COUNTY OF SAN DIEGO
Health and Human Services Agency

LIVE WELL SAN DIEGO

L - 26: Safeguarding Protected Information

POLICY: See HHSA-L-26 Safeguarding Protected Information, at www.cosdcompliance.org.

DEFINITIONS: See HHSA Policy L-30 Privacy Definitions.

PROCEDURES:

1. Workspace and Desks

a. Ensure Protected Information (PI) is always attended to. Lock your computer (Ctrl + Alt + Delete or Windows + L) when stepping away and keep paper documents out of sight and secured when not in use.

b. At the end of each day:

   i. Confirm that your desk is clear and the confidential shred bin is empty.

   ii. Secure any paper records and County assets (e.g., laptops, tablets, flash drives) in a locked filing cabinet or office with a second layer of security (e.g., cable lock or badge-restricted room).

2. Printer, Copiers, and Faxes

a. Use only County-approved printers/copiers/fax machines in secured work areas.

b. Retrieve printed PI promptly from shared devices and confirm that you only collect your own items.

c. Print, scan, or copy PI only when necessary and follow County approval processes.

d. When faxing PI, especially in BHS, PHS, or other Self-Sufficiency services, staff must:

   i. Contact the recipient by phone to confirm the fax number.

   ii. Confirm successful transmission and retain the fax receipt.

   iii. Follow best practices to prevent misdirected faxes:

      a. Send a test fax to confirm the number is active.

      b. Use a County-approved fax coversheet that includes a **confidentiality disclaimer**. This disclaimer should inform recipients that the information is private and instruct unintended recipients to destroy the fax and notify the sender.

         ⓘ ***NOTE:*** Including a confidentiality notice does not replace caution – staff must still verify the recipient before sending.

3. Conference and Interview Rooms

a. Use discretion when displaying PI on whiteboards, charts, screens in shared spaces or during screensharing.

b. Clear PI from tables, boards, and surfaces at the end of each meeting.

c. For BHS, PHS, or other Self-Sufficiency services, escort visitors through areas where PI is accessible. While most County locations use badge readers to monitor facility access, programs should consider maintaining visitor logs when escorting external visitors into areas containing PI if badge scanning is unavailable or bypassed.

4. **Emails**

    a. Ensure all protected information (e.g. PHI, PII, sensitive data) sent outside the County network is encrypted.

        i. Mobile Device Limitation: County-managed mobile devices (e.g. iPhone, Android) cannot encrypt email(s) through the Outlook app. To send encrypted emails from a mobile device, one of the following conditions must be met:

            a. You log into Outlook via Microsoft Office Web Access, or

            b. The sender is on the HHSA Mandatory Email Encryption list, or

            c. All email recipients are on the vetted HHSA TLS Business Partner list.

        ii. **Exception – Individual Request for Unencrypted Communication**

            a. In limited cases, individuals may request that their own protected information be sent unencrypted.

            b. This must be documented using HHSA Form 23-05 or in a written request, acknowledging that they understand and accept the risks of unencrypted communication.

            c. Third parties (e.g. attorneys, representatives) may not request unencrypted delivery on someone else's behalf.

            d. For more detailed guidance, refer to HHSA Privacy Procedure L-05 and check with department policy and procedures before complying with a request.

    b. Never send or forward PI or work-related email(s) to personal email accounts.

    c. When replying or forwarding emails with PI:

        i. Verify the recipient(s) email address. Double-check the email address for accuracy before sending and ensure the intended recipients are authorized.

        ii. Limit distribution. Share only with those who need the information and only include the minimum necessary PI.

        iii. Review the full email thread before replying to ensure no sensitive information is inadvertently shared.

        iv. If you receive an unencrypted email that contains PI, follow these steps:

            a. Do not reply directly to the unencrypted email.

            b. Start a new message using a County-approved secure method, such as encrypted email or a phone call.

