

Applicability:	UW Medicine Affiliated Covered Entity
Policy Title:	Identity Theft Prevention
Policy Number:	COMP.302
Superseded Policy:	PP-31
Date Established:	October 11, 2017
Date Effective:	November 24, 2020
Next Review Date:	November 24, 2023

PURPOSE

The following policy establishes the UW Medicine Identity Theft Prevention Program (ITPP) for new and existing patient accounts and sets the requirements for identifying, investigating and responding to identity theft red flags involving patient accounts.

DEFINITIONS

See [UW Medicine Compliance Glossary](#).

POLICY

The University of Washington (UW) is subject to Identity Theft Rules, 16 C.F.R. § 681, which imposes specific duties regarding the detection, prevention and mitigation of identity theft on creditors, including non-profit organizations and government entities that maintain covered accounts, including the requirement to develop and implement a written ITPP. The [UW Administrative Policy Statement \(APS\) 35.2 Identity Theft Prevention: Red Flag Rules](#) sets forth the UW level ITPP and applies to all UW covered accounts.

UW Medicine maintains and administers an ITPP to detect, prevent and mitigate identity theft in connection with new or existing patient accounts. UW Medicine entities collect registration and billing information to create patient accounts and/or bill for the provision of healthcare services. Patient accounts are a specific subset of covered accounts. UW Medicine has established a specific ITPP for this subset of covered accounts. Where appropriate, the UW Medicine ITPP incorporates safeguards established by the UW guidelines. For all other types of covered accounts, UW Medicine adheres to [UW APS 35.2](#) and the [UW Guidelines for Preventing, Detecting and Mitigating Identity Theft](#).

The UW Medicine ITPP includes the following components:

1. Risk assessment;
2. Internal safeguards to prevent and mitigate identity theft;
3. A list of relevant red flags for patient accounts;
4. Recommended procedures to follow when red flags are detected; *and*

5. Standard contract language requiring entities that provide services associated with patient accounts to have policies and procedures to detect, prevent and mitigate the risk of identity theft.

The Chief Compliance Officer is the designated UW Medicine official responsible for the following: overseeing development and maintenance of the UW Medicine ITPP; overseeing training of workforce members; establishing requirements and timelines for entity status reports; coordinating system-wide assessments and case management for issues involving multiple entities; updating the program as needed; and preparing status reports.

I. Verifying Patient Identity

UW Medicine workforce members shall verify patient identity at every visit. Acceptable documentation is government issued photo identification (ID) (for example: passport, driver's license or equivalent, military or tribal ID or permanent resident card).

- A. Upon initial registration, adult patients are asked to show documentation of identity that includes address information, with the following exceptions:
 - a. If the patient requests emergency evaluation or treatment, UW Medicine will not delay a medical screening examination in order to obtain documents verifying identity.
 - b. Workforce members may use professional judgment to waive the production of photo ID if a delay in care could put the patient's health and safety at risk.
- B. If the patient refuses or is unable to provide a photo ID, the workforce member documents that the photo ID was "not provided" in the document status field in the registration system. If the document status field already indicates "not provided" and the provision of care is not required under the Emergency Medical Treatment and Labor Act, the workforce member consults their manager to determine if the appointment should be re-scheduled to another time when the patient can provide a valid ID.
- C. The documents provided at initial registration may be scanned into the electronic medical record and used to verify the patient's identity on subsequent visits.
- D. On all subsequent visits, UW Medicine workforce members re-verify patient identity. Workforce members may use professional judgment to verify the identity of patients they know by sight without requiring them to produce photo ID.

II. Red Flags

UW Medicine workforce members shall be alert to the red flags for patient accounts.

