



Surveillance Technology Policy

Call Recording,
Human Services Agency

The City and County of San Francisco values privacy and protection of San Francisco residents’ civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Call Recording itself as well as any associated data, and the protection of City and County of San Francisco residents’ civil rights and liberties.

PURPOSE AND SCOPE

The Department’s mission is:

At the San Francisco Human Services Agency, we are committed to delivering essential services that support and protect people, families, and communities. We partner with neighborhood organizations and advocate for public policies to improve well-being and economic opportunity for all San Franciscans.

The Surveillance Technology Policy (“Policy”) defines the manner in which the surveillance technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure the surveillance technology. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- <i>Authorized uses for Call Recording technology at SFHSA vary by Program:)</i>
- <i>San Francisco Benefits Network (SFBN), CalWORKs (CW), Department of Disability and Aging Services (DAS) MediCal & CalFresh Eligibility (DAS Eligibility), In-Home Supportive Services Independent Provider Assistance Center (IHSS IPAC. To collect telephonic signatures: (Telsig); and Quality Assurance (QA)</i>
- <i>To provide quality assurance: Family and Children Services (FCS)</i>
- <i>To collect evidence for use in official civil, administrative, and criminal investigations: Special Investigations Unit (SIU)</i>

Surveillance Oversight Review Dates

PSAB Review: 3/23/2023

COIT Review: TBD (list all dates at COIT, and write “Recommended: MM/DD/202X” for rec date)

Board of Supervisors Approval: TBD

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Department may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department’s mission and provides important operational value in the following ways:

Call Recording Technology helps to deliver services more efficiently. Additionally, call recording ensures that we are delivering services in an equitable manner to all citizens.

Description of Technology

Call recording technology allows our organization to record and store audio recordings from our call centers. The system is configured to monitor when call center agents are on a call and captures the conversation as an audio wav file. The audio files are stored in a secured on-premises server.

Authorized users (typically call center supervisors/manager) can log into the application to conduct quality assurance reviews of their staff's audio recordings or retrieve a needed telephonic (verbal) signature.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
<input type="checkbox"/>	Education	
<input type="checkbox"/>	Community Development	
<input type="checkbox"/>	Health	
<input type="checkbox"/>	Environment	
<input type="checkbox"/>	Criminal Justice	
<input type="checkbox"/>	Jobs	
<input type="checkbox"/>	Housing	
X	Other: Consistent and equitable service delivery, Reduced time to service delivery	The use of HSA call recording technology for telephonic signature reduces processing time by eliminating the need for obtaining an ink signature from clients, in compliance with California Assembly Bill 135. The use of call recordings for QA ensures that HSA staff provide appropriate, equitable customer service

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
X	Financial Savings	Call recording also results in financial savings by eliminating the need to print, mail and process client intake and renewal packets
X	Time Savings	Call recording at HSA eliminates the need for obtaining ink signatures (preparing packets, mailing them, receiving and processing the returned packet). Therefore HSA staff use less time on client onboarding activities.
<input type="checkbox"/>	Staff Safety	
<input type="checkbox"/>	Data Quality	
<input type="checkbox"/>	Other	

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's [Data Classification Standard](#).

The surveillance technology collects some or all of the following data type(s):

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
Voice Audio	.WAV	Level 2, 3, & 4

Notification: When clients call one of the HSA call centers, they hear a recorded announcement that calls are recorded for quality and training purposes. When an HSA call center agent calls a client, the agent, after introducing themselves, is supposed to obtain the client's consent to be recorded by stating: "Before we continue, please know that this call will be recorded for quality assurance purposes; is that all right with you?"

Department includes the following items in its public notice:

- Information on the surveillance technology
- Description of the authorized use
- Type of data collected
- Data retention
- Department identification
- Contact information

Access:

All parties requesting access must adhere to the following rules and processes:

In order to request access to the call recording system, a formal request must be approved by a senior business manager and an IT manager, and fulfilled by IT staff. The individual receiving access must complete onboarding training that includes guidelines. All those with access to call recordings are provided clear guidelines on usage and expectations on appropriate and prohibited use. For SFBN, CW, DAS Eligibility, IHSS IPAC, access to call recordings is restricted to supervisors and managers; other users of Call Recording Technology cannot access call recordings. Program Director oversees compliance, which is enforced by Section managers. All those with access to call recordings are provided clear guidelines on usage expectations. on appropriate and prohibited use. For FCS, access to call recordings is restricted and requires authorization via HSA Information Technology and Child Welfare Agency management. Access is available only to Program Directors, Program Managers, and Protective Services Supervisors of the Emergency Response Section. Access is via an application which logs all user activities (identity along with date and time of access). For SIU, staff do not have direct access to call recordings. Call recordings must be requested from the IT Information Security Office via the IT Investigations Request Form. This form requires demonstration of a legitimate business need and documents the specific case name and number associated with the requested recording. In order to request access to the call recording system, a formal request must be approved by a senior business manager and an IT manager, and fulfilled by IT staff. The individual receiving access must complete onboarding training that includes guidelines. All those with access to call recordings are provided clear guidelines on usage and expectations on appropriate and prohibited use.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- SFBN, CW, DAS Eligibility, IHSS IPAC, IT

