Human Resources Administration
Department of Social Services

OFFICE OF POLICY, PROCEDURES AND TRAINING

James K. Whelan
Executive Deputy Commissioner

Lorraine Williams
Director of Procedures, APS

APS Policy Bulletin #2021-05
Date: August 17, 2021 **DISTRIBUTION: *ALL STAFF***

CLIENT CONFIDENTIALITY

Purpose: The purpose of this policy bulletin is to inform APS staff of the client confidentiality policy and ensure that all APS and vendor staff protect client privacy and adhere to confidentiality rules. The term "client" includes persons referred to APS, persons who are currently receiving services, and those who have received services in the past.

OVERVIEW

Federal, state, and local privacy laws apply to the collection, retention and disclosure certain identifying information including, but not limited to, social security numbers, addresses, financial information, marital status information, and protected health information, such as health insurance status. Identifying information means any information obtained by or on behalf of the City that may be used on its own or with other information to identify or locate an individual.

A confidential document is defined as a document that contains any information that is private, or not for public dissemination. Most Agency records and all client records are confidential. Disclosing confidential information is harmful to DSS's clients. It also harms the Agency by causing the public to lose trust in the Agency's ability to protect confidential information. Improper disclosure of confidential information is often a violation of the law and can lead to financial liability to the Agency.

POLICY

In general, an employee may not use or disclose protected health information pertaining to a client of HRA/DSS except as permitted or required by law. Personally identifiable information includes the following:

1. Medical and or mental health information, which includes treatment history and any demographic information that can identify an individual;
2. an individual's HIV status;
3. that the individual has been diagnosed or treated for substance and/or alcohol use;
4. domestic violence history, address information for survivors of domestic violence, and location of domestic violence emergency residential programs;
5. that a particular individual has applied for, has received or currently is a recipient of public assistance, food stamps, Medicaid or other public assistance benefits;

6. immigration status;
7. an individual's involvement with child welfare services;
8. any case specific information related to enforcement of child support obligations or the establishment of paternity;
9. ID NYC applicant/recipient information; and/or
10. Information concerning an applicant for or recipient of adult protective services.

To document the client's agreement to release confidential information, a completed Authorization for Release of Health Information Pursuant to HIPAA (**OCA-960**) is required.

Data Security Incidents

A data security incident occurs when confidential information is disclosed to a third party without authorization, whether the disclosure is intentional or accidental. Examples of possible data security incidents include, but are not limited to:

- Loss, theft, or improper disposal of Agency equipment, including BlackBerrys, Agency issued cell phones, CDs, thumb drives, portable devices, desktop computers, laptops, photocopiers, fax machines.
- Loss, theft, or improper disposal of employee-owned devices used for agency purposes.
- Loss, theft, or improper disposal of hard copy documents that contain confidential and personally identifiable information. Individually identifiable information may relate to employees and clients.
- Misdirection of emails and faxes containing confidential information that are sent to unintended parties.
- Suspected instances of computer hacking.
- Release of confidential information in response to a fraudulent email or telephone call.
- Disclosure of confidential information to the internet or any social media sites.
- Unauthorized copying of confidential Agency information to personal electronic devices, such as routers, thumb drives, etc.
- Improper use or disclosure of confidential information obtained from city or state-owned databases such as APSNET, WMS, HRA OneViewer, etc.

In some cases, a data security incident may be considered a breach. Whether a disclosure constitutes a breach is a legal determination to be made by OLA.

In the event of an unauthorized disclosure of confidential information, APS staff should report the incident to their supervisors. Supervisors should refer the incident to their Director, Deputy Director, or designee. A completed Data Security Incident Form (**DSS-2**) must be submitted to OLA Chief Data Privacy Officer.

Note: Refer to the DSS Data Security Incident Procedure: What to Do in the Event of an Unauthorized Disclosure and Breach Prevention Measure (**Procedure No. 17-09**) for further information and guidance.

Vendor staff must report the unauthorized disclosure of confidential information to their supervisors. Supervisors will report the disclosure to the Director, Deputy Director, or designee. The unauthorized disclosure of confidential information must be submitted to APS Administration, who will notify the DSS Chief of Data Security of the incident.

Releasing or Disclosing Information Concerning Clients

In general, DSS's policy prohibits staff from disclosing confidential information to anyone outside the Agency, or to any employee whose duties do not require such disclosure, without valid authorization from the client. Client information may be released to an "authorized representative" without a signed **OCA-960**. Authorized representatives include the following:

- An individual the client names, in writing, as an "authorized representative;"
- A person appointed by the court (i.e., Art. 81 Guardian, Guardian Ad Litem, Court Evaluator);
- The client's legal counsel who provides a signed engagement/retainer agreement or Notice of Appearance; or
- An agent the client names in a properly executed Power of Attorney.

Staff must forward any documentation designating the individual as an authorized representative to the Office of Legal Affairs at OLAAPSReferrals@hra.nyc.gov for review prior to releasing confidential information by phone or in writing.

Client information may be released without written authorization from the client, or authorized representative, under the following circumstances **only**:

1. **To a provider of services –** Information can be released only if it is necessary to determine the need for services, or to provide for and arrange services.

2. **Requests by the Court –** Information can be released when directed by the court indicating that the information is necessary for a party in a criminal or civil case, or it is needed to determine an issue before the court. OLA must review all requests made by courts prior to releasing client information.

