FACULTY PRACTICE GROUP – Ambulatory Operations

STANDARDS AND GUIDELINES

UCLA Health System
Faculty Practice Group

SECTION:	Front Office Practice Operations	PAGE:	1 OF 4
SUBJECT:	Medical Identity Theft -- Prevention and Response Procedure	EFFECTIVE:	May 1, 2009

PURPOSE:

The purpose of this procedure is to establish Faculty Practice Group requirements and outline mechanisms to prevent, detect, and respond to identity/medical identity theft. These procedures are governed by federal, state and university policies to safeguarding information.

BACKGROUND:

The Federal Trade Commission (FTC) has issued a set of regulations known as "Red Flag Rules" requiring the development and implementation of medical identity theft prevention and detection. All UCLA Health System and Medical Sciences (UCLA) departments which work with "Covered Accounts" are required to implement a written departmental Identity Theft Prevention and Response Program" (Program) protecting those accounts for which payment owed from an outside entity (e.g. patient, third-party payor, lessee) is deferred until after the date of service or made via multiple periodic payments ("Covered Accounts"). The Program should include the following components: Prevention, Detection and Response (Investigation and Mitigation)

DEFINITIONS:

Workforce: All faculty, staff, students, trainees, volunteers, business associates who access restricted or confidential information during the course of their duties.

Medical Identity Theft: Medical identity theft occurs when someone uses a person's name and/or other parts of a person's identity, e.g. insurance information, without that person's knowledge or consent, to obtain medical services or goods or to make false claims for medical services or goods.

Photographic Identification (Photo ID): Means a driver's license, a State identification card, a public, government, or private employment identification card, a firearm owner's identification card, or an issued passport.

Identification: Means a birth certificate, health insurance card a social security card, a firearm owner's identification card, a credit card, a debit card, student ID or Resident Alien Card.

PROCEDURES:

Prevention:

- Ask for identification before services are rendered unless medical necessity dictates otherwise. Two forms of identification are recommended. One should to be a photo ID. When staff request photo identification, staff should explain the reason for the request to the patient or provide developed educational documents. *(See definition).*
- At minimum each practice should have a process to examine the photo-ID and the signature on it. Additionally the signature should be compared to any signatures obtained by the practice.
  - For patient's without a photo ID, ask the patient to validate key demographic information already in the registration database, *e.g., last 4-digits of SSN, DOB, MR#, current address and phone number, mother's maiden name, related parties, name of primary care physician (for established patients).*
  - Make sure patients know it is against the law to "share" their insurance coverage. This should be done through standardized signage in registration or admitting areas AND by adding to new patient letters (see recommended verbiage*)* --clearly informing patients at check in they will need to provide identification and one is a photo ID.

- For practices that provide non in-person service, a procedure to ensure patient identity should be implemented.

Detection:

Triggers of potential identity theft for identification –

1. Patient presenting does not match photo presented
2. Patient presents for an episode of care and is recognized by practitioners as someone other than the patient presenting himself/herself to be
3. Same name or date of birth, with changes in social security number
4. Different first name, with same last name or vice versa, but with the same social Security Number
5. Similarities in name and DOBs with a slight change in social security numbers
6. Multiple hyphenated names and they are given in different orders, or the name is not consistent with prior visits
7. Owner's name of the social security number does not match that of patient's name
8. Patient's behavior and goals of treatment are different than that claimed by the patient or are directed toward obtaining prescriptions
9. Clinical markers different from case to case
10. Patient presents with conditions or services clearly inconsistent with prior visits in the medical record
11. Patient admits to using another person's identity for services
12. Insurance information in patient database is different than that claimed by the patient.
13. Allergy and laboratory information is inconsistent with prior visits in the medical record
14. Patient receives bills or a collections notice for medical services that were not received
15. Patient notices discrepancies on the "Explanation of Medical Benefits" notice from their insurance company, Pro fee bill, or specimen bill, including payment for services not received
16. Patient notified of medical data breach
17. Billing complaints for services not received
18. Complaint or question from a patient based on the patient's receipt of a bill for another individual, for a product or service that the patient denies receiving; or a Notice of insurance benefits for services never received
19. Complaint or question from a patient about information added to a credit report by a health care provider (unpaid bill)
20. Dispute of a bill by a patient who is the victim of financial identity theft
21. Inconsistent medical records:
    - Medical records show treatment that is inconsistent with a physical examination or medical history as reported by the patient.
    - Personal information inconsistent with information already on file.
    - Name or address discrepancy on identification & insurance information:
    - Signature discrepancy, e.g., driver's license signature doesn't match the consent form signature
    - Address on file does not match address provided by the consumer
    - Mail sent to the customer is returned repeatedly as "undeliverable"
    - Possible duplicate records with inconsistent information.
22. Presentation of suspicious documents
    - Altered or forged documents
    - Photographic ID does not match the consumer presenting the ID

