

ALEXANDER MEDICAL GROUP

IDENTITY THEFT PREVENTION PROGRAM

Scope: Patients, and/or the person(s) responsible for a patient's financial obligations, may at times be in a continuing relationship to pay for services received from Alexander Medical Group (AMG). This policy is established to comply with Federal Trade Commission rules regarding identity theft, as applicable to AMG operations.

Policy: AMG will maintain reasonable policies and procedures to detect and mitigate identity theft related to personal information received or maintained by AMG for the purposes of obtaining reimbursement for services.

This program supplements, but does not replace or supersede, any policies, procedures or practices of AMG to protect the confidentiality, privacy, security or accuracy of individually identifiable health information or employee's personal information. The privacy and security of employee records and protected health information, including financial records will continue to be protected in accordance with existing applicable law and regulation as it may be amended from time to time.

Definitions: "Red Flags" are those patterns, practices or specific activities that signal possible identity theft. Red Flags include, but are not limited to, the following:

1. Suspicious documents such as
 - Identification cards or documents that appear to have been altered or forged, or contain information that is not consistent with existing records.
 - The photograph or physical description on identification cards or documents provided to AMG is inconsistent with the appearance of (or information known about) the individual
2. Suspicious personal identifying information, such as social security number in a range that does not correlate with date of birth, or invalid phone number or address that is not resolved with reasonable effort to obtain accurate information.

Procedure:**Detection/Reporting:**

1. Staff that suspect that a Red Flag has been implicated in relation to an individual with which AMG has a continuing relationship to obtain payment for services shall report such incident to his/her supervisor.
2. If the Red Flag cannot be reconciled after a preliminary review of available records, and review of additional information from medical records, comparison with other government-issued identification cards and/or documents, and after making reasonable attempts to obtain clarification from the patient, family and/or responsible party, the attached form should be completed promptly (“Identify Theft Report of Suspicious Conduct/Documents”) and provided to the Chief Financial Officer (CFO) or authorized designee.
3. Intentional Fraud: Any indication that an identification card, number and/or other eligibility information provided to AMG by or on behalf of an individual, in order to obtain coverage under commercial insurance plans, workers’ compensation, automobile accident coverage, government programs or other third party payers, is intentionally provided under fraudulent circumstances and/or does not belong to the individual presenting for admission or care and treatment will be reported to the CFO or authorized designee immediately. The attached form (“Identity Theft Report of Suspicious Conduct/Documents”) should be completed and provided to the CFO or authorized designee promptly.
4. Fiscal records related to the incident are retained in order to review the possible identity theft incident(s) until the matter is resolved. Fiscal records include, but are not limited to, the following:
 - a. Demographic information collected from a patient or responsible person,
 - b. Any transactions related to payment for services and/or deferred payment plans,
 - c. Documents related to insurance coverage or eligibility for third party reimbursement (Medicare, Medicaid, etc.)

Responses:

5. As appropriate to the situation and findings upon review, any of the following responses may be made:
 - Placing a flag or amendment in the patient's medical record and/or patient accounts file that indicates how the incident was resolved,
 - Providing notice to insurers/government programs and/or law enforcement agencies of a substantiated incident, subject to patient confidentiality protections,
 - Changing methods of security protections, such as passwords and security codes,
 - Closing patient accounts that were affected by the incident, and
 - Other appropriate responses to mitigate the situation.
6. Incidents that meet the definition of criminal identify theft, as defined in state law, will be reported to Legal Affairs/Corporate Compliance Officer, who will notify local law enforcement as necessary. The AMG Corporate Health Information Security and Privacy Officer is consulted when such reports are made to ensure that AMG policy and applicable law regarding privacy and security of patient's health information is followed.
7. Incidents that involve a breach by AMG of its policies to protect the security and privacy of patient's protected health information which results in unauthorized access or disclosure of patient/resident protected health information are also reported in accordance with the Health Information Security and privacy Incident Reporting policy.

Updating program:

8. The AMG Identity Theft Prevention Program, and/or related department procedures or guidance, will be updated as needed to reflect changing risks, alerts from law enforcement, industry practices, and changes in methods related to preventing and detecting medical identity theft.