L – 24: Privacy Incidents

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 an actual 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. If actual or suspected privacy incident involves **500 or more individuals**, **immediately** notify the Agency Privacy Officer (APO) by email; for all other incidents, follow steps below.
      - Submit an initial Privacy Incident Report (PIR) online within one (1) business day. To access the landing page and link to the PIR web-form **click here**. This web page link is also accessible on the Agency Compliance Office public website at www.cosdcompliance.org. Do not include Protected Information in the web-form report; provide copy or sample of information involved in incident, only if directed by APO;
      - Take prompt corrective action to investigate incident, suggest corrective action plan in the web-form to APO, and document in web-form mitigation of any risks or damages involved with the Privacy Incident;
      - Continue to investigate and update the PIR online within 72 hours, as applicable.
      - If needed, complete the final PIR online within seven (7) working days of discovery. If Program needs additional time, Program Manager shall inform the APO.

B. Client Notification for HHSA incidents.

1. APO shall confer with Program Manager and provide direction as to whether client notifications are required.
2. If required, Program Manager shall ensure notifications are completed within timeline provided by APO. This shall include:
   a. Program Manager shall draft notification letter using APO template. Program Manager shall send draft notification letter to APO for review and approval.
   b. Contractors shall submit draft notifications to APO compliant with CA Civil Code §1798.29
   c. APO shall obtain approval from the State, as applicable and as circumstances permit.
   d. Program Manager shall send notifications to the affected clients without unreasonable delay. Any delay with reporting must be approved by the APO.
3. Provide signed copies of notification letters to APO, including date letters were sent, and copy of certified receipt if applicable, within three (3) working days of distribution.
4. Work with APO regarding other required notifications, as below.

5. Maintain official 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 applicable federal entities, such as the Office of Civil Rights, APO shall make all necessary reports within required timeframes, currently 60 days for breaches impacting 500 or more individuals and by February 28 for all incidents occurring the previous calendar year that impacted fewer than 500 individuals.
      c. APO shall additionally make all required reports to applicable State entities, such as CA Department of Health Care Services, CA Department of Aging, CA Department of Social Services, and CA Department of Public Health. Current State reporting requirements are:
         1) APO will immediately send notice to State of an applicable security incident that includes data provided to the State by the Social Security Administration.
         2) APO will send notice to State of other breaches using the State's approved report within one (1) business day.
         3) APO will send an updated report to State within seventy-two (72) hours as applicable.
         4) APO will send complete report to State within ten (10) working days.
         5) As necessary, APO may submit additional reports after ten (10) day period.
      d. APO shall also work with Program and County Counsel to 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. If incident involves contractor, additional requirements are found in Information Privacy and Security Provisions (Article 14).

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