- SSN number – has not been issued or is listed on the SSA's Death Master File
- Invalid address or phone number; phone number associated with a pager or answering service

23. Lack of information: A patient who has an insurance number, but never produces an insurance card or photo ID or other physical documentation of insurance.
24. Notice from consumers, law enforcement or others of unusual activity related to a covered account

Response (Investigation and Mitigation)

Medical Identity Theft is suspected or discovered while patient is on-site:

- If services are for Emergent/urgent care, then care is provided as the first priority and the investigation of identity is addressed after care is stabilized. (EMTALA requirements).

- It is not the staff's responsibility to restrain the patient in any way if there is potential/actual identity theft.

  If staff suspect/detect Identity/Medical Identity Theft they are required to:

  - If possible, photocopy all identification presented.
  - Immediately notify the Practice Manager or designee.
  - The Manager should attempt to resolve obvious registration issues (e.g., change of address, maiden name).
  - If identity theft is suspected at the point of service, the Supervisor / Manager will approach the patient for verification of identification.
  - Review with the patient the importance of correct identification and patient safety.
  - If after speaking with the patient, the patient presents different information, proceed to gather the new information and process verification as per usual protocol, documenting interventions.
  - Immediately document any refusal to comply or any unresolved issue in the Compliance section of the Event Reporting system.
  - If the situation requires further investigation, the manager should notify the Compliance Officer.

1. The Compliance Officer will coordinate the investigation of potential identity theft incidents and will involve as necessary:
   - Risk Management
   - Legal Affairs
   - Privacy Officer
   - Patient Admissions and Registration-To apply any applicable alerts
   - Medical Records- Who after determination of identity theft will implement their departmental process for rectifying the Patient Record as appropriate
   - Billing departments -Who after determination of identity theft will follow their departmental process for rectifying the Patient Bill as appropriate
   - Information Security Officer
   - UCPD

2. If it is suspected or determined that there has been a breach of Personal Information under California State Law, UCLA Policy 420 will be followed to report the breach.

Medical Identity Theft is discovered after patient is discharged:

Critical Note: Prior to assuming identity theft in the event of a patient complaint, the department receiving the complaint, needs to discuss the circumstances with the patient in order to determine if the case is a result of mistaken billing or mislabeled medical records.

In order to do this the department needs to obtain as many facts as possible from the patient and then work with the appropriate department i.e.; point of care or billing to first ascertain the activity was not a mistake. To this end the department that receives the patient's call should obtain as much information as possible and clarify with the patient what they are expecting to have happen.

If there indeed has been a mistake the receiving department will work with HIMS and Billing as outlined above to remediate the patient bill and Medical Record as appropriate.

If after review of the circumstances the case is not a result of a mistake and appears to be Identity/Medical Identity Theft, the receiving department will contact the UCPD who will be responsible for conducting the initial investigation and notifying the appropriate departments and external law enforcement agencies as outlined above.

Patient Follow up:
Unless otherwise indicated by UCPD, Legal Affairs or Risk Management, the department that received the initial call should follow up with the patient regarding outcome or referral to other departments.

REVISION HISTORY

Effective Date:
Review Date:
Revised Date: