PURPOSE AND SCOPE
The following policy statements establish the UW Medicine Identity Theft Prevention Program (ITPP) for new and existing patient accounts and articulate key responsibilities for program oversight and implementation; verifying patient identity at the time of registration and subsequent visits; requirements for identifying and responding to identity theft red flags involving patient accounts; for correcting errors in the medical record/designated record set resulting from identity theft; verifying, correcting and resolving notifications of address discrepancy received from consumer reporting agencies involving UW Medicine patients.

This policy is applicable to all UW Medicine entities.

POLICY PRINCIPLES/STATEMENT
The University of Washington (UW) is subject to Title16, Code of Federal Regulations (CFR) Part 681 “Identity Theft Rules.” Section 16 CFR 681.2 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 Guidelines for Preventing, Detecting and Mitigating Identity Theft (http://www.washington.edu/admin/rules/policies/APS/35.02.html) set forth the UW level ITPP and apply to all UW covered 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 specific subset of covered accounts.

DEFINITIONS
1. Covered account means an account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or
transactions, or any other account for which there is a reasonably foreseeable risk from identity theft. Under the Identity Theft Rules, a UW Medicine patient account is a covered account.

2. **Creditor** means any entity that regularly extends, renews, or continues credit or any entity that regularly arranges for the extension, renewal or continuation of credit.

3. **Identity theft** means fraud committed using the identifying information of another person.

4. **Patient account**, for purposes of the UW Medicine ITPP, refers to a covered account that is offered or maintained by a UW Medicine entity for an individual in connection with the provision of healthcare services.

5. **Red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

6. **Designated record set** means an individual's medical and billing records maintained by or for a UW Medicine healthcare professional and used, in whole or in part, by or for UW Medicine to make decisions about the individual.

7. **Records** means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for UW Medicine.

8. **Notification of address discrepancy** means 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.

**POLICY**

I. UW Medicine will maintain and administer an ITPP in order to detect, prevent and mitigate identity theft in connection with new or existing patient accounts.

II. The UW Medicine Board Compliance Committee will receive periodic assessments of the effectiveness of the UW Medicine ITPP.

III. Workforce members who become aware of red flags, or discover other indications of potential identity theft will immediately report the information to their manager. Managers will then report to UW Medicine Compliance or their entity Patient Identification and Clarification Committee (PICC).

IV. The UW Medicine ITPP includes the following components:

- A. Risk Assessment;
- B. Internal safeguards to prevent and mitigate identity theft;
- C. A list of relevant red flags for patient accounts;
D. Recommended procedures to be followed when red flags are detected; and
E. 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.

V. UW Medicine will adhere to the UW Guidelines for Preventing, Detecting and Mitigating
Identity Theft for other types of covered accounts that may exist. Where appropriate, the UW
Medicine ITPP incorporates safeguards established by the UW Guidelines.

VI. UW Medicine will verify patient identity at the time of every visit.

A. Upon initial registration, adult patients will be asked to show documentation of
identity that includes address and insurance information except that: 1) if the patient
requests emergency evaluation or treatment, UW Medicine will not delay a medical
screening examination in order to obtain documents verifying identity; and 2) staff may
use professional judgment to waive the production of photo identification (ID) if a
delay in care could put the patient’s health and safety at risk.

B. On all subsequent visits, UW Medicine will verify patient identity using the documents
described below except that workforce members may verify identity of patients they
know by sight without requiring them to produce photo ID.

Documentation of Identity:

1. A government issued photo ID (for example: passport, driver’s license or
equivalent, military or tribal ID, or permanent resident card) is the preferred
identity documentation. These documents may be scanned into the electronic
medical record (EMR) and used to verify the patient’s identity on subsequent
visits.

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. When the document status field is already set to “not provided,”
and the provision of care is not required under the Emergency Medical Treatment and
Active Labor Act (EMTALA), the workforce member consults with their manager to
determine if the appointment should be re-scheduled and ID must be provided.

VII. All UW Medicine workforce members will be alert to discrepancies in documents, patient
information and the red flags for patient accounts. See examples of red flags in the FAQ
section below.

VIII. UW Medicine investigates concerns involving potential identity theft associated with patient
accounts. See related procedure section below.
IX. If it is determined that a patient has not been a victim of identity theft and there is an outstanding bill for services, UW Medicine will notify the patient in writing that he/she is responsible for payment and state the basis for its determination.

X. If it has been determined that a patient is a victim of identity theft, the following actions will be taken:

A. UW Medicine will promptly isolate and a correct inaccuracy in the patient’s designated record set;
B. Notify the patient in writing or by phone;
C. Instruct billing areas to cease collection. If the accounts had been referred to collection agencies, the collection agencies will be instructed to cease collection activity;
D. Cooperate with any law enforcement investigation;
E. 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;
F. If an adverse report had been 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
G. Notify all other UW Medicine entities as necessary to resolve and/or restore the accuracy of account information.

XI. When identity theft involves an individual receiving care under the name of another person who has been a UW Medicine patient, any documents identified as not belonging to the known patient will be segregated to prevent them from being read or used in the patient’s treatment. In such cases, all files relating to the patient will be reviewed; any information relating to the identity theft will be removed, marked in error or suppressed (as applicable to whether paper documents or electronic systems are affected).

XII. When a notice of address discrepancy is received from a consumer reporting agency, then UW Medicine will verify that the report relates to a patient about whom the information is requested. For more information, see related procedure section below.

