Overview

Purpose

The purpose of this Standard Practice is to provide procedures to be followed in the event of a breach of Personally Identifiable Information (PII) occurring in a Human Services (HS) department.

Throughout this Human Services Policy and Standard Practice (HSPSP) section, the term "department" is inclusive of both departments and divisions.

Implementation

HS must protect PII maintained or used by the County. Many preventive measures and safeguards have been implemented to minimize the occurrence of unauthorized access, use, or disclosure of information; however, there may be instances in which an information breach occurs. All HS staff, volunteers and any others granted access to HS facilities or resources containing PII, must read, understand, and comply with this Standard Practice.

Forms

The following forms are referenced in this HSPSP and are available as attachments to this section:

- Privacy/Security Incident Report (HSPSP 1503)
- Human Services (HS) Privacy and Security Representatives List (HSPSP 1505)

In this Standard Practice

This Standard Practice contains the following topics:

Reporting Responsibilities

Overview

A breach occurs when Personally Identifiable Information (PII) is lost, stolen, destroyed, disclosed, or accessed without authorization compromising the security, confidentiality, or integrity of the information. Human Services (HS) departments are responsible for ensuring all actual or suspected breaches of information are reported timely to the appropriate parties.

Legal requirements

Federal and state laws govern the protection of confidential information. It is the policy of HS to protect the privacy, integrity, and confidentiality of PII, as required by law through the application of appropriate safeguards. All HS departments have a responsibility to utilize these safeguards and protect all information, systems, and data at all times.

Department/ division responsibilities

All HS departments and divisions are responsible for maintaining and sustaining staff awareness of the breach of information Policy and Standard Practice, which outlines processes for:

- Timely and accurate notification of suspected information that is lost, stolen, misused, or accessed without authorization.
- Parties responsible for receiving, evaluating, and responding to reports of possible breaches of information within their respective department/division.
- Providing immediate notification of any breach to the Privacy and Security Officer (PSO) to obtain consultation and external notification authorization.

HS staff responsibilities

Early discovery and response to an information breach is essential to stop, rectify, and mitigate any harm. All HS staff must:

- Understand their reporting responsibility,
- Know how to report an actual/suspected information breach, and
- Do so without hesitation or fear of reprimand.

Continued on next page

Reporting Responsibilities, Continued

Privacy and Security Representative (PSR) responsibilities

All HS departments have a designated Department Privacy and Security Representative (PSR) to ensure all actual or suspected breaches (within their department) are identified and immediately reported to the PSO. The Department PSR is responsible for:

- Coordinating/consulting with individual HS Department Managers/ Supervisors in response to reports of a breach of information.
- Ensuring prompt corrective action is taken to mitigate any risks or damages involved with the breach and protect the operating environment.
- Routing the completed Privacy/Security Incident Report (HSPSP 1503) to the HS PSO inbox at HSPrivacySecurityOfficer@hss.sbcounty.gov.
- Initiating the fact-finding process involving reports of suspected or actual PII security breaches.
- Maintaining close consultation with the PSO and the Human Resources Business Partner (HRBP), if applicable, during the investigation process.
- Meeting with the PSO to discuss department privacy and security issues and ongoing preventive measures.

Note: Designated Department PSRs are identified on the Human Services (HS) Privacy and Security Representatives List (HSPSP 1505).

Privacy and Security Officer (PSO) responsibilities

HS has designated the PSO to oversee and monitor the compliance of PII policies. The PSO, in consultation with the Privacy and Security Compliance (PSC) Team (including County Counsel), is responsible for:

- Coordinating/consulting with the PSR during investigations of a PII breach.
- Ensuring the PSR and/or impacted department(s) notify the owner of the breached PII in writing (if applicable).
- Consulting with the HRBP, as needed, on appropriate corrective and disciplinary actions as a result of a breach of PII.
- Completing/maintaining a Breach Log of all reported incidents/breaches.
- Working with HS departments to implement measures to prevent reoccurrence of incidents.
- Meeting with PSRs to discuss potential security risks/threats and ongoing preventive measures.
- Reviewing department-specific policies and forwarding through the appropriate channel for approval/denial of such measures.
- Reporting all locally verified breaches to the State.
- Acting as County liaison with the State.

Continued on next page

Reporting Responsibilities, Continued

Privacy and Security Compliance (PSC) Team responsibilities

The Privacy and Security Compliance (PSC) Team consists of the:

- PSO,
- County Counsel representative, and
- Privacy Team at Program Development Division (PDD).

Responsibilities of the PSC Team are identical to the responsibilities of the PSO. Refer to the *Privacy and Security Officer (PSO) responsibilities* block in this section.

Reporting Procedures

Overview

Human Services (HS) departments must ensure all breaches of Personally Identifiable Information (PII) are reported timely and accurately. The reporting requirement is intended to:

- Reduce the occurrence and severity of incidents.
- Identify any other potential risks/threats.
- Promptly mitigate any damages and rectify the problem.
- Implement measures to prevent reoccurrence of incidents.

This section outlines the reporting procedures for all HS departments in the event of a security incident or breach of PII.

Breach Log

The Breach Log is an online database maintained by the Privacy Team at Program Development Division (PDD) and is located on the HS SharePoint site. The HS Privacy and Security Officer (PSO) completes and maintains the Breach Log, documenting all reported incidents and breaches.

Access to the Breach Log is limited to:

- HS PSO and back-up, and
- County Counsel representative.

Continued on next page

Reporting Procedures, Continued

Incident reporting

The following table describes the procedures for reporting a security incident within all HS departments:

Stage	Description
1	Discoverer reports the security incident immediately to his/her supervisor/manager.
2	Supervisor/manager: • Collects as much information as possible about the incident, and • Notifies the department Privacy and Security Representative (PSR) immediately, but no longer than 24-hours, of the reported incident.
3	PSR and Human Resources Business Partner (HRBP), if applicable: • Initiates a fact-finding process immediately, utilizing information obtained from the reported security incident, • Documents all findings on the Privacy/Security Incident Report (HSPSP 1503), and • Emails the HSPSP 1503 to the HS PSO inbox within 24 hours.
4	Privacy and Security Compliance (PSC) team: • Investigates the incident, • Consults with County Counsel, and • Determines whether the finding is an incident or a reportable breach, and:

If it is determined to be a(n)...	Then...
Incident (non-reportable breach),	• Determine if a corrective action plan is needed, • Document all findings on the Breach Log, and • Notify the department PSR and close out report entry in the Breach Log.
Reportable breach,	Refer to the *HS PSO steps for reporting a breach* block in this Standard Practice.

Continued on next page

Reporting Procedures, Continued

HS PSO steps for reporting a breach

The HS PSO will follow the steps below when reporting an actual breach of PII:

Step	Action
1	Consult with the PSC team to determine the appropriate local, state and/or federal representatives or department where notification is required under federal or state law.
2	Determine what is involved with the breach, and: • Document all findings on the Breach Log and attach the completed Privacy/Security Incident Report (HSPSP 1503) and any supporting documentation, • Forward all reports and supporting documentation to the appropriate local representative as necessary, and • Notify the department PSR.
3	Consult with the department PSR, HRBP, and/or Department of Health Care Services (DHCS) as necessary to: • Complete an investigation, • Obtain any additional information and/or documentation, • Determine corrective action and/or disciplinary action, • Complete and forward the DHCS Privacy Breach Report to the DHCS Privacy and Information Security Officers, and • Update the Breach Log and attach the DHCS Privacy Breach Report.
4	Update the Breach Log with **Closed** status once notified by DHCS that all required information has been received and the reported breach has been closed.
5	Coordinate with department and PSR to implement measures to prevent any future reoccurrences.

Continued on next page

Reporting Procedures, Continued

Non-reportable breach

When a breach is determined non-reportable (an incident), the HS PSO will do the following:

- Document the event as an incident.
- Notate all final findings and conclusions on the:
  - Breach Log, and
  - Privacy/Security Incident Report (HSPSP 1503).

  Note: Indicate the incident was determined to be a non-reportable breach.
- Send notification of investigation results to the PSR.

Reporting timeframes

The table below outlines the reporting timeframes mandated by the State, when reporting a PII incident and/or breach. It is imperative all departments, managers/supervisors, and department PSRs adhere to the timeframe requirements.

Reporting Party	Actions Taken	Timeframe to Report
Discoverer	Notify Manager/Supervisor	Day of discovery
Manager/Supervisor	• Initiate fact-finding process, • Document all findings on the HSPSP 1503, and • Notify Department PSR.	
Department PSR	• Conclude fact-finding process, and • Forward the HSPSP 1503 to the HS PSO inbox.	Within 24-hours of reported discovery
PSO	• Review HSPSP 1503, and • Notify PSC team.	Day of reported discovery from PSR
	• Complete DHCS Privacy Breach Report, and • Notify DHCS Privacy and Information Security Officer.	Within 24-hours of receipt of the HSPSP 1503 from the PSR
	• Finalize the DHCS Privacy Breach Report, and • Forward to DHCS Privacy and Information Security Officer.	Within 10 days of discovery

Continued on next page

Reporting Procedures, Continued

Enforcement	HS departments are responsible for enforcement of HS privacy and security policies. Violations of these set policies require corrective action and/or disciplinary action in accordance with Human Resources policies and County Personnel Rules. It is the responsibility of the department Manager/Supervisor, HRBP, and PSR to determine the appropriate corrective action plan(s) and/or disciplinary action(s) for all violations of privacy and security policies. However, the HS PSO must also be notified of any plan(s) and/or action(s) taken for breach documentation and tracking purposes, to provide to the State for review and/or any further action determined necessary by the State or the County.
Litigation or administrative proceedings	In the event of litigation or administrative proceedings, based on privacy and security of PII violation claims and/or State or Federal laws or agreements, HS must cooperate and make all reasonable efforts to ensure the availability of the individuals involved in the claim(s).