- A. Examples of red flags for patient accounts include, but are not limited to:
 - A complaint or question from a patient based on the following types of (or similar) issues:
 - A bill for another individual;
 - A bill for a product or service that the patient denies receiving;

- A bill from a healthcare professional that the patient never patronized;
 - A notice of insurance benefits (or explanation of benefits) for health services never received;
 - Collection notice from bill collector.
 - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
 - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
 - Identifying information given by the patient is not consistent with the entity's records or with other information furnished by the patient.
 - The Social Security Number (SSN) furnished by the patient has not been issued, is listed in the Social Security Administration's Death Master File, or is otherwise invalid. The following numbers are always invalid:
 - The first three digits are in the 800, 900, or 000 range, are in the 700 range above 772 or are 666;
 - The fourth and fifth digits are 00; *or*
 - The last four digits are 0000.
 - The SSN or other identifying information furnished by the patient is the same as the SSN or other identifying information for a different individual in the entity's records.
 - The address given by the patient does not exist or is a post office box.
 - The phone number given by the patient is invalid or is associated with a pager or an answering service.
 - The patient fails to furnish identifying information or documents or cannot provide it after repeated requests.
 - Information in the medical record differs from information provided by the patient or found on clinical examination.
 - The patient's signature does not match the signature attributed to the patient in the entity's records.
 - The entity receives notification from patients, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts held by UW Medicine.
 - The entity receives a notice of address discrepancy¹ from a consumer reporting agency.
- B. The list above is not exhaustive. Workforce members should be alert for other types of discrepancies in information relating to patient identification.
- C. Workforce members who become aware of red flags or discover other indications of potential identity theft shall immediately report the information to their manager. Managers shall then report to UW Medicine Compliance or their entity Patient Identification and Clarification Committee.

¹ Communication from a consumer reporting agency in response to a UW Medicine request for a patient's credit report that indicates a substantial difference between the patient's address in the request and the patient's address in the reporting agency's files.

III. Investigations

UW Medicine shall investigate concerns involving potential identity theft associated with patient accounts.

- A. Each entity shall assign responsibility for investigating and responding to red flags in accordance with entity procedures and generate periodic status reports to entity leadership and UW Medicine Compliance.
- B. If it is determined that a patient is a victim of identity theft, the following actions shall be taken:
 - 1. Promptly isolate and correct any inaccuracy in the patient's designated record set;
 - 2. Notify the patient in writing or by phone;
 - 3. Instruct billing areas to cease collection; if the account has been referred to a collection agency, instruct the collection agency to cease collection activity;
 - 4. Cooperate with any law enforcement investigation;
 - 5. Ascertain whether an insurance company, government program, patient or other payor has made payment on the account, notify the payor of the incident and arrange for a refund of the amount paid;
 - 6. If an adverse report was made to a consumer reporting agency, notify the agency of the incident and explain that the account was not the responsibility of the patient; *and*
 - 7. Notify all other UW Medicine entities as necessary to resolve and/or restore the accuracy of account information.

IV. Remediation

When identity theft involves a UW Medicine patient's record, any documents identified as not belonging to the patient shall be segregated and any information relating to the identity theft shall be removed, marked in error or suppressed (as applicable to whether paper documents or electronic systems are affected).

V. Address Discrepancy

When UW Medicine receives a notice of address discrepancy from a consumer reporting agency, UW Medicine shall verify that the report relates to a patient about whom the information is requested.

VI. Endorsement

The UW Medicine Board Compliance Committee shall review and endorse the UW Medicine ITPP, including any material changes to the program.

REGULATORY/LEGISLATION/REFERENCES

- Identity Theft Rule, 16 C.F.R. § 681.

PROCEDURE ADDENDUM(S) REFERENCES/LINKS

- [UW Medicine Compliance Glossary.](#)
- [UW APS 35.2 Identity Theft Prevention: Red Flag Rules.](#)
- [UW Guidelines for Preventing, Detecting and Mitigating Identify Theft.](#)
- [University of Washington Social Security Number Standard.](#)

APPROVALS

/s/ Beth DeLair
Beth DeLair
Chief Compliance Officer, UW Medicine
Associate Vice President for Medical Affairs, UW

11/30/2020
Date