



# Privacy and Security Contractor Requirements Summary

PDD:MP:LP (11/14)



**Human Services**

[www.SBCounty.gov](http://www.SBCounty.gov)

# Privacy and Security Contractor Requirements Summary

## Table of Contents

Section	Description	Page
1	Definitions	3
2	Disclosure Requirements	3
3	Training	3
4	Oversight	4
5	Physical Security	4
6	Computer Safeguards	4
7	System Security Controls	4
8	Audit Controls	5
9	Paper Document Controls	5
10	Breaches and Personally Identifiable Information (PII)	5
11	Compliance by Contractor	6
12	Assessments and Reviews	7
13	Assistance in Litigation	7

## 1. Definitions

- a) Personally Identifiable Information (PII) – Information that can be used alone, or in conjunction with any other information, to identify a specific individual. Personally Identifiable Information includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper.

## 2. Disclosure Requirements

- a) Contractor and its employees and volunteers may only use or disclose PII to perform functions, activities or services directly related to carrying out the provisions of this Agreement.
- b) Contractor and its employees and volunteers shall protect from unauthorized use or disclosure all PII.
- c) Contractor shall promptly transmit to the County all requests for disclosure of any PII not authorized by this Agreement.
- d) Access to PII shall be restricted to only those employees and/or volunteers of Contractor who need the PII to perform their official duties in connection with carrying out the provisions of this Agreement.
- e) Any person, who acquires, accesses, discloses or uses PII in a manner or for a purpose not in connection with this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

## 3. Training

Contractor agrees to:

- a) Advise all employees and volunteers who have access to PII of the confidentiality of the information, the safeguards required to protect the information, and the possibility of civil and criminal sanctions for failure to safeguard the information.
- b) Train and use reasonable measures to ensure compliance with the privacy and security requirements of this Agreement by all employees and volunteers who assist in carrying out the provisions of this Agreement.
- c) Ensure new employees and volunteers complete a privacy and security awareness training within 30 days of hire and prior to accessing PII. Contractor must also provide an annual refresher in addition to ongoing reminders on privacy and security safeguards thereafter to all employees and volunteers.
- d) Maintain records indicating each employee's and/or volunteer's name and the date on which the initial privacy and security awareness training was completed.
- e) Retain training records for inspection for a period of three years after completion of the training.
- f) Ensure all employees and volunteers, who access, use or disclose PII to carry out the provisions of this Agreement sign a confidentiality statement prior to accessing PII. The confidentiality statement shall include at a minimum general use, security and privacy safeguards, unacceptable use, and enforcement policies.

## 4. Oversight

Contractor agrees to:

- a) Establish and maintain ongoing management oversight and quality assurance for monitoring compliance with the privacy and security safeguards regarding PII in this Agreement.
- b) Management oversight and monitoring activities must be performed by an employee or volunteer whose job function is separate from those who use or disclose PII as part of their routine duties.

## 5. Physical Security

Contractor agrees to:

- a) Access and store PII in an area that is physically safe from access by unauthorized persons during working and non-working hours.
- b) Secure all areas where PII is stored must only be accessed by authorized individuals with coded key cards, door keys or access authorization.
- c) Store paper records containing PII in a locked space, such as a locked file cabinet, locked file room, locked desk or locked office whenever information is housed with or a location is shared with another business.

## 6. Computer Safeguards

Contractor agrees to:

- a) Encrypt mobile devices, workstations and electronic files where PII is stored using a FIPS 140-2 certified algorithm bit or higher.
- b) Ensure minimum necessary amount of PII is downloaded to a mobile device hard drive when absolutely necessary for current business purposes.
- c) Ensure emails sent outside the Contractor's email environment that include PII are sent via an encrypted method using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution.
- d) Have a commercial third-party virus software solution for all workstations, laptops and other systems that process and/or store PII. The commercial third-party virus software must be updated when a new anti-virus definition/software release is available.
- e) Ensure workstations, laptops and other systems that process and/or store PII have current security patches applied and are up-to-date.
- f) PII is wiped from systems when the data is no longer legally required.

## 7. System Security Controls

Contractor agrees to ensure all systems containing PII:

- a) Provide an automatic timeout after no more than 20 minutes of inactivity.
- b) Display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User shall be directed to log off the system if they do not agree with these requirements.

