Appalachian State University
Communication Disorders Clinic

RED FLAGS RULE POLICY
(IDENTIFYING AND RESPONDING TO INDICATIONS OF IDENTITY THEFT)

This policy is established by the Charles and Geneva Scott Scottish Rite Communication Disorders Clinic (subsequently referred to in this document as the "Clinic") to comply with The Federal Trade Commission's (FTC) Red Flags Rule, which requires certain businesses and organizations to develop a written program to identify warning signs, or "red flags", of identity theft.

The Clinic shall follow all federal and state laws and reporting requirements regarding identity theft. This policy outlines how the Clinic will identify, detect and respond to the Red Flags Rule mandated by federal law. A "red flag" is defined as a pattern or a specific activity which indicates possible identity theft.

This identity theft prevention and detection compliance program is hereby approved by the University Attorney's office, with an effective date of November 1, 2009, and is subject to revision, as required by federal or state law.

The Director of the Clinic is assigned the responsibility of implementing and maintaining the Red Flags Rule requirements and shall be provided sufficient resources and authority to fulfill those responsibilities. The Director of the Clinic will also serve as the privacy official for the Clinic.

Pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards shall be implemented to reasonably safeguard protected health information and other sensitive information related to patient identify from any intentional or unintentional use or disclosure.

All business associates must be contractually bound to protect patient health information to the extent required by, an as set forth in, this policy. Any business associate who violates this requirement will be required to correct the problem, followed by termination of the agreement/discontinuation of services, if after corrective action, the business associate's measures still fail to comply with this policy.

By the November 1, 2009, compliance date, all workforce members shall be trained regarding the policies and procedures governing compliance with the Red Flags Rule. All new members of the workforce shall receive training regarding these policies and procedures within a reasonable time period after employment. Such training shall be included in any orientation received by new employees. Training documentation will include the name of the workforce member and the date of training. Workforce members will be trained regarding changes to these policies and procedures within a reasonable time, but in no event will such training occur later than the effective date of such changes.
Training regarding changes to the Red Flags policies and procedures will be documented by indicating the names of personnel, the dates of training, and the subject matter.

Procedures

I. Identifying Red Flags – In the course of patient care the Clinic may encounter suspicious or inconsistent documents or activity that may signal identify theft. The Clinic identifies the

following as potential red flags. Procedures describing how to detect and respond to these red flags are included.

- A complaint or question from a patient based on the patient's receipt of the following:
  - A bill for another individual;
  - A bill for a product or service the patient denies receiving;
  - A bill from a health care provider the patient never patronized;
  - A notice of insurance benefits (explanation of benefits) for services never received.

- Records showing diagnostic, consultative or treatment services that are inconsistent with findings by the service provider, or inconsistent with a medical history provided by the patient.

- A complaint by a patient that health insurance benefits for legitimate services is denied due to benefits being depleted or a yearly/lifetime cap has been reached.

- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

- A patient who presents an insurance number but never produces an insurance card or other documentation of insurance.

- A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, to include [but not limited to] Medicaid and Medicare fraud alerts.

- Information provided by a patient that is inconsistent with documents provided by the referral source.

II. Detecting Red Flags – The Clinic staff will be alert to discrepancies in documents and patient information that suggest risk of identity theft or fraud. The Clinic will verify patient identify, address and insurance coverage at the time of patient registration.

- When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment [this request will be included in the written correspondence all patients receive after an appointment is made]:
  - Driver's license or other photo identification
  - Current health insurance card
  - If the patient or legal guardian does not have photo identification, they will be asked to bring a bill showing a current residence.
  - Foster parents or guardians must show proof of their status.

- When the patient arrives for the appointment, the patient will be asked to produce the information listed above. Copies will be made of both the photo identification and the insurance card. The copies will be placed in the client chart.

- When a chart is audited by the Billing Specialist, the photo identification information will be included in the chart audit form at the front of the chart.

- The clinician in charge of the case may need to have the client or parents stop by the office in order for the photo identification to be copied, or the clinician may need to verify the photo comparing it to the client or parents.

- Staff should be alert for the possibility of identity theft in the following situations:
    - The photograph on a driver's license or other photo identification 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 submitted by the patient is inconsistent with information on another form of identification or with information already in the patient's records.
    - An address or telephone number is discovered to be inconsistent, 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 for the patient;
    - If collected, the social security number or other identifying information in the patient's records is the same as identifying information in the practice's records for another patient, or the social security number is discovered to be invalid.

III. Responding to Red Flags – If an employee of the Clinic detects any suspicious activity that may suggest fraud or identity theft, or if a patient claims to be the victim of identity theft, it is to be reported to the director of the Clinic for investigation. If the fraudulent activity involves protected health information covered under the HIPAA security standards, the Clinic will apply its existing HIPAA security policies and procedures to the response as well.

If suspected fraudulent activity (i.e. red flag) is detected by an employee, the following procedures are to be followed:

- The employee should gather all documentation and report the incident to the Clinic director;

- The Clinic director in consultation with the University Attorney will determine whether the activity is fraudulent or authentic;

- If the activity is determined to be fraudulent, the Clinic will take the following immediate action:
    - Cancel any transaction made;
    - Notify appropriate law enforcement
    - Notify the affected person;
    - Notify affected clinical faculty and/or supervisory staff;
    - Assess impact to the practice.

If a patient claims to be the victim of identify theft, the following procedures are to be followed:

- The patient should be encouraged to file a police report for identity theft, if he/she has not already done so;

- The patient should be encouraged to complete the ID Theft Affidavit developed by the FTC, and should provide supporting documentation;

- The Clinic will compare the patient's documentation with personal information in the practice record;

- If following the investigation, it appears the patient has been a victim of identity theft, the Clinic will take proper remedial action (to include patient notification);

- The director will determine if any other records and/or service providers are linked to inaccurate information. The patient is responsible for contacting ancillary service providers;

- If following investigation, it does not appear the patient has been a victim of identity theft, the Clinic will take whatever action(s) it deems appropriate.