SAN BERNARDINO COUNTY
Human Services

Human Services
Privacy and Security
Contractor Requirements Summary

Human Services
Privacy and Security
Contractor Requirements Summary

Table of Contents

Privacy and Security Contractor Requirements Summary

1. **Definitions**

   Contractor – For the purpose of this document, “contractor” refers to contractor, contractor’s employees and volunteers.

   Personally Identifiable Information (PII) – Information that can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual, or can be used to access their file. PII may be electronic, paper, verbal or recorded. PII includes, but is not limited to:

   a) Name,
   b) Social Security Number (SSN),
   c) Date of birth,
   d) Address,
   e) Photo Identification,
   f) Driver’s License,
   g) Biometric record,
   h) Place of birth,
   i) Mother’s maiden name, and
   j) Identifying number/document (i.e. Case number, Client Index Number (CIN), etc.)

2. **Disclosure Requirements**

   Contractor agrees to:

   a) Use and disclose PII to perform functions, activities or services directly related to carrying out the provisions in your contract.
   b) Protect PII from all threats of misuse, disclosure, damage or loss.
   c) Not duplicate and disclose PII without written approval from the County. Promptly transmit to the County all requests for disclosure of any PII not authorized by this document.
   d) Restrict PII access only to those employees and/or volunteers of Contractor who need the PII to perform their official duties in connection with carrying out the provisions of your contract.
   e) Limit access to authorized personnel based on the least set of privileges needed to perform job duties within their scope, ensuring separation of duties to reduce risks, conflict of interest, fraud, abuse etc.
   g) Report to the County of any person who acquires, accesses, discloses or uses PII in a manner or for a purpose not authorized in this document.
   h) Non-disclosure agreement signed by personnel who dispose/destroy case files or other print media.

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, operating procedures, 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 outlined in this document by all employees and volunteers who assist in carrying out the provisions of this document.
   c) Ensure new employees and volunteers complete the County’s mandatory Privacy and Security Training for Contractors/Service Providers within **30 days of hire** and prior to accessing PII. Thereafter, Contractor must also provide **annual** refresher

training or three or more reminders per year of the privacy and security safeguards outlined in this document to all employees and volunteers.

d) Maintain training records that include employee name and date training was completed.

e) Retain training records for inspection for a period of **three (3) years** after completion of the training.

f) Ensure all employees and volunteers, who access, use or disclose PII carry out the provisions outlined in this document, and sign the County's confidentiality statement prior to accessing PII.

4. **Confidentiality Statement**

Contractor agrees to ensure all staff, including volunteers, sign the County's Confidentiality statement prior to accessing PII and annually thereafter. The signed statement shall be retained for a period of **three (3)** years following the conclusion of employment.

5. **Background Check**

Contractor agrees to:

a) Conduct a background screening of all employees/volunteers before they may access PII.

b) Conduct screening commensurate with the appropriate level of access granted to perform administrative functions according to position or title.

c) Retain background screening documentation for **three (3) years** following the conclusion of employment.

6. **Management Oversight and Monitoring**

Contractor agrees to:

a) Establish and maintain ongoing management oversight and quality assurance including random sampling of work product, for monitoring compliance with the PII privacy and security safeguards outlined in this document. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.

b) Management oversight and monitoring activities must be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the use or disclosure of PII.

7. **Information Security and Privacy Staffing**

Contractor agrees to:

a) Designate staff who are accountable for compliance with these and all other requirements stated in this document.

b) Assign staff to be responsible for administration and monitoring of all security related controls stated in this document.

8. **Physical Security**

Contractor agrees to:

a) Use and store PII in an area that is physically safe from access by unauthorized persons at all times.

b) Secure all areas where PII is stored and restrict access to authorized individuals by using one or more of the following:

- Properly coded key cards,

- Authorized door keys, and
- Official Identification.

c) Issue identification badges to all staff and require staff to wear these badges where PII is used, disclosed, or stored.

d) Ensure paper records containing PII are locked when unattended at any time and stored in locked spaces such as locked file cabinets, file rooms, desks or offices.

e) Have written policies that prohibit staff from leaving PII records unattended/unsecured at any time in a vehicle unless secured in the trunk, but never overnight, or for extended periods of time.

f) Have written policies that prohibit staff from leaving PII records unattended at any time in airplanes, buses, trains, etc., including baggage areas.

g) Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

h) Ensure there are security guards or monitored alarm system at all times at the facility where 500 or more individually identifiable records of PII is used, disclosed or stored. (Exhibit B, p 10 and PSA p. 6, letter F).

i) Ensure each physical location, where PII is used, disclosed or stored has procedures and controls that ensure an individual whose access to the facility is terminated is promptly escorted from the facility by an authorized employee and access is revoked.

j) Ensure data centers with servers, data storage devices and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized staff. Visitors to the data center area must be escorted at all time by authorized staff.

9. **Technical Security Controls**

Contractor agrees to:

a) Encrypt mobile devices, workstations and electronic files where PII is used, stored and/or processed using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk.

b) Ensure only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded or exported to a mobile device hard drive.

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 anti-virus software solution for all workstations, laptops and other systems that process and/or store PII. The commercial third-party anti-virus software should have automatic updates for definitions scheduled at least daily.

e) Ensure workstations, laptops and other systems that process and/or store PII have critical security patches applied, with system reboot if necessary and are updated regularly.

f) When data is no longer legally required, all PII must be cleared, purged, or destroyed consistent with National Institute of Standards and Technology (NIST) SP 800-88, Guidelines for Media Sanitization, such that PII cannot be retrieved.

