Exhibit OO12.x

UNIVERSITY of VIRGINIA
HEALTH SYSTEM

Vice President and Chief Executive Officer of the Medical Center

MEDICAL CENTER POLICY NUMBER NO. 0286

A. SUBJECT: Prevention, Detection, and Mitigation of the Theft of Patients' Identities

B. EFFECTIVE DATE: April 1, 2014 (R)

C. POLICY:

In accordance with the University of Virginia's overall Identity Theft Prevention Program ("Program"), the Medical Center is committed to preventing, detecting and mitigating the incidence of the theft of patients' identities ("identity theft"). This commitment includes coordinating, reviewing, and overseeing Medical Center policies and procedures in order to:

1. identify indicators of identity theft ("red flags");

2. detect identified red flags and respond appropriately to detected red flags in order to prevent and mitigate identity theft; and

3. respond to new or evolving risks

The Medical Center requires staff and employees to appropriately identify patients and confirm personal demographic information as well as insurance information at time of registration for each patient visit, during treatment, at time of billing, and before confidential patient information can be released. Additional policies relevant to the prevention, detection and mitigation of incidents of identity theft include Medical Center Policy No. 0021 "Confidentiality of Patient Information"; Medical Center Policy 0092 "Release of Patients' Protected Health Information"; Medical Center Policy No. 0027 "Charge Control and Documentation"; Medical Center Policy 0201 "Patient Identification", and Medical