

## **Identity Theft Prevention**

### **Policy**

It is the policy of Mid-Ohio Psychological Services to ensure that every effort be taken to avoid identity theft. To this end, Mid-Ohio Psychological Services will comply with Federal and State regulations and laws governing identity theft. It is the responsibility of the Executive Director and the Administrative Coordinator to develop and implement procedures to facilitate compliance with Federal and State regulations/laws to reduce the probability that identity theft can occur within the organization.

### **Procedure**

In these procedures, “staff” refers to all agency staff members including non paid staff such as interns and volunteers.

- A. Staff will ask clients to provide identification at the first session.
  1. Staff will request documentation of identity and make copies of the documentation provided:
    - a) Examples of evidence of identity include but are not limited to: Driver’s license, passport, or other government issued photo ID.
    - b) If the photo ID does not have current address, staff will request a utility bill, lease, or other evidence of current address.
    - c) Current insurance, Medicare, or Medicaid card.
  2. Staff will verify that the ID photo looks like the client and that other descriptions in the ID, like height and weight, appear to be correct.
  3. Copies of this information shall be kept in the client’s file.
- B. Clinical and Support Staff will be alert to and act on evidence of fraud.
  1. Staff shall be alert to suspicious activity such as:
    - a) Identification documents that appear altered or forged
    - b) Information provided by the client is inconsistent e.g., information on one form of identification submitted is different from information on another form of identification (such as age, address, occupation)
    - c) Suspicious change of address notice (for example a move from an expensive to an inexpensive neighborhood)
    - d) Evidence that paper or electronic records may have been compromised, for example, you discover that a staff member accessed client files without authorization, or that locked client files have been broken into.

2. Staff shall act upon suspicious activities or evidence of identity theft as appropriate by:
  - a) Checking with other members of the agency regarding suspicious events. For example, if staff receives a suspicious change of address notice, staff will ask the clinical staff treating that client to consider whether such a change is consistent with information the client has reported in treatment.
  - b) Contacting the client to verify suspicious information
  - c) If there is still a suspicion of identity theft after taking the verification steps above, contacting local law enforcement after obtaining the client's permission.
  - d) Changing password on electronic record accounts that may have been compromised
  - e) Notifying clients where it appears that they may have been victims of identify theft.
- C. The agency will respond to reports of identity theft by reporting concerns to clients, law enforcement, and others as appropriate.
- D. The agency will ensure that support and clinical staff are trained on implementing the policies.
  1. Support and clinical staff will be trained in the implementation of these policies
  2. Support and clinical staff will be required to review this policy and procedure annually.
- E. The agency will have business associates sign *Red Flag Agreements*. The agency will determine whether it has business associate who handles client information, e.g., billing services, collection agencies, accountants. It will ask those business associates to do one of the following:
  1. Sign an addendum to the business associates contract that the agency already has in place as part of HIPAA Privacy Rule/Security Rule compliance; or if no business associates contract is in place,
  2. Sign a standalone agreement, or
  3. Provide a copy of its own Red Flags Program and state that such Program meets the requirements of the Federal Red Flag Rules.
- F. The agency will re-evaluate these procedures periodically. The agency will annually re-evaluate whether these policies and procedures are effective and appropriate for detecting and preventing identify theft in light of the agency's actual experience with actual or suspected identity theft and in light of any new information learned by the agency regarding identity theft risks.

## **Red Flag Agreement for Business Associates**

This Agreement is made between Mid-Ohio Psychological Services, Inc (Agency) and \_\_\_\_\_ (Business Associate).

The parties are agreeing to take such action as necessary to comply with the requirements of the Federal *Red Flag Rules*. The purpose of this Agreement is to make the Agency compliant with the requirements of the *Red Flag Rules* (12 CFR Section 681.2, (b) (10) and (e)(4)) and that the Agency ensure that the activities of the Business Associate will be conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

A. Business Associate shall be alert to and act on evidence of fraud.

Business Associate shall be alert to suspicious activity such as:

1. Identification documents that appear altered or forged
2. Information provided by client is inconsistent, for example, information on one form of identification submitted is different from information on another form of identification (such as age, address, occupation)
3. Suspicious change of address notice (for example a move from an expensive to an inexpensive neighborhood)
4. Evidence that your paper or electronic records may have been compromised, for example, you discover that a staff member accessed client files without authorization, or that locked client files have been broken into

Business Associates shall act upon suspicious activities or evidence of identity theft as appropriate by notifying Agency as follows:

1. Notifying the Agency of suspicious activity
2. Investigating any suspicious activity that may have occurred within Business Associate's operation, for example unauthorized access by Business Associate's employees
3. Taking corrective action to the extent that suspicious activity appears to have occurred within Business Associate's operation
4. Changing passwords on electronic record accounts that may have been compromised
5. Notifying Agency where it appears that Agency or its clients may have been victims of identity theft

B. Business Associates will ensure that its staff is trained on implementing this agreement. Business Associate's management and employees will be trained in the implementation of these polices. Business Associate's management and employees will be given a copy of this policy to read and initial.

BUSINESS ASSOCIATE:

AGENCY:

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name and Title

\_\_\_\_\_  
Print Name and Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date