MULTIPURPORSE SENIOR SERVICES PROGRAM BRANCH DATA SECURITY POLICY

It is the policy of the California Department of Aging's (CDA) Multipurpose Senior Services Program (MSSP) Branch to apply appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information (PHI).

The following security and privacy policy is *supplemental* to CDA's department-wide policy and CDA's Standard Agreements with MSSP Providers.

Legal Authority

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The HIPAA Privacy Rule (2003)
- CDA's Standard Agreement with MSSP Providers - Special Terms and Conditions, Exhibit D, Multipurpose Senior Services Program, Article IX on Monitoring, Assessment, and Evaluation
- The CDA Interagency Agreement with the Department of Health Care Services, the single State Medicaid agency,

Objective

To ensure that MSSP procedures are sufficient to safeguard the security and privacy of PHI and to ensure a process is in place in case of a data breach.

Coverage

This policy applies to the CDA MSSP Manager, MSSP Staff, and MSSP Branch Support Staff.

Guidelines for Security

The following guidelines shall apply to on-site Utilization Reviews (UR), Alternative URs/desk reviews, handling of confidential Monthly Client Data Reports, Client Lists for URs, and the handling of PHI within the MSSP Branch.

<u>Electronic Data Security:</u>

1. When client data is being transferred electronically, ensure the following guidelines are enacted to reduce risk:

a. Secure Website: Provide the information and instructions to MSSP sites to upload confidential electronic PHI (ePHI) to CDA's MSSP Branch's Secure Transfer File Protocol (STFP) website.
b. Data Storage Devices: Only encrypted USB Flash Drives *that are password protected* may be used for storage, data back-up, and transfer of computer files.
c. Laptops: Ensure laptops are safeguarded at all times. Log off the computer while ePHI is active.
d. When ePHI is received, ensure all non-essential information is immediately deleted if possible. Non-essential information may be dependent upon the nature of the documentation received. For example, client lists include client name and number, but do not require Social Security numbers, addresses, or birthdates.
e. When ePHI is transferred, ensure non-essential client identifiers are deleted (i.e., client names, addresses, and Social Security numbers).
f. Workforce Security: Limit review of ePHI to only those persons authorized to have access to such information (i.e., MSSP managers, designated MSSP staff, and audit team members.
g. Regularly review these records and delete ePHI when no longer needed (e.g., once the project has been finalized, UR Report or corrective action plan approval letter has been issued, etc.). All documents containing PHI related to that project must be placed in a confidential shred bin (e.g., Client List, care plans, progress notes, etc.). Documents containing PHI must not be placed in recycling bins or trash cans.
h. Close or log off of laptops to avoid unauthorized personnel from viewing documents containing ePHI.

<u>Hard Copy Information Security:</u>

<u>During on-site UR:</u>

1. Conduct an informal security risk assessment of the work environment by giving consideration to the following:
   a. Is the work area located in a common area?
   b. Is the work area located in a high traffic area?
   c. Is secure access entry required to the work area?
   d. Can the work area be secured?

2. Based on the risk assessment, make adjustments to safeguard PHI and any other private information as necessary, including but not limited to the following:
   a. Ensure records are locked when away from the room
   b. Place documents faced down when not reviewing.

c. Place documents faced down when others enter the room
d. Secure all documents during breaks, lunch and at the end of work day

Transporting Hard Copy Information During Travel:

1. Documents containing PHI should never be left unattended in a vehicle or other unsecure location.

2. Documents containing PHI should always be locked in the trunk of vehicle during transport.

3. Documents containing PHI must remain in the possession of MSSP staff at all times and stored in “carry-on” bags when in flight. Documents containing PHI should never be stored in “checked” baggage.

4. Documents containing PHI should never be viewed in public areas such as on a plane or in a hotel lobby or business center where others may be able to view the PHI.

5. MSSP staff should take steps to safeguard documents containing PHI in their homes and prevent others from viewing the documents until their return to the office.

Shipping Records for Alternative Utilization Desk Reviews (Shipping Records between MSSP sites and CDA):

1. When faxing client list to an MSSP site:
   a. Confirm the fax number to which the information is being sent and be sure that it has been entered correctly into the fax machine.
   b. Use a cover sheet that does not include any identifiers (i.e., should not include participant name, participant number, etc.) and should include a statement similar to the following: “The information contained in this facsimile may be privileged, confidential, and/or protected from disclosure. This facsimile may contain protected health information (PHI); dissemination of PHI should comply with applicable federal and state laws. If you are not the intended recipient, or an authorized representative of the intended recipient, any further review, disclosure, use, dissemination, distribution, or copying of this facsimile is strictly prohibited. If you think you have received this facsimile in error, please notify the sender by telephone.” Remove and shred list after the fax has been completed.