- 2913 Program Specialist (18)
 - 2914 Social Worker Supervisor (4)
 - 2907 Eligibility Supervisor (51)
 - 2917 Program Support Analyst (3)
 - 1093 IT Operations Support Admin III (1)
 - 1094 IT Operations Support Admin IV (2)
 - 1095 IT Operation Support Admin V (1)
 - 1043 IS Engineer - Senior (1)
 - 0923 Manager II (10)
- FCS
 - 2944 Protective Services Supervisor (2)
 - 0923 Manager II (2)
 - 0932 Manager IV (1)
- SIU
 - 2913 Program Specialist (2)
 - 2966 Welfare Fraud Investigator (6)
 - 0922 Manager I (1)

B. Members of the public

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's [Open Data](#) portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also request access by submission of a request pursuant to San Francisco's [Sunshine Ordinance](#). No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Training:

To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses dictated by this policy. Department shall also require that all individuals requesting data or regularly requiring data

access receive appropriate training before being granted access to systems containing PII.

More specifically, Department training will include:

Prior to accessing call recordings, staff are provided training on how to use the application; how to listen to a recording; how to search for a recording; how to tag or save a recording. Staff are also trained on appropriate and inappropriate use. Staff in Programs who utilize call recording technology are required to take an annual Technology and Confidentiality training. Calls are reviewed to ensure call quality and adherence to privacy and technology policies

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

Department shall ensure compliance with these security standards through the following:

Access to call recording system is controlled with strong passwords. Audits are completed quarterly by IT to ensure that only authorized personnel have accounts in the application. Furthermore, transmission of voice call data between the telephony system and the call recording system takes place entirely within a secured local area network (LAN) in an on-premise HSA datacenter. Transmission of recordings from the system servers to individual workstations (for listening or download) is secured by use of TLS encryption. Data at rest on the voice recording system is protected by logical controls restricting access to authorized user IDs that have provided strong username-password authentication. Individual recordings that have been downloaded to user workstations are protected by operating system filesystem access controls as well as full disk encryption using federal standards for encryption algorithms. Network controls prevent access to the voice recording system using unauthorized (non-agency) workstations or devices.

Data Storage: Data will be stored in the following location:

- Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)
- Department of Technology Data Center
- Software as a Service Product

☐ Cloud Storage Provider

Data Sharing: Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (*See Data Security*)

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- Confirm the purpose of the data sharing aligns with the department's mission.

- Consider alternative methods other than sharing data that can accomplish the same purpose.

- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.

- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

A. Internal Data Sharing:

The department shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
-----------	----------------

<p>SFBN, CW, DAS Eligibility, IHSS IPAC: For regular business operations, these Programs do not share call recordings with any other departments inside the City and County of San Francisco. As part of official investigative activities, these Programs' call recordings may be shared with other CCSF department; see the SIU section for details.</p> <p>FCS: For regular business operations, FCS staff do not share call recordings with any other departments inside the City and County of San Francisco. As part of official investigative activities, FCS call recordings may be shared with other CCSF department; see the SIU section for details.</p> <p>SIU: As part of official investigative activities, call recording audio files may be shared with other CCSF department; Recordings may be shared with other CCSF department; see the SIU section for details.</p>	<p>SFBN, CW, DAS Eligibility, IHSS IPAC: For regular business operations, these Programs do not share call recordings with any other departments inside the City and County of San Francisco. Special Investigation Unit may share these Programs' call recordings, and sheriff's department as part of official investigative activities.</p> <p>FCS: For regular business operations, FCS staff do not share call recordings with any other departments inside the City and County of San Francisco. Special Investigation Unit may share FCS call recordings as part of official investigative activities.</p> <p>SIU: As part of investigations, call recordings may be shared with the district attorney's office, police department, and sheriff's department. None of these Programs share any call recordings with other City departments; exceptions are handled by SIU.</p>
--	---

Frequency - Data sharing occurs at the following frequency:

SFBN, CW, DAS Eligibility, IHSS IPAC: For regular business operations, these Programs do not share call recordings with any other departments inside the City and County of San Francisco. As part of official investigative activities, these Programs' call recordings may be shared with other CCSF department; see the SIU section for details.

