Weber Human Services
Identity Theft Prevention Policy

Purpose:
Weber Human Services (WHS) is committed to protecting the privacy of the Protected Health Information ("PHI") of our clients and the Personal Information ("PI") of both our clients and our employees. Identity Theft Prevention Policy (the "Policy") guides this commitment as it achieves the following purposes:

1. To detect, prevent, and mitigate Identity Theft and other forms of fraud regarding the disclosure or use of the PI and/or PHI of any client, employee, or any other individual related to WHS business;
2. To provide a process and related guidance for investigating allegations of Identity Theft resulting from a breach of security, or from the unauthorized acquisition and/or use of an individual's PI and/or PHI; and
3. To provide a process for appropriately notifying affected individuals and government agencies upon a breach of security or upon the unauthorized acquisition and/or use of an individual's PI and/or PHI.

Applicable Law:
The federal Red Flags Rule requires WHS to design and implement a written identity theft prevention program to prevent, detect, and mitigate identity theft in connection with certain accounts. WHS is subject to the Red Flags Rule because the Rule considers healthcare providers to be the "creditors" of their clients.

Scope:
This Policy applies to all WHS employees and anyone associated with WHS (collectively referred to herein as "WHS"). This Policy should be read in conjunction with applicable HIPAA privacy and security policies.

Policy:
It is the policy of WHS to:

1. Follow procedures to detect and investigate Identity Theft or breaches of PI or PHI;
2. Investigate all reports of a breach of security or of an unauthorized acquisition and/or use of the PI or PHI of any client, employee, or any other individual related to WHS business.

Definitions:
See Attachment A for explanation of the defined terms used in this Policy and Procedure Document.

Procedure—Red Flags and Identity Theft:

1. Identification of Red Flags and Identity Theft: Although not all WHS employees typically deal with Covered Accounts, all WHS employees, physicians, other clinicians should be familiar with

how to identify Identity Theft. Generally, an individual may become aware of potential Identity Theft from the following sources:

a. Suspicious documents;
b. Suspicious PI or suspicious identifying information;
c. Suspicious or unusual use of Accounts; and/or
d. Alerts from clients, employees, victims of Identity Theft, law enforcement, or others.

All reports or allegations of Identity Theft shall be directed to the Corporate Compliance Officer. However, depending on the nature of the allegation, the following people should first be contacted:

- Allegations pertaining to client information shall be directed to the Privacy Officer who will also notify the Corporate Compliance Officer.
- Allegations pertaining to information stored or maintained in computer systems shall be reported to the Security Officer who will notify the Corporate Compliance Officer.

For examples of more specific Red Flags and related prevention procedures and resolutions, please see Attachment B.

2. Detection of Red Flags and Identity Theft: WHS employees, physicians, other clinicians must also make efforts to detect Red Flags and Identity Theft. Those efforts should include, at a minimum:
    a. Require identification (such as by a driver's license or other government issued identification, insurance card);
    b. Verify forms of identification if necessary;
    c. Verify requests for change of billing address; and
    d. Verify identification and authority before releasing identifying information.

*Note that in the event of suspected Identity Theft, WHS physicians and other clinicians should report the matter to the applicable department manager for follow-up and response. The physicians' and clinicians' primary responsibility is the care and treatment of the client. The manager shall be responsible for reporting to the Corporate Compliance Officer.

3. Response to Red Flags and Identity Theft: The following steps may be taken to respond appropriately to Red Flags and instances of Identity Theft in order to prevent further Identity Theft and possibly reduce the harm caused by Identity Theft:
    a. Monitoring an Account for evidence of Identity Theft;
    b. Contacting the client or Colleague;
    c. Changing any passwords, security codes, or other security devices that permit access to an Account;
    d. Reopening an Account with a new Account or medical record number,
    e. Not opening a new Account;
    f. Closing an existing Account;
    g. Not attempting to collect on an Account or not referring an Account to a debt collector;
    h. Notifying law enforcement; and/or

i. Determining that no response is warranted under the particular circumstance.

4. Program Administration: WHS Colleagues shall be trained in Red Flag identification and Identity Theft prevention in accordance with their duties. WHS's program to identify Red Flags and prevent Identity Theft (the "Identity Theft Prevention Program") shall be updated periodically to reflect changes in risks of Identity Theft to clients, Colleagues, and others based on such factors as:
    a. WHS's experience with Identity Theft;
    b. Changes in the methods of Identity Theft;
    c. Changes in the methods to detect, prevent, and mitigate Identity Theft;
    d. Changes in the types of Accounts that WHS offers or maintains; and
    e. Changes in WHS's business arrangements.

ATTACHMENT A
DEFINITIONS

A. General Definitions

"Colleagues" means all WHS employees and temporary, per diem personnel, volunteers, students and others rendering paid or unpaid services to WHS, including all WHS agents.

B. Red Flags and Identity Theft Definitions

"Account" means a continuing relationship established by: (1) a client with WHS to obtain health care services in exchange for payment by the client or a third party; or (2) a Colleague to provide services in exchange for payment by WHS.

"Covered Account" means (1) any Account WHS offers or maintains, primarily for personal (client or employee) purposes, that involves multiple payments or transactions, including one or more deferred payments; and (2) any other Account WHS identifies as having a reasonably foreseeable risk of Identity Theft. WHS has identified the client billing and payment plans and other types of deferred payment plans as Covered Accounts. Covered Accounts and Accounts are used interchangeably in this Policy.

"Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

1. Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code; or
4. Telecommunication identifying information or access device (as defined in 18 USC 1029(e).

"Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. Examples of Red Flags include: alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; the presentation of suspicious documents; the presentation of suspicious personal identifying information such as a suspicious address changes; the unusual use of, or other suspicious activity related to an Account; and notice from clients, Colleagues, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with client Accounts or Colleague Accounts.

Attachment B

Red Flag Identification and Identity Theft Prevention Procedures

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	POSSIBLE RESOLUTION OF RED FLAG
Documents provided for identification appear to have been altered or forged.	Stop the admissions/billing process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Personal identifying information provided by the client is not consistent with other personal identifying information provided by the client. For example, there is a lack of correlation between the SSN range and date of birth.	Stop the admissions/billing process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
The SSN provided is the same as that submitted by other persons opening an Account or other clients.	Stop the admissions/billing process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Client has an insurance number but never produces an insurance card or other physical documentation of insurance.	Stop the admissions/billing process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with client.
Records showing medical treatment that is inconsistent with an examination or with a medical history as reported by the client.	Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: age, race, and other physical descriptions may be evidence of medical identity theft.	Depending on the inconsistency and review of previous file, either delay/do not open a new account, or terminate services. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with client.
Complaint/inquiry from an individual based on receipt of: • A bill for another individual • A bill for a product or service that the client denies receiving • A bill from a health care	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.

provider that the client never patronized • A notice of insurance benefits (or EOB) for health services never received		Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with client.
Mail sent to the client is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the client's account.	Verify client's current mailing address.	Client is found and contact information is updated.
WHS is notified by client, a victim of identity theft, a law enforcement authority, or any other person that it has open a fraudulent account for a person engaged in identity theft.	Investigation to determine if billing was made fraudulently.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with client.
Personal identifying information provided by the client is associated with known fraudulent activity as indicated by internal or third-party sources. For example: • The address on an application is the same as the address provided on a fraudulent application; or • The phone number on an application is the same as the number provided on a fraudulent application.	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with client.