2. In the event that a fax is received by an unintended recipient, MSSP staff should obtain the person's contact information, attempt to identify the misdirected document, and then contact the MSSP Health Program Specialist/Privacy Officer. Recipients of the misdirected document should be informed to shred the document. When receiving faxed documents
   a. MSSP staff should monitor the MSSP fax machine (located within access-controlled area within the California Department of Aging building within the MSSP section) on a regular basis for unanticipated faxes and to distribute these documents to the intended recipient.
   b. When a fax arrives, it should be reviewed to verify the number of pages against the faxed cover page. If page(s) are missing, contact the sender and request the document be retransmitted.
   c. Follow any instructions on the fax cover page.
   d. If a fax is received in error, the MSSP staff recipient should inform the sender of the error. Unless instructed otherwise by the sender, the fax must be placed in a confidential shred bin.

3. When receiving a confidential FedEx shipment of client records for alternative UR/desk review:
   a. Email the MSSP site the FedEx shipping label received from CDA's Contracts and Business Services Section (CBSS). Inform the site to seal the package and ensure it is marked "**CONFIDENTIAL**".
   b. Track shipment process via FedEx's online tracking system using the tracking number provided by CBSS above to ensure receipt by the intended recipient.

      *In the event that documents are sent to, or received by, an unintended recipient, MSSP staff should obtain the person's contact information, attempt to identify the misdirected documents, and then contact the MSSP Health Program Specialist/Privacy Officer to notify him/her of the situation. The recipient should be instructed to return the package to the sender.

   c. CBSS will notify MSSP when the shipment has arrived. The shipment may also be tracked via FedEx's online tracking system to ensure shipment arrives by Friday morning (usually by 10:30AM).
   d. Assigned MSSP analyst will retrieve package from CBSS and sign log noting receipt of package.
   e. Along with another MSSP staff member, assigned analyst will open package and verify correct records were received.
   f. Email the MSSP site a confirmation that all required records and documents were received or notify the MSSP site of any discrepancy.

g. Assigned MSSP analyst will hand deliver the package to the assigned Nurse Evaluator (NE). The NE will lock up the package in a designated file cabinet.
h. The NEs review records Monday-Thursday of alternative UR period. When not in use, records will remain locked in a file cabinet. Records shall not be removed from within access-controlled areas within CDA's building. Records must be locked up in a designated file cabinet at the end of each business day.

4. When shipping a confidential FedEx shipment back to an MSSP site:
   a. Ask the NE to retrieve the package with records from the locked file cabinet. In the presence of the NE, the assigned MSSP analyst will confirm all original records and documents are in the package. Seal the package and ensure the box is marked "**CONFIDENTIAL**".
   b. Assigned MSSP analyst will hand deliver package and form to CBSS for shipping.
   c. CBSS will email tracking number to MSSP staff person requesting the shipment. MSSP staff will forward the tracking information to the MSSP site and monitor tracking to ensure package arrives to the MSSP site.

Processing Client Data Reports:

1. On a monthly basis, MSSP sites upload client data to the Secure File Transfer (SFT) website. Each MSSP site has their own userID, password, and specific folder to upload data containing PHI. Only designated MSSP staff have authorization to access the SFT website.

2. Client data is downloaded from the SFT and placed in the specific Fiscal Year (FY) and month folder in CDA's secure shared drive. Only MSSP and CDA's Information Technology Branch staff have access to the MSSP secure shared drive.

3. Client data is loaded into the MSSP Database, located on the MSSP Branch S: Drive (S:\MSSPDATA\Mini-MSSP Application).

4. The MSSP Database produces two documents monthly which contain client data.

5. After the documents are submitted to the Department of Health Care Services and the Department of Social Services, the client data on the SFT website is permanently deleted.

Client Lists for URS:

1. When preparing the Client List for the UR, client data is downloaded from the MSSP Database for a specific MSSP site and placed into an Excel document, which is saved on the MSSP Branch secure designated S: Drive (S:\00_All Site Folders\(Site ## NAME)\(FY-FY)\UR).

2. The Client List document is hand delivered by the assigned MSSP analyst to the assigned NE . The NE will lock up the document in a designated file cabinet.

3. The NE will review the document to select clients for the final Client List. Once selected, the NE will notify the assigned Analyst. The NE will dispose of the document in the confidential shred bin.