    d. Outlook and Team Calendar Invites

        i. Calendar invitations sent via Outlook or Microsoft Teams cannot be encrypted. Do not include PI (e.g., full client names, case numbers, demographic or health information, or other sensitive details) in calendar invites sent outside the County.

        ii. Use first names, initials, or generic appointment labels when scheduling meeting with clients or external parties.

e. Optional Confidentiality Notice (Optional)

i. While not required, it is recommended to include a confidentiality notice when emailing third parties outside the County network and the message contains PI.

ii. Sample Notice: CONFIDENTIALITY NOTICE: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain information protected by applicable laws and regulations. If you are not the intended recipient, you may not review, use, copy, disclose, or distribute this message or its attachments. Please notify the sender and delete the message and all attachments immediately.

a. Including the notice does not replace the need for encryption or recipient verification.

b. This notice does not establish attorney-client privilege.

f. Security and Phishing Awareness

i. Do not open, reply to, forward, or click links or attachments from unknown or suspicious senders.

ii. Avoid downloading files or enabling macros in a suspicious email.

iii. Watch for email spoofing. Review sender addresses for subtle misspellings or impersonations of County partners.

iv. Report suspicious emails using the Phish Alert Button in Outlook to notify IT Security.

v. If you are unsure whether an email is legitimate, contact your supervisor before responding.

5. Phones and Verbal Communication

a. Ensure verbal conversations involving PI are held in private settings where others cannot overhear. Avoid discussing sensitive information in hallways, elevators, shared workspaces, or public areas.

b. Contact clients using County-issued phones only. Never use your personal phone number to communicate with clients.

c. Text messaging is not a secured method of communication for PI even when using a County-issued phone.

i. Use a County-approved, secured alternative (e.g., encrypted email, fax, verbally) when communicating about PI.

ii. For more detailed guidance, refer to HHSA Privacy Procedure L-05 and check with department policy and procedures before complying with a request.

d. Do not take photos of clients or PI using personal phones.

e. Be mindful of any PI you leave in a voicemail or on answering machine messages.

f. Always verify the identity of callers before discussing or disclosing PI over the phone.

6. Social Media

a. Never post PI on personal or public social media accounts.

b. Do not share photos, client stories, screen captures, or work-related updates that could directly or indirectly reveal PI.

c. When in doubt, do not post. Even de-identified details may lead to re-identification when combined with other publicly available information.

7. Handling & Storing PI

a. PI must only be stored on County-approved, encrypted devices.

b. When sharing PI

i. Confirm that recipients are authorized.
ii. Use the minimum necessary standard.

c. Maintaining Accurate Records

i. Ensure client records are accurate and up to date, including verifying addresses before use or disclosure.

d. Do not store Protected Health Information (PHI) on SharePoint Online, OneDrive, or MS Teams. These platforms are not approved for HIPAA-covered information.

i. Only Personally Identifiable Information (PII) may be stored in SharePoint or OneDrive if access is appropriately restricted. Use the S:\ Drive or other County-approved HIPAA-compliant systems to store PHI.

ii. If there is uncertainty about whether information qualifies as PHI or whether a storage platform is approved for PHI, County staff must consult internal guidance or a supervisor before storing the data.

e. Do not leave PI unsecured or visible in public, client-accessible, or shared spaces.

8. Assets and Asset Management

a. Departments are responsible for maintaining an up-to-date inventory of all County-issued assets (e.g., desktops, laptops, tablets, smartphones, portable storage devices).

b. Departments are responsible for identifying and monitoring each staff member’s assigned assets, primary work location (on-site or remote), and access to systems or shared folders containing PI. Access must be promptly terminated when an employee separates, changes roles, or no longer requires system access.

c. Departments must immediately report any lost or stolen County asset(s) to the Business Assurance & Compliance.

9. Leaving the Office

a. Obtain permission from your supervisor before removing PI from a County facility.

b. Staff must complete HHSA Form 23-26 prior to removal, regardless of duration.

c. Keep PI and County assets (e.g. laptops, tablets, portable media devices) with you at all times.

d. When offsite or at home

i. Secure paper and devices in a locked, safe location.

ii. Never leave PI in a car overnight.

iii. For field staff:

a. Do not leave PI unattended in a car or trunk, even briefly.
b. PI may never be checked on an airplane.

