Policy Number: UFCD, Operations, 6.14
Effective Date: July 2009
Last Revised Date: April 2023
Next Review Date: April 2025
Policy/Guideline Custodian: Associate Dean of Clinical Affairs and Quality
Category: Operations-Clinical

Title
Red Flag Policy
Policy

Policy Statement

It is the policy of the College of Dentistry at the University of Florida to follow all federal and state laws, along with reporting requirements regarding identity theft. Specifically, this policy outlines how the college will: (1) identify, (2) detect and (3) respond to these red flags. This compliance program and associated policy is reviewed and updated by the Associate Dean for Clinical Affairs & Quality and the Director of Finance, and approved by the dean of the college as needed.

The Associate Dean for Clinical Affairs & Quality is assigned the responsibility of implementing and maintaining the Red Flag Rule requirements. Furthermore, it is the policy of the college that this individual is provided sufficient resources and authority to fulfill these responsibilities.

Pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

College employees, students and volunteers are required to protect sensitive patient information to the same degree as set forth in the policy. It is also the policy of the college that employees, students and volunteers who violate this expectation will be dealt with first by an attempt to correct the problem, and if that fails by possible termination or the discontinuation of services.

All appropriate employees, students and volunteers will be trained annually beginning with the August 1, 2009 compliance date on the policies and procedures governing compliance with the Protecting Social Security Numbers & Identity Theft Prevention. New members of the

workforce will receive training during the onboarding process. Students will receive training on these matters prior to entering clinics as primary providers. Training will also be provided should any policy or procedure materially change. This training will be provided within a reasonable time following the change. Furthermore, it is the policy of the college that training will be taken and documented through the Privacy Office.

PROCEDURES:

I. Identify red flags. In the course of caring for patients, the college may encounter inconsistent or suspicious documents, information or activity that may signal possible identity theft. The following procedures describe the process for detection and response to red flags.

1. A complaint or question from a patient based on a patient's receipt of:
   - A bill for another individual;
   - A bill for a product or service that the patient denies receiving;
   - A bill from a health care provider that the patient never patronized; or
   - A notice of insurance benefits (or explanation of benefits) for health care services never received.
2. Records showing dental treatment that is inconsistent with a physical exam or with a medical history as reported by the patient.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
4. A patient or health insurer report that coverage for legitimate services is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
6. A dispute of a bill by a patient who claims to be a victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
8. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud alert.

II. Detect red flags. College employees, and students will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. The college will verify patient identity, address and insurance coverage at the time of patient registration/check-in.

1. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
   - Driver's license or other photo ID;

- Current dental insurance card; and
- Utility bills or other correspondence showing current residence if photo ID does not show the patient's current address. If the patient is a minor, the patient's parent or guardian should bring the information listed above.

2. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have visited the practice within the last six months.
3. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.
4. Staff should be alert for the possibility of identity theft in the following situations:
   - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
   - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
   - Information on one form of identification is inconsistent with information on another form of identification or with information already in the practice's records.
   - An address or telephone number is discovered to be incorrect, non- existent or fictitious.
   - The patient fails to provide identifying information or documents.
   - The patient's signature does not match a signature in the practice's records.

III. Respond to red flags. If an employee, student or volunteer of the college detects fraudulent activity or if a patient claims to be a victim of identity theft, the college will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, the college will also apply its existing HIPAA security policies and procedures to the response.

If potentially fraudulent activity (a red flag) is detected by an employee, student or volunteer of the College of Dentistry:

1. The employee, student or volunteer should gather all documentation and report the incident to his or her immediate supervisor.
2. The supervisor will determine whether the activity is fraudulent or authentic.
3. If the activity is determined to be fraudulent, then the college should take immediate action. The UF Privacy Office should be contacted immediately for guidance which may include the following actions:
   - Cancel the transaction;
   - Notify appropriate law enforcement;
   - Notify the affected patient;
   - Notify affected dentists; and

- Assess impact to the practice.

If a patient claims to be a victim of identity theft:

1. An Incident Report should be completed and sent to the Privacy Office for documentation purposes.
2. The patient should be encouraged to file a police report for identity theft if it has not been done already.
3. The patient should be encouraged to complete the "ID Theft Affidavit" developed by the Federal Trade Commission (FTC), along with supporting documentation.
4. The college will compare the patient's documentation with personal information in the practice's records.
5. If following investigation, it appears that the patient has been a victim of identity theft the college will promptly consider what further remedial act/notifications may be needed under the circumstances.

If a patient requests a change in their personal information:

1. If in person or by phone prior to any changes, a question will be asked by the staff processing the change to verify the identity of the person.
2. The question/s would be the person's birth date and or driver license number.
3. Once the identity is verified the changes will be made to the information.

Definitions

A "red flag" as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

References

UF Privacy Office: Identity Theft Prevention Program and Red Flag Rules

Contact Information

Policy Contact

Dr. Panagiotis Zoidis, Associate Dean for Clinical Affairs and Quality
pzoidis@dental.ufl.edu

Important Dates

- Original Effective Date: July 20, 2009, Approved by: Dr. Teresa A. Dolan, Dean
- Revised: May 2014, Approved by: Dr. A. Isabel Garcia, Dean
- Revised: April 2023, Approved by: Dr. A. Isabel Garcia, Dean