Security Incident Reporting:

In order to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents, to the extent practical, the MSSP Branch will use the following process in documenting security incidents and their outcomes:

1. Immediately report to the MSSP Branch Supervisor any breach of ePHI. This may include reporting lost or stolen laptops, lost data storage devices, or known breaches of the Secure Website

2. Document the incident in writing

3. Review formal documentation and determine whether the post-incident analysis requires security policies to be updated

4. Maintain a log of security incidents related to the unit

Guidelines for Privacy

The following guidelines shall be adhered to for both on-site URs, Alternative UR's/desk reviews, handling of confidential Monthly Client Data Reports, Client Lists for URs, and any other PHI.

The review, collection, documentation, or maintenance of PHI is limited to legitimate business of the MSSP Branch (i.e., conducting an on-site UR, performing alternative desk UR, preparing utilization reports, etc.):

1. Do not use or disclose the information other than as permitted or required by law.

2. Use appropriate safeguards to prevent use or disclosure of the information other than as required.

3. Minimize the use of PHI to information necessary to meet the MSSP objectives. Delete, blackout, or remove unnecessary information, if feasible.

4. Maintain control over PHI at all times. Do not leave PHI around for unauthorized access or use (i.e., leaving client files open while not in use, leaving PHI on the desk when not working on the UR).

During On-Site UR:

1. Interview MSSP site staff to identify their internal controls over client files and personal information while under UR (i.e., returning files at end of the day, locking the room where MSSP staff are performing fieldwork, or moving files to an approved location).

2. Maintain copies of client files in a secure location (i.e., ensure no copies are left behind on the copier, maintain copies in a locked case, and minimize the amount of PHI to be copied, as appropriate).

During Alternative Utilization Desk Review:

Maintain privacy of PHI while at a workstation to minimize access necessary to complete CDA's UR obligations (i.e., keep PHI in locked cabinets, log off of computer screens when not in use, and minimize open display of PHI while working with the documents on a desk).

Privacy Incident Reporting:

Identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to the MSSP Branch; and document security incidents and their outcomes.

1. Immediately report to the MSSP Branch Supervisor any breach of PHI. This may include lost or misplaced documents, exposure to unauthorized personnel, or lost data storage devices.

2. Identify, document, report, and retain records of security incidents.

3. Review formal documentation and determine whether the post-incident analysis requires security policies to be updated.

Notice of Privacy Practices:

The CDA MSSP Branch receives PHI as a Business Associate of an oversight agency for MSSP sites and does not issue separate notices of privacy.

Guidelines for Breach

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or privacy of the PHI. Compromise of the security or privacy of the PHI poses a significant risk of financial, reputational, or other harm to the individual.

In case of a breach:

1. Document the investigative details, as follows:
    a. Incident/Name
    b. Date of Event/Date of Discovery
    c. Number of Individuals Affected
    d. Point of Contact
    e. Brief Summary/Findings
    f. Source of Incident (who was responsible)

2. Conduct a risk assessment of the suspected or known breach to determine whether significant harm will result from the breach. When assessing risk, things to consider may include, but are not limited to, the following:
    a. Extent of breach (i.e., localized, depth, inadvertent, etc.)
    b. Secured or unsecured PHI
    c. Intentional or unintentional disclosure
    d. Number of individuals involved
    e. Type of information breached (i.e., Social Security numbers, zip codes, etc.)
    f. Whether electronic information is encrypted

3. Notify affected Individuals: When significant harm may result from the breach, the MSSP Branch Manager will ensure proper steps are taken to notify individuals within sixty (60) days of the breach.

4. If the breach involves more than 500 individuals, then the MSSP Branch will ensure notification to the proper authorities has been completed by CDA in accordance with United States Department of Health and Human Services' requirements.

5. Log the incident/breach on the MSSP Branch Incident/Breach Log and fill out CDA form 1025 with the following information:
    a. Description of what happened
    b. Date of breach
    c. Date of discovery
    d. Number of clients affected
    e. Description of types of unsecured/secured information breached
    f. Description of notification action taken
    g. Steps taken to mitigate breach and avoid similar breach in the future

Guidelines for Data Retention and Destruction

1. Records retained shall have privacy identifiers (i.e., name, date of birth, address, and Social Security numbers) removed, blacked out, or removed to the extent possible.

2. Destruction of these work papers shall be done through confidential removal services and in accordance with MSSP Archive Policies and Procedures.

Guidelines for Disclosure

PHI and privacy identifiers obtained through the MSSP process shall not be disclosed beyond the MSSP Branch. However, this policy does not preclude MSSP staff from conferring with authorized MSSP staff over findings and providing technical assistance.

Guidelines for Training

All new employees will receive training regarding this MSSP Field Policy prior to handling/being exposed to PHI/ePHI and personally identifiable information.

Annually, all MSSP Branch Staff are to:

- Review the policy
- complete the CDA Privacy and Information Security Awareness Training