L - 26: Safeguarding Protected Information

10. Teleworking and Remote Access

a. County staff approved for remote work or hybrid must complete the required annual remote work agreement in accordance with HHSA policy and maintain compliance with the terms outlined by Agency Human Resources.

b. Remote Access and Storage

i. Only use County-approved VPN solutions.

ii. Do not use public Wi-Fi when working with PI.

iii. County staff must follow County policy for secure password use and multi-factor authentication (MFA) when accessing systems remotely

iv. Keep paper PI locked away when not in use – never leave it unattended.

v. Save electronic PI only on County-approved encrypted devices.

vi. Return paper PI to a County facility for shredding – do not shred PI at home

c. Home Workstations

i. Use a privacy screen or position monitors away from view.

ii. Lock your screen when stepping away.

iii. Restrict access to your work devices from others in your household.

iv. Do not print PI at home unless expressly authorized by your supervisor and consistent with County policy.

d. Personal Printers (when permitted)

i. Obtain prior supervisor approval before printing any documents containing County PI while teleworking.

ii. Only print the minimum necessary information required to perform your job.

iii. Do not use personal printers at copy shops (e.g., UPS, FedEx) or those belonging to others.

iv. Promptly delete files from the printer's internal memory after printing. Refer to the printer manual for instructions.

e. Telehealth and Video Conferencing

i. Conduct meetings in private spaces to avoid others overhearing PI.

ii. Use only County-approved platforms (e.g., MS teams, Webex). Others require prior approval.

iii. Meeting transcription

a. Provide meeting notice and receive consent prior to recording.

b. Turn off transcription for sensitive topics unless there is a documented need and program approval.

iv. Use County-approved file-sharing platforms:

a. Use the S:\ Drive or other HIPAA-compliant systems to store or share PHI.

b. Use SharePoint for de-identified PII, with access restrictions.

c. Never transmit or store PI using chat windows, meeting recordings, or unapproved cloud platforms.

v. Unplug, disable or mute the microphone of any listening devices (e.g., Alexa, Google, Siri) during calls involving PII or PHI.

11. Artificial Intelligence (AI) Tools

a. County-approved Platforms Only

i. Use only County-approved AI tools integrated into secure environments. Public or consumer AI platforms (e.g., ChatGPT, Gemini) are not authorized for PI.

b. Prohibition of PI in AI Tools

i. Do not input, upload, or share Protected Information (PHI, PII, sensitive data) into any AI tool unless explicitly approved and compliant with County policy.

c.

i. If AI is used for drafting or analysis, ensure no client identifiers or sensitive details are included. Use generic or de-identified data. See HHSA Privacy Procedure L-21 for additional guidance.

ii. AI-Assisted Meeting Transcriptions and Summaries

a. Turn off transcription for sensitive topics unless there is a documented need and program approval.

d. Verification of Outputs

i. AI-generated content must be reviewed for accuracy and compliance before use in official communications or records.

12. Disposing of PI

a. Shred paper containing PI using a County-approved shred bin or Countywide shredding service.

b. For questions about proper disposal of electronic devices or digital storage, refer to Property Reutilization Services.

13. Self-Identified Misuse/ Suspected Disclosure

a. When staff become aware pf an actual or suspected disclosure of PII, PHI, or sensitive information notify supervisor and follow HHSA Privacy Procedure L-24 Privacy Incidents.

14. Training Requirements

a. Staff who handle Protected Information (PI) are required to complete annual privacy training.

b. Refresher training is available through Business Assurance & Compliance (BAC) to support continued compliance and reinforce safeguarding practices.

QUESTIONS/INFORMATION: Please contact HHSA Business Assurance and Compliance (BAC) by email at Compliance.HHSA@SDCounty.ca.gov or by phone (619) 237-8571.