10. **User ID and Password Controls**

Contractor agrees to:

a) Issue all users a unique user name for accessing PII. Promptly disable, delete, or change the password within 24 hours of the transfer or termination of an employee. **Note**: Twenty-four (24) hours is defined as one (1) working day.

b) Passwords:
- Are not to be shared.
- Must be a non-dictionary word.
- Must not be stored in readable format on the computer or server.
- Must be changed at minimum of every 90 days or less, or if revealed or compromised.

c) Must be at least eight characters composed from at least three (3) of the following four (4) groups from the standard keyboard:
1) Upper case letters (A-Z)
2) Lower case letters (a-z)
3) Arabic numerals (0-9)
4) Special characters (!,@,#, etc.)

11. **System Security Controls**

Contractor agrees to:

a) Provide an automatic timeout, requiring re-authentication of the user session 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, by authorized users. User shall be directed to log off the system immediately if they do not agree with these requirements.

c) Have a logical control feature for unsuccessful login attempts, no fewer than three and no greater than five.

d) Designate a specific individual to issue PINs, passwords, credentials, etc.

e) Obtain a non-disclosure statement from vendor when sending a computer, hard drive, or other computing or storage device offsite for repair.

f) Remove information from electronic devices before sending to an external vendor for service or when donating, selling or placing equipment with another organization.

g) Ensure PII is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in a geographic or virtual area not subject to U.S. law.

12. **System Logging**

Contractor agrees:

a) The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.

b) To restrict the automated trail to authorized users, which includes the initiator of the request, along with a time and date stamp for each access and log both successful and failed accesses. These logs must be read-access only and maintained for three years from the date of occurrence.

c) To enable database logging functionality if PII is stored in a database.

13. **Audit Controls**

Contractor agrees to implement the following audit control mechanisms:

a) At least an annual system risk assessment/security review that ensures administrative, physical and technical controls are functioning effectively and provide an adequate level of protection.

b) Reviews should include vulnerability scanning tools.

c) A process or automated procedure to review system logs for unauthorized access.

d) A process for investigating and reporting to the County anomalies identified by interviewing employees and/or volunteers and witnesses and taking corrective action, including discipline, when necessary.

e) A documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

14. **Paper Document Controls**

Contractor agrees to:

a) Dispose of PII in paper form through confidential means, such as Cross-cut shredding or pulverizing.

b) Escort visitors in areas where PII is contained, and keep PII out of sight while visitors are in the area.

c) Send an encryption test email to EncryptionCheck@hss.sbcounty.gov prior to providing services.

d) Not remove PII from the premises of Contractor, except for routine business purposes or with express written permission from the County.

e) Do not leave faxes containing PII unattended and keep fax machines in secure areas away from unauthorized persons, including unauthorized staff. 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.

f) Seal and secure mailings containing PII from damage or inappropriate viewing of PII to the extent possible.

g) Use a secure courier and tracking method that includes verification of delivery and receipt when mailing 500 or more individually identifiable records containing PII in a single package.

h) Encrypt all disks and other transportable media sent through the mail using the County's approved encryption solution.

15. **Emergency Plan**

Contractor agrees to establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency.

16. **Assessments and Reviews**

Contractor agrees to allow the County to inspect facilities, systems, books and records of the Contractor, with reasonable notice from the County, in order to perform assessments and reviews. Such inspections shall occur at times that take into account the operational and staffing demands of Contractor.

17. **Breaches of Personally Identifiable Information (PII)**

a) **Discovery and Notification of Breach** - Contractor shall notify the County HS Privacy and Security Officer (PSO) and team **immediately upon discovery** by telephone at (909)383-9665 and email at HSPrivacySecurityOfficer@hss.sbcounty.gov of a suspected or actual breach of security of PII.

1. A breach of PII refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term where PII is used in a manner not permitted by your contract which compromises the security/privacy of PII.
2. 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 reports have been filed.

b) **Contractor shall take:**

1. Prompt corrective action to mitigate any risks or damages involved with the actual or suspected breach and to protect the operating environment.
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

c) **Investigation of Breach/Written Report** - Contractor shall immediately investigate such breach and within **five (5)** working days of the incident, produce a written report detailing:

1. Specific data elements involved and the extent of the data involved in the breach;
2. Description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PII;
3. Description of where PII is believed to have been improperly transmitted, sent, or used;
4. Description of the probable causes of the breach; and,
5. Detailed corrective action plan including measures that were taken to halt and/or contain the breach.

18. **Compliance by Contractor**

Contractor agrees to enter into written agreements with any agents or subcontractors who assist in carrying out the provisions of the contract and to which Contractor provides PII, including restrictions on disclosure of PII and the use of appropriate administrative, physical, and technical safeguards to protect such PII contained in this document. Contractor shall incorporate, when applicable, the relevant provisions of this document into each subcontract to such agents or subcontractors, including the requirement that any actual or suspected breach be reported immediately to the County.

19. **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 the contract 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.

20. **Technical Assistance**

    The Human Services (HS) Privacy and Security Team is available to assist Contractors with privacy and security questions and provide technical assistance as needed.

    Email: hsprivacysecurityofficer@hss.sbcounty.gov
    Contact: 909-383-9665