3. **A court evaluator, MHL Article 81 guardian, or SCPA Article 17(A) guardian -** Requests for client information must be sent to OLA for review unless previously advised by OLA to comply with the request (e.g., cases where APS has petitioned for guardianship).

   NOTE: APS may share case information with a Guardian Ad Litem (GAL) but are not required to do so. If APS staff plans to provide case records to a GAL, the case records must be reviewed by OLA for possible redaction.

4. **Grand jury** requests – OLA must review grand jury requests prior to releasing client information.

5. **Requests from a District attorney, Department of Investigation, Police Department, or Sheriff –** Information may be released only if the request states that:
    - The information is necessary for a criminal investigation or prosecution;
    - There is reason to believe the investigation or prosecution involves or affects a client; and
    - There is reason to believe that the information requested is related to the investigation or prosecution.

    All requests made by the district attorney or law enforcement counsel must be forwarded to OLA prior to any disclosure.

In addition, the requesting party must ensure that released information will stay confidential and used only for the purposes described.

NOTE: These rules apply to current clients as well as former clients, referred individuals, and applicants of APS.

Staff that receive a request for confidential information must forward the request to their immediate supervisor. Supervisors will forward the request to the Director, Deputy Director or designee for submission to OLA.

Requests for Case Records

Before complying with a request for APS records, the request must be forwarded to OLA for review.

Information can be withheld if it would reveal:

1. The referral source;
2. Anyone who has cooperated in an APS investigation or assessment; or
3. Information that would be detrimental to the interests or safety of the source or person involved.

Staff who receive a request for client case records must be forwarded to their supervisor. The supervisor will forward the request to the Director, Deputy Director, or designee. The request will be submitted to OLA for review. OLA will redact any referral source-related information and confidential information contained in the client's case record. Vendors that receive requests for client case record will forward the request to APS Administration via email.

Working with Client Files

Confidential information should not be left unattended on staff desks or in other unsecured areas of the office. When staff exit their work areas, they must take every precaution not to leave any confidential information where it may be visible or accessible. Staff should log-off or lock their computers when they are away from their desks to ensure that no unauthorized person accesses information or performs unauthorized work from their computers.

Staff who are authorized to take work home (or e-mail electronic documents to their computer at home) are responsible for ensuring family members or other individuals do not view the documents. When accessing and using confidential work-related materials, staff must keep all materials within the Agency's electronic environment such as through remote access or Agency email accounts. Staff may not use personal email accounts or cloud-based computing services that are not approved and provided by the Agency.

The following are best practices for safeguarding confidential client information:

- Keep case records in locked files.
- Mark case records "Confidential."
- Do not use Agency issued devices for personal use and do not share Agency issued devices with others.
- Do not remove case records from the office without authorization.
- Transmit records from one location to another in sealed envelopes marked "Confidential."
- Interview clients in areas that maximize privacy.
- Conduct business in a private area away from others, especially when conducting calls.

Staff Responsibilities Concerning the Use of E-mail

Staff must take all reasonable precautions to ensure that unauthorized individuals do not have access to information on the staff member's e-mail account. Official APS business should be communicated via Agency issued e-mails and staff should not use personal e-mails for these types of correspondence. These precautions include safeguarding passwords and changing them periodically. Guidelines for staff use of e-mail are contained in DSS E-Mail Policy, Procedure No. 07-06, March 22, 2007.

Staff should be cautious when including confidential information in e-mail correspondence. E-mail records, once opened, become irrevocable. Staff should also be aware that anything that they write in an e-mail message may be forwarded by the recipient of the e-mail to others, without the sender's control, approval, or knowledge. Social Security numbers should never be included in the subject line of an e-mail. Staff may also manually encrypt emails by including the word "encrypt" in the subject line of emails for added protection. Before sending large electronic files containing confidential information via e-mail, staff should consult with ITS and/or the OLA Chief Data Privacy Officer to determine what is the most appropriate and secure method for such e-mail transmissions.

Staff should maintain their passwords in a secure location known only to them and should not share them with others.

The following is an example of standard disclaimer language that should be placed at the end of an e-mail containing confidential information:

"This e-mail communication, and any attachments, may contain confidential and privileged information for the exclusive use of the recipient(s) named above. If you are not an intended recipient, or the employee or agent responsible to deliver it to an intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please notify me immediately by replying to this message and delete this communication from your computer. Thank you."

Staff Communications

Staff members are prohibited from discussing clients and/or their cases in the presence of others not involved in the cases and should be especially careful in public areas including elevators, restrooms and waiting areas.

Employees should not discuss any confidential matter with anyone either in person or on the telephone unless they are acting in conjunction with their job requirements or is specifically authorized by their supervisor. Moreover, discussions involving confidential information should be held in as private an area as possible, and in a volume so only those authorized to participate in the conversation can hear what is being discussed. If an employee has any question as to whether an individual is entitled to information, supervisory staff should be consulted before the information is disclosed.

Effective Immediately.

References

- Public Health Law, Article 27(F)
- The Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 and 164
- Identifying Information Law, Local Laws 245 and 247
- DSS Confidentiality Policy – Executive Order 746
- DSS Data Security Incident Procedure: What to Do in the Event of an Unauthorized Disclosure and Breach Prevention Measure, Procedure No. 17-09, September 14, 2017

Related Form(s)

OCA-960 Authorization for Release of Health Information Pursuant to HIPAA