## 8. Audit Controls

Contractor agrees to ensure all systems processing and/or storing PII have:

- a) At least an annual system security review, which shall include administrative and technical vulnerability assessments.
- b) An automated trail, which includes the initiator of the request, along with a time and date stamp for each access. These logs must be read only and maintained for three years. A routine procedure must be in place to review system logs for unauthorized access. Contractor shall investigate anomalies identified by interviewing employees and/or volunteers and witnesses and taking corrective action, including discipline, when necessary.
- c) A documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

## 9. Paper Document Controls

Contractor agrees to:

- a) Dispose of PII in paper form through confidential means, such as cross cut shredding and pulverizing.
- b) Not remove PII from the premises of Contractor, except for routine business purposes or with express written permission of the County.
- c) Send an encryption test email to [EncryptionCheck@hss.sbcounty.gov](mailto:EncryptionCheck@hss.sbcounty.gov) prior to providing services.
- d) Not leave faxes containing PII unattended and keep fax machines in secure areas. All faxes must contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers must be verified with the intended recipient before a fax is sent.
- e) Use a bonded courier with signature receipt must be when sending large volumes of PII (500 or more records containing PII). All disks and other transportable media sent through the mail must be encrypted using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution.

## 10. Assessments and Reviews

In order to enforce this Agreement and ensure compliance with its provisions, Contractor agrees to allow the County to inspect facilities, systems, books and records of the Contractor, in order to perform assessments and reviews. Such inspections shall occur at times that take into account the operational and staffing demands of Contractor.

## 11. Breaches of Personally Identifiable Information

### A. *Discovery and Notification of Breach*

- I. Contractor shall notify the County HS Privacy and Security Officer immediately by telephone at (909) 383-9665 and email at [HSPrivacySecurityOfficer@hss.sbcounty.gov](mailto:HSPrivacySecurityOfficer@hss.sbcounty.gov) upon the discovery of a suspected or actual breach of security of PII.
  - i. A breach of PII includes the acquisition, access, use, or disclosure of PII in a manner not permitted by this Agreement which compromises the security or privacy of the PII.
  - ii. The initial notification must include contact and component information; a description of the breach or loss with scope, number of files or records; type of equipment or media; approximate time and location of breach or loss; description of how the data was physically stored, contained or packaged (e.g. password protected, encrypted, locked briefcase, etc.); whether any individuals or external organizations have been contacted; and whether any other reports have been filed.
- II. Contractor shall take:
  - i. Prompt corrective action to mitigate any risks or damages involved with the actual or suspected breach and to protect the operating environment.
  - ii. Any action pertaining to such unauthorized disclosure requirement by applicable federal and state laws and regulations.

### B. *Investigation of Breach/Written Report*

- I. Contractor shall immediately investigate such breach and within five working days of the incident, produce a written report detailing:
  - i. Specific data elements involved and the extent of the data involved in the breach;
  - ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PII;
  - iii. A description of where PII is believed to have been improperly transmitted, sent, or used;
  - iv. A description of the probable causes of the breach; and,
  - v. A detailed corrective action plan including measures that were taken to halt and/or contain the breach.

## 12. Compliance by Contractor

Contractor shall require that any agents or subcontractors which assist in carrying out the provisions of this Agreement and to which Contractor provides PII agree to the same privacy and security safeguards as are contained in this Agreement, and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract to such agents or subcontractors.

## 13. Assistance in Litigation

In the event of litigation or administrative proceedings involving the County or the State based upon claimed violations by Contractor of the privacy and security of PII or federal or state laws or agreements concerning privacy or security of PII, Contractor shall make all reasonable efforts to make itself and any subcontractors, agents, employees and volunteers assisting in carrying out the provisions of this Agreement and using or disclosing PII available to the County or the State at no cost to the County or the State to testify as witnesses. The County shall also make all reasonable efforts to make itself and any agents and employees available to Contractor at no cost to Contractor to testify as witnesses, in the event of litigation or administrative proceedings involving Contractor based upon a claimed violation by the County of the privacy or security of PII, or state or federal laws or agreements concerning privacy and security of PII.