FCS: For regular business operations, FCS staff do not share call recordings with any other departments inside the City and County of San Francisco. As part of official investigative activities, FCS call recordings may be shared with other CCSF department; see the SIU section for details;

SIU: Call recordings are infrequently shared with other CCSF departments, and only when necessary as part of an official civil, administrative, or criminal investigation. None the Programs share call recordings; SIU handles any sharing of data with

other City departments. Recordings may be shared with other CCSF department; see the SIU section for details.

B. External Data Sharing:

The department shares the following data with recipients external to the City and County of San Francisco:

Data Type	Data Recipient
<p>SFBN, CW, DAS Eligibility, IHSS IPAC: For regular business operations, none of these Programs share call recordings with any outside entities. As part of official investigative activities, these Programs' call recordings may be shared with outside entities; see the SIU section for details.</p> <p>FCS: For regular business operations, FCS staff do not share call recordings with any outside entities. As part of official investigative activities, FCS call recordings may be shared with outside entities; see the SIU section for details.</p> <p>SIU: As part of investigations, call recordings may be shared with the district attorney's office, police department, and sheriff's department in other counties. Programs do not share call recordings with outside entities. SIU handles any external sharing when needed; see the SIU section for details.</p>	<p>SFBN, CW, DAS Eligibility, IHSS IPAC: For regular business operations, none of these Programs share call recordings with any outside entities. As part of official investigative activities, these Programs' call recordings may be shared with outside entities; see the SIU section for details.</p> <p>FCS: For regular business operations, FCS staff do not share call recordings with any outside entities. As part of official investigative activities, FCS call recordings may be shared with outside entities; see the SIU section for details.</p> <p>SIU: As part of investigations, call recordings may be shared with the district attorney's office, police department, and sheriff's department in other counties. Programs do not share call recordings with outside entities. SIU handles any external sharing when needed; see the SIU section for details.</p>

Frequency - Data sharing occurs at the following frequency:

Programs do not share call recordings; SIU handles sharing of call recordings, when needed.

SIU: Call recordings are rarely shared with outside entities, only when necessary as part of an official civil, administrative, or criminal investigation.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

The Department’s data retention period and justification are as follows:

Retention Period	Retention Justification
Federal regulations, 45 Code of Federal Regulations 164.3161 and 45 Code of Federal Regulations 164.5282, set the retention requirement for case information at 6 years following case closure. There are exceptions that require case information to be retained for longer periods.	The retention period is established in compliance with Federal and State regulations

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Exceptions to the retention period include when there is an open federal or state audit, when criminal or civil litigation is involved, or for public records requests under the Sunshine Ordinance.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Practices: Call Recording
- Processes and Applications: On a quarterly basis, a report will be automatically generated from HSA’s business intelligence systems that identifies cases that have reached the end of their retention period. The report will contain external phone numbers associated with each case, along with start and end dates the phone number was associated with that case. Authorized HSA IT staff will run an application procedure in the call

recording system to delete calls matching the criteria in the report (calls within date range to/from external phone number).

COMPLIANCE

Department Compliance

Department shall oversee and enforce compliance with this Policy using the following methods:

SFBN, CW, DAS Eligibility, IHSS IPAC: Access to call recordings is restricted to supervisors and managers; other users of Call Recording Technology cannot access call recordings. Program Director oversees compliance, which is enforced by Section managers. All those with access to call recordings are provided clear guidelines on usage expectations.

FCS: Access to call recordings is restricted and requires authorization via HSA Information Technology and Child Welfare Agency management. Access is available only to Program Directors, Program Managers, and Protective Services Supervisors of the Emergency Response Section. Access is via an application which logs all user activities (identity along with date and time of access).

SIU: SIU staff do not have direct access to call recordings. Call recordings must be requested from the IT Information Security Office via the IT Investigations Request Form. This form requires demonstration of a legitimate business need and documents the specific case name and number associated with the requested recording.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

SFBN, CW, DAS Eligibility, IHSS IPAC

For regular business operations, none of these Programs share call recordings with other entities (internal and external). As part of official investigative activities, these Programs' call recordings may be shared with other entities; see the SIU section for details.

