Monterey County Behavioral Health
Policy and Procedure

Policy Number	356
Policy Title	Protected Health Information (PHI) Taken to Off-Site Locations
References	Code of Federal Regulations, Title 45, Section 160.103 (45 CFR 160.103; Definitions) 45 CFR 164.514 (De-identification; Minimum Necessary) 45 CFR 164.530 (Privacy Rule: Administrative Requirements: Safeguards; administrative, technical, and physical safeguards)
Form	None
Effective	August 28, 2014

POLICY

It is the policy of the Monterey County Behavioral Health (MCBH) to limit the removal of individually identifiable protected health information (PHI) from any office or healthcare facility unless absolutely necessary in order to provide services to our clients. In those cases where staff must transport or carry PHI off campus and away from County healthcare facilities, they must take steps to assure that the information is limited to the minimum necessary to accomplish the task at hand, and that appropriate administrative, technical and physical safeguards are employed to reduce the risk of a breach of privacy. No staff will be permitted to take, copy, or create PHI to carry with them to an off-site location unless permitted to do so by their supervisor and by County policy.

I. Safeguards:

Prior to removing PHI from the safety and security of a County office or facility, staff shall take the following steps:

A. Administrative Safeguards

1. Staff must assure that the creation, use or transport of PHI away from their office or facility is necessary to their job and no reasonable alternatives exist.

2. Staff should confirm that County policy and their supervisor permits the creation, use, or transport of the PHI away from the office or facility in the manner proposed, and the supervisor is aware that this staff person is engaged in this practice.

3. Staff must assure that only the "minimum necessary" information is taken, and that no identifying information is included with the PHI that is extraneous or unnecessary to the task at hand. De-identification of as much of the PHI as is feasible should be done prior to removing it from the office or facility; for example, if a page from the chart will suffice, only that page should be copied and taken. Similarly, if the client's name,

address and phone number are needed for a field case worker to contact and meet with the client, the client's birth date and social security number should not be included with the "paperwork" that leaves the office or facility; if initials or first name/last initial or vice versa suffices, full names should not be used.

4. After the visit or task is finished, the PHI should be promptly returned to the office or facility and stored securely; or, if it is not part of the designated record set and is no longer needed (for example, a brief list of client names and addresses to be seen that day) it should be shredded or otherwise destroyed as appropriate.

B. Physical Safeguards

1. Any paper documents containing PHI should be kept with staff at all times. PHI should not be left on a table, in an office, or in any private or public place where it is not constantly within sight and control of staff.

2. If documents cannot be returned the same day that they are removed from the office or facility, they should be kept with staff inside their home rather than in a locked vehicle. Staff must not allow unauthorized household members to view the documents.

3. If documents must be kept in a locked vehicle, for example while other clients are seen in their homes, they should be kept in the locked glove box or trunk of the car, or otherwise covered or kept out of sight, so that it is not apparent that PHI or other confidential information is in the car.

C. Technical Safeguards:
View the following Monterey County Information Technology policies at http://www.in.co.monterey.ca.us/infosec/:

- Monterey County Information Security & Privacy Appropriate Use Policy
- Monterey County Security & Privacy Security Policy
- Monterey County Security & Privacy Data Privacy Policy
- Monterey County Information Security & Privacy Social Media Usage Policy
- Monterey County Information Security Standards

Briefly, the following steps must be taken:

1. If PHI is on a laptop computer or other electronic device such as a phone, the device must be password protected and PHI stored on it should be encrypted.

2. Personal electronic devices should not be used to routinely store PHI and any PHI that is temporarily on such a device should be promptly removed/deleted when it is no longer needed.

3. Personal electronic devices should be equipped with lost device "wiping capability" so that if the device is lost, misplaced or stolen, the data on it can be remotely erased.

II. Breach or loss of PHI "in the field":

If any of the paperwork, written information, client chart, or any electronic device with PHI on it is lost, misplaced or stolen, a breach report must be filed with MCBH Quality Improvement (QI) so that a proper investigation can be conducted, and if necessary, the patient can be notified and the breach reported.