CAROLINAS COLLEGE OF HEALTH SCIENCES
POLICY AND PROCEDURE

ADMINISTRATIVE

SUBJECT: IDENTITY THEFT AND INFORMATION BREACH

REVIEWER: Dean of Administrative and Financial Services*
Dean of Student Services and Enrollment Management

POLICY

Carolinas College of Health Sciences values and respects the confidentiality of personal information which, if misused, could lead to identity theft. The college's practices and procedures will be designed to maintain the security and integrity of identifying information related to teammate and student records. Teammates of the college will implement those practices and procedures to prevent, detect, and mitigate breaches in the security of identifying information. Further, all college teammates will recognize and respond to "red flags" of identity theft. "Red flags" are defined as a pattern, practice, or specific activity that indicates the possible existence of a misuse of identifying information. College practices, procedures, and personnel awareness will comply with the commitments of Atrium Health to prevent identity theft, as described in the system's administrative policy Identity Theft and Information Breach (ADM.PH 200.16).

PROCEDURE

1. Teammates handling identifying information must prevent use by unauthorized internal and external parties by securing the information at all times.

2. Teammates will identify potential sources of identifying information. Examples include a person's first name or first initial and last name in combination with any of the following identifying information:
   - Social security number (SSN)
   - Driver's license
   - Checking or savings account number
   - Credit or debit card number
   - Personal Identification (PIN) code
   - Electronic identification numbers
   - Electronic mail names or addresses
   - Any other numbers or information used to access a person's financial resources
   - Medical information
   - Fingerprints
   - Passwords
   - Parent's legal surname prior to marriage
   - Unencrypted personal data

3. The teammate will be able to identify "red flags." Examples of "red flags" include but are not limited to:
   - Alerts, notification, or other warning received from consumer reporting or fraud detection agencies.
   - Presentation of suspicious documents.
   - Presentation of suspicious personal identifying information, such as unexplained or frequent address and phone number changes.
   - Unusual payment practices.
   - Notice of possible identity theft.
   - Duplicate or inconsistent addresses, telephone numbers, birth dates, or SSNs for different people or that do not work.
   - Questions about benefits for services that were not received.

- Documents that appear to be forged or altered, including insurance cards, driver's licenses, birth certificates, or other identifying documents.
- Missing computers, security codes, or other devices or information that could be used to access individual information.

4. Discrepancies or suspicions should be confirmed by detailed inquiry to determine the presence of a "red flag." If the explanation is plausible, then the information may be accepted.

5. To report a "red flag," the suspicion and supporting facts are presented to a member of the college's leadership team. If that manager concurs with the finding, the suspicion and supporting facts are presented to dean of administrative and financial services. If the dean concurs with the suspicion that the information provided by the individual is false, the incident will be reported immediately to the Red Flag Response Team by calling the Customer Care Line at 704-355-8363. The report includes:
   - Name, telephone number, and department of teammate making report.
   - Nature of the "red flag," information involved and date of occurrence.
   - Names of suspected perpetrator and victim.
   - Other relevant information.

6. The response team will use the Red Flag Response Team Procedure to investigate the incident.

7. In no event should college teammates contact the potential victim of the information breach unless instructed to do so by the response team.

8. The Identity Theft and Information Breach policy and procedure will be reviewed bi-annually.

REFERENCES

Related Policies to Consult
Atrium Health:

ADM.PHI 200.16 Identify Theft and Information Breach Policy
IS.PHI 600.01 Communications Environment Acceptable Use Policy

Adopted 4/09; Revised 2/13, 12/15, 8/18; Reviewed 5/20
*Denotes primary reviewer.