the Office of the County Counsel as needed.

~~7.~~8. Third-Party Data-Sharing

It shall be permissible for data from badge ~~and biometric~~ readers ~~may~~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 believes that the ~~information~~data shows ~~suspicious~~behavior or ~~illegal~~ 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; 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.

~~8.~~9. Training

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

~~9.~~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 ~~may~~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

_____

Rob Coelho
Office of the County Counsel