FCS

For regular business operations, FCS staff do not share call recordings with any other entities (internal and external). As part of official investigative activities, FCS call recordings may be shared with outside entities; see the SIU section for details.

SIU

Any entity receiving call recordings will do so on a need-to-know basis as part of an official civil, administrative, or criminal investigation.

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.

- BN, CW, DAS Eligibility, IHSS IPAC
 - 0922 Manager I
 - 0923 Manager II
 - 0931 Manager III
 - 0932 Manager IV
- FCS
 - 0932 Program Director
 - 0923 Program Manager
- SIU
 - 0922 Manager I
 - 0932 Manager IV

Sanctions for Violations

Sanctions for violations of this Policy include the following:

SFBN, CW, DAS Eligibility, IHSS IPAC

First Offense: Verbal warning delivered by immediate manager or supervisor.

Second Offense: Written warning. An email or letter is sent to the individual, reminding them of a prior verbal warning about improper use of call recordings, and consequences of a third offense.

Third Offense: Administrative action. Under the guidance of HSA Personnel Department, possible suspension (days of unpaid leave) or revocation of access to the Call Recording Technology.

FCS

Based on the employment status of the person violating the Surveillance Technology Policy and the impact to confidentiality, the response to any violation could range from counseling to dismissal. As a basic guideline, the response falls within the framework described below.

First Offense: Staff who use the platform inappropriately will receive initial counseling on appropriate use of call recordings. The Emergency Response management team will also send periodic reminders to staff on best practices regarding appropriate use.

Second Offense: In consultation with HSA Human Resources a progressive discipline response will be developed up to and including a 3 month probationary period with decreased access and increased monitoring.

Third Offense: In consultation with HSA Human Resources a progressive discipline response will be developed up to and including termination of employment or involuntary reassignment. Additional sanctions for violations of policy will be taken in accordance with the Human Services Agency Discipline Policy and Procedures, as described in section 9-13 of the Human Services Agency Personnel Procedures Handbook.

SIU

First Offense: Verbal warning delivered by immediate manager or supervisor.

Second Offense: Written warning. An email or letter is sent to the individual, reminding them of a prior verbal warning about improper use of call recordings, and consequences of a third offense.

Third Offense: Administrative action. Under the guidance of HSA Personnel Department, possible suspension (days of unpaid leave) or revocation of access to the Call Recording Technology.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Raw Data: Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.

Exigent Circumstances: An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Public Inquiries

SFBN, CW, DAS Eligibility, IHSS IPAC

SFBN

Hotline: (415) 558-4700

Fax (415) 355-2300

Service Center Locations:

1235 Mission St, San Francisco CA 94103

1440 Harrison St, San Francisco CA 94103

Email Address: Food@sfgov.org or SFMedi-Cal@sfgov.org

Postal Address: SFHSA, P.O. Box 7988, San Francisco, CA 94120

CalWORKS

Hotline: (415) 557-5100

Fax: (415) 557-5478

Service Center Locations:

170 Otis St, San Francisco CA 94103

3120 Mission St, San Francisco CA 94110

801 Turk St, San Francisco CA 94102

Email Address: calworks@sfgov.org

Postal Address: SFHSA, P.O. Box 7988, San Francisco, CA 94120-7988

DAS Eligibility

Hotline: (415) 557-6555

Service Center Location:

2 Gough St. San Francisco Ca 94103

IHSS IPAC

Hotline: (415) 557-6200

Fax: (415) 557-5481

Service Center Location:

2 Gough St. San Francisco Ca 94103

Email Address: ihss@sfgov.org

Postal Address: SFHSA, Attn: 2350, P.O. Box 7988, San Francisco, CA 94120

FCS

Members of the public can register complaints or concerns with the HSA Ombudsperson at (415) 558-2828 or by email, todd.wright@sfgov.org.

SIU

Complaints and concerns reg. SIU use of call recordings can be submitted via email to HSASIU@sfgov.org or by contacting Bunyan Johnson: bunyan.johnson@sfgov.org or (415) 503-4823.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

SFBN, CW, DAS Eligibility, IHSS IPAC

Supervisors are expected to respond to all calls and emails within 1 business day. Since a manager review would also be required for misuse of this technology, the Manager's response needs to happen within 1-2 business days of the report.

FCS

The HSA Ombudsperson is contracted to provide independent response to complaints or concerns including tracking of concerns from initial contact to resolution within 2 business days.

SIU

An SIU manager would review reports of alleged misuse of call recordings and respond within 2 business days of receipt of the report.

Inquiries from City and County of San Francisco Employees

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.