REGULATORY/LEGISLATION/REFERENCES
- Identity Theft Rules, 16 C.F.R. § 681
  (http://www.access.gpo.gov/nara/cfr/waisidx_08/16cfr681_08.html)

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

Cross References
- APS 35.2 Identity Theft Prevention: Red Flag Rules
  http://www.washington.edu/admin/rules/APS/35.02.html
- HMC Policy 135.17, Patient Identification Clarification Process
• UW Medicine Compliance Policy: PP-11 Verifying the Identity and Authority of Individuals requesting Disclosure of Protected Health Information.
• UW Medicine Master Patient Index Affiliation Policies and Procedures
• UW Medicine Registration Standards Policy on Names
• HMC Policy 5.77 Patient Identification
• HMC Policy 100.12 Electronic Alerts
• UWP Identity Theft Program
• UW Medicine Compliance Policy: PP-24 Amendment of Protected Health Information
• UW Medicine Compliance Policy: PP-25 Accounting of Disclosures of Protected Health Information
• UW Medicine Compliance Policy: PP-26 Definition of a Designated Record Set
• University of Washington Social Security Number Standard

Related Procedures

1. To initiate an investigation, request the following:
   a. Copy of a signed photo ID (such as a state driver’s license);
   b. Copy of the filed police report for identity theft;
   c. Completed and signed copy of one of the following:
      i. The ID theft complaint form supplied by the Federal Trade Commission (FTC); or
      ii. A written statement that includes the following information:
         • A declaration that the individual is a victim of identity theft;
         • Any other identification document that supports the statement of identity theft;
         • Specific facts supporting the claim of identity theft;
         • Any other explanation that the individual did not incur the debt;
         • Correspondence disputing the debt;
         • Documentation of the residence of the individual at the date of service, (examples include copies of utility bills, tax statements or other statements from businesses sent to the individual at his or her residence);
         • A telephone number for contacting the individual;
         • Concerns regarding the person who registered in his or her name;
         • A statement that the representations are true, correct and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification.

2. Address discrepancy review:
   a. Compare information received from the reporting agency with entity records (for example: registration changes, change of address notifications and account information).
b. Contact the patient to verify address.
c. Utilize other reasonable means to verify that the correct address is associated with the patient and consumer report.

After establishing a reasonable belief that the correct address is known, the entity will promptly provide it to the reporting agency that issued the notification of address discrepancy.

**Related Guidelines**
Guidelines provide best-practice advice.

**Frequently Asked Questions (FAQs)**
Examples of red flags:

1. A complaint or question from a patient based on the patient’s receipt of:
   a. A bill for another individual;
   b. A bill for a product or service that the patient denies receiving;
   c. A bill from a healthcare professional that the patient never patronized; or
   d. A notice of insurance benefits (or explanation of benefits) for health services never received;
   e. Collection notice from bill collector.

2. The patient submits a driver’s license, insurance card, or other identifying information that appears to be altered or forged.

3. The photograph on a driver’s license or other photo ID submitted by the patient does not resemble the patient.

4. Identifying information given by the patient is not consistent with the entity’s records or with other information furnished by the patient.

5. The Social Security Number (SSN) furnished by the patient has not been issued, is listed on the Social Security Administration’s Death Master File, or is otherwise invalid. The following numbers are always invalid:
   a. The first three digits are in the 800, 900, or 000 range, are in the 700 range above 772, or are 666;
   b. The fourth and fifth digits are 00; or
   c. The last four digits are 0000

6. 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.

7. The address given by the patient does not exist or is a post office box.
8. The phone number given by the patient is invalid or is associated with a pager or an answering service.

9. The patient fails to furnish identifying information or documents or cannot provide it after repeated requests.

10. Information in the medical record differs from information provided by the patient or found on clinical examination.

11. The patient’s signature does not match the signature attributed to the patient in the entity’s records.

12. 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.

13. The entity receives a notice of address discrepancy from a consumer reporting agency.

The list above is not exclusive. Workforce members should be alert for other types of discrepancies in information relating to patient identification.

Additional Contacts
HMC PICC: hmcpicc@uw.edu
UWMC PICC: upicc@uw.edu

ROLES AND RESPONSIBILITIES
Roles and responsibilities associated with the oversight, implementation and management of the UW Medicine ITPP include the following:

1. The Chief Compliance Officer/Associate Vice President for Medical Affairs is the designated UW Medicine Official for the ITPP 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 a system-wide status report.

2. Each entity assigns responsibility for investigating and responding to red flags and generates periodic status reports.
   
   a. For Harborview Medical Center (HMC), Northwest Hospital & Medical Center (NWH), King County Public Hospital District No. 1 d/b/a Valley Medical Center and Clinics (VMC), UW Medical Center (UWMC), UW Neighborhood Clinics (UWNC) and Airlift Northwest (ALNW): Assistant Director of HIPAA Compliance, UW Medicine Compliance
b. For: Assistant Director of HIPAA Compliance, UW Medicine Compliance  
c. For School of Medicine: Director of Compliance, School of Medicine  
d. For UW Physicians: Compliance Officer, UWP  
e. For CUMG: Compliance Officer, CUMG

**AUTHORITIES**

<table>
<thead>
<tr>
<th>Custodian</th>
<th>Responsible Officer</th>
<th>Implementation Officer</th>
<th>Administrative Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td><strong>Owner</strong></td>
<td><strong>Auditor</strong></td>
<td><strong>Endorser</strong></td>
</tr>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Executive Compliance Committee</td>
</tr>
</tbody>
</table>

**APPROVALS**

UW Privacy Official  
Johnese M. Spisso, Chief Health System Officer,  
UW Medicine & Vice President for Medical Affairs, UW