# L – 24: Privacy Incidents

**POLICY:** See L-24 Privacy Incidents at www.cosdcompliance.org.

**DEFINITIONS:** See HHSA Policy L-30.

**PROCEDURES:**

A. Reporting HHSA Privacy Incidents:
   1. When HHSA staff becomes aware of a real or suspected Privacy Incident, HHSA staff shall immediately notify their supervisor;
   2. Program Supervisor shall immediately notify Program Manager;
   3. Program Manager (or delegate) shall:
      a. Immediately notify the Agency Privacy Officer (APO) by email;
      b. Complete the HHSA Form 23-24 and submit to APO within one (1) business day. Do not include Protected Information on the report; and provide copy or sample of information involved in incident, if directed by APO;
      c. Take prompt corrective action to investigate incident and mitigate any risks or damages involved with the Privacy Incident; and
      a. Submit an updated Form 23-24 to the APO within three (3) business days of the discovery and a final and complete Form 23-24 to the APO within nine (9) working days. If Program needs additional time, Program shall inform the APO.

B. Client Notification for HHSA incidents. Program Manager shall:
   1. Ensure necessary client notifications are completed within thirty calendar (30) days of initial report. This shall include:
      a. If Program Manager is unsure whether or to whom client notifications are required, Program Manager shall perform initial analysis and consult APO by tenth ($10^{th}$) calendar day following initial incident report.
      b. Program Manager shall draft notification letter using Agency Compliance Office approved template. APO shall provide template upon request. Program Manager shall send draft notification letter to APO by twentieth ($20^{th}$) calendar day for APO approval.
      c. Program Manager shall send notifications to the affected clients. Notifications shall be made to individuals without unreasonable delay and in no event later than thirty (30) calendar days after the initial report. Any exceptions to the thirty (30) day policy must be approved by the APO by the twentieth ($20^{th}$) calendar day.
   2. Provide signed copies of notification letters to APO, including date letters were sent, and copy of certified receipt if applicable.
   3. Work with APO regarding other required notifications, as below.
   4. Maintain copy of notification letters as required by retention policies for a client's chart or file.

C. APO role in HHSA Privacy Incidents:

1. Determine whether a Privacy Incident occurred and the corrective action plan proposed by the program manager is adequate;
2. Perform a Breach Assessment of the incident by considering the probability that Protected Information (PI) has been compromised, considering:
    a. The nature and extent of the PI involved, including the likelihood someone can identify he individual whose data was compromised
    b. Who was the unauthorized recipient of the PI
    c. Whether the PI was actually acquired or viewed
    d. The extent to which risk to the PI has been mitigated
3. The result of the Breach Assessment shall determine whether notifications are required. If required, APO shall ensure notifications are appropriate and timely, as follows:
    a. If client notification is required, APO shall work with Program Manager (as above);
    b. APO shall handle notifications to federal or State entities; and APO shall also ensure media is notified when required.

D. Outside HHSA Privacy Incidents: When HHSA staff become aware of a known or suspected privacy incident involving County Protected Information, they shall immediately notify the APO via email.

**QUESTIONS/INFORMATION:** HHSA Privacy Officer at 619-338-2808