FIRST 5 SAN BERNARDINO	Number 18-01
	Effective 05-09-18
	Page 1 of 7
NON-PUBLIC PERSONALLY IDENTIFIABLE INFORMATION	Approved:  **Chair**

PURPOSE

There are numerous policies within the County of San Bernardino Human Services Department (HS) regarding confidentiality. Personally Identifiable Information (PII), and Personal Health Information (PHI) of which First 5 San Bernardino (F5SB) aligns with when applicable. However, this policy outlines F5SB's Non-Public Personally Identifiable Information practices which aligns with federal and state mandates regarding any/all confidential information maintained by F5SB electronically or in paper format, which can potentially be used to uniquely identify, contact, or locate members of the public.

The protection of confidential information is not specific to PII and/or PHI, but covers more of a broad spectrum of information/data utilized to administer F5SB initiatives. Therefore, F5SB staff shall adhere to this policy in conjunction with:

- San Bernardino County Personnel Rules
- Standards for Employee Conduct
- HS Policy and Standard Practice (HSPSP) Manual Section 15
- Department/Division policies/procedures

POLICY

All client/customer information is strictly confidential. Such information may be contained in verbal, printed, electronic or any other identifiable form or record. Confidential information includes, but is not limited to:

- Name
- Social Security Number
- Physical description
- Contact information (home address, telephone number, e-mail address, etc.)
- Financial matters
- Public benefit status
- Medical
- Employment
- Criminal history information and/or
- Any other information deemed to be confidential as per department requirements.

F5SB staff, contractors, volunteers, and others granted authorized access to confidential information are responsible for protecting/securing the information, having knowledge of, and being in compliance with, this policy.

The term "non-public personally identifiable information" as used in this policy is any piece of information maintained by the F5SB electronically or in paper format, which can potentially be used to uniquely identify, contact, or locate F5SB employees or members of the public. Examples are information, such as but not limited to, social security numbers, driver's license numbers, financial and health information that is not subject to disclosure under the Public Records Act, Government Code Section 6250 *et seq.*

POLICY AMPLIFICATION

To prevent loss or fraudulent use, it is the responsibility of every F5SB officer, employee, agent and volunteer to preserve the integrity, security and confidentiality of non-public personally identifiable information received, collected, stored or transmitted. Therefore, all departments and divisions shall establish and implement policies and procedures for protecting the integrity, security and confidentiality of non-public personally identifiable information received, collected, stored and transmitted within their respective department or division.

GUIDELINES

This standard practice contains the following topics:

General Requirements

INTRODUCTION

Confidential information used to conduct F5SB business requires appropriate safeguards to protect from accidental/deliberate misuse, disclosure, damage, or loss. F5SB departments/divisions must ensure confidential information is only accessed by or disclosed to authorized staff/persons that have a legal/reasonable need to know in order to perform/administer their assigned program. This section outlines the confidentiality requirements for all F5SB departments/divisions.

MANAGER/ SUPERVISOR responsibilities

F5SB Managers/Supervisors have the responsibility to ensure confidential information is protected and secured at all times. Managers/Supervisors need to be aware of the risks and potential consequences of confidentiality breaches, and must be committed in their efforts to uphold the integrity of the individual's confidentiality, leading by example through their own adherence to these requirements.

Managers shall:

- Monitor workplace practices to ensure confidential information is protected and secured at all times.
- Ensure staff is aware of and comply with all confidentiality requirements.
- Limit and control employee access to confidential information to the minimal amount needed to perform the assigned job function.
- Immediately mitigate and deal firmly with breaches of confidentiality.
- Seek advice from County Counsel whenever uncertain whether or not information should be released and how it is to be released.

Continued on next page

General Requirements, Continued

STAFF responsibilities

F5SB staff must be diligent in their efforts to protect/secure the confidentiality of client's/customer's information. All staff, volunteers, and those granted access to F5SB resources must adhere to the following:

- Only access confidential information as necessary to perform a job function, activity, or service directly related to the administration of F5SB initiatives.
- Never access confidential information for personal use, family, or friends.
- Secure confidential information, do not leave unattended on desks or in unsecured areas.
- Secure printed documents containing confidential information from inappropriate access, not leaving on printers, fax machines, or copiers.
- Not release any confidential information to an unauthorized person or agency without written authorization from the customer or service recipient, or approval from a supervisor, manager, County Counsel, or court order.
- Dispose of confidential information in locked shred containers only (individual shred boxes prohibited).
- Do not access/send confidential information from communication devices (Laptop, Personal Digital Assistant (PDA), or any other handheld/mobile information technology device) unless proper access control mechanisms are in place and approved by department/division management.
- Report all actual or suspected breaches of confidentiality to department/division manager or supervisor.

Access to Confidential Information

INTRODUCTION

To ensure confidential information is protected and secured, F5SB departments/divisions shall have adequate security measures in place. These measures shall include, but are not limited to, the use of passwords and access controls to protect the security of the information from unauthorized staff/persons.

ACCESSING INFORMATION

Access to confidential information must only be authorized on a "need-to-know" basis and not merely by position or title. HS departments/divisions must ensure access to confidential information is only granted to staff that require the information to administer a F5SB initiative.

Managers/Supervisors are responsible for requesting the appropriate level of access for their staff and must ensure the minimum necessary access is requested for the assigned job functions. When access to confidential information and computer system(s) is no longer required, authorization must be terminated immediately.

INAPPROPRIATE ACCESS

Inappropriate access is taken very seriously within F5SB. Staff shall not access, view, or otherwise review any information pertaining to:

- Their own case/record, nor shall staff review any information pertaining to a relative, friend or acquaintance.
- Any case/record in which the staff person does not have a need to know in order to complete his/her assigned duties.
- Any access, discussion, and/or questions regarding an employee's own case/record shall only be conducted by the appropriate assigned worker or other person as designated by the appointing authority. This type of inquiry should not be conducted on F5SB time. If an employee is uncertain with whom to inquire, questions should be directed to their manager/supervisor.
- A breach of confidentiality, whether intended or done negligently, may result in disciplinary action (including termination from employment), criminal penalties, and/or civil liability.

Release of Confidential Information

INTRODUCTION

Federal, state and county regulatory guidelines were created to protect the customer from identification, exploitation or embarrassment that could result from the release of information identifying them as having applied for or having received public assistance. This section outlines confidentiality requirements; however, due to the uniqueness and complexity of the various programs, staff should refer to department policy/procedures for appropriate release specific to their administered human service program.

INFORMATION SHARING

Confidential information shall not be discussed or exchanged between staff, except for legitimate business purposes or otherwise permitted by law. Such discussion or exchange of information must occur in confidential surroundings, for legitimate consultation purposes only.

Customer privacy must be maintained to the fullest extent possible. F5SB staff must consult with their manager/supervisor prior to releasing confidential information. All requests for information, including subpoenas and public records requests must **immediately** be forwarded to a manager/supervisor. Managers/Supervisors are responsible for forwarding such requests to the departments/divisions custodian of records or County Counsel.

RELEASE OF INFORMATION WITH CONSENT

A client/customer has the right to receive factual information relating to eligibility provided solely by the client/customer contained in any applications and records kept by F5SB. No information may be provided through telephone or other electronic medium without first verifying the identity of the person to whom the information is provided, and that he/she is authorized to receive such information. Use a combination of the following to confirm a customer's identity:

- Driver's License Number
- Identification (ID) Number
- Last four (4) of Social Security Number (SSN)
- Date of Birth (DOB)
- Case number
- Address

A client's/customer's confidential information can be released to an authorized representative when a written, signed and dated authorization has been obtained. An authorized representative is a person or group who has authorization from the customer to act on their behalf. Written consent or authorizations for release of information shall be dated and shall expire one year from the date given unless a shorter time period is specified.

Continued on next page

Release of Confidential Information, Continued

RELEASE OF INFORMATION WITHOUT CONSENT

Confidential information may be released for purposes of administration of a human service program. This allowable flow of information applies to any aid or services administered or supervised by:

- County Welfare Departments
- F5SB and/or HS contractors
- California Department of Social Services (CDSS)
- Department of Health Care Services (DHCS)
- Department of Health and Human Services (HHS)
- Social Security Administration (SSA)
- Federal, State, and F5SB Auditors (performing fiscal audits or procedural reviews to determine if fiscal accountability is being maintained)
- Legislative committees (authorized by law to audit records)

TRAINING

If cases are used for departmental authorized training, no confidential information may be identifiable through either written or verbal materials.

CONTRACT PROVISIONS

Whenever a contract or Memoranda of Understanding (MOU) is entered into with a public or private agency which involves the release of confidential information, the contract shall contain a provision insuring the information will only be used in accordance with the administration of a human service program.

Transmission of Confidential Information

INTRODUCTION

F5SB departments/division must take reasonable measures to ensure confidential information is transmitted appropriately to the receiving party and that there is a legitimate need for the information requested. This section outlines security measures that F5SB staff must adhere to when transmitting confidential information over an electronic communications network.

E-MAIL CONFIDENTIALITY REQUIREMENTS

To avoid release of confidential information to an unauthorized person, or when sending confidential information outside of the F5SB network, no identifying information should be included in the subject line or body of an e-mail.

It is suggested a unique identifier (de-identification) to the confidential information be utilized such that a client/customer cannot be identified. Only as necessary, should confidential information be included in the subject line or body of an e-mail in **one** of the following manners:

- First name (with last name initial)
- Last name only
- Case number
- Any other identifying number

ATTACHMENTS

Any additional client/customer information that is being e-mailed must be transmitted in a Word, PDF document, or Item that is attached to the e-mail and not displayed in the body of the e-mail.

FAXING

A universal F5SB Fax Coversheet has been developed to ensure all out-going faxes include a statement of confidentiality. This fax coversheet shall be used when faxing confidential information.

The coversheet is available in the F5SB shared drive. Staff shall adhere to the following requirements regarding faxing. Fax machines:

- Must be kept in secured areas where information is not available to unauthorized persons, including unauthorized staff.
- Confidential transmission must not be left unattended.
- Fax numbers must be verified with the intended recipient prior to sending.
- Receipt of transmission must be verified with the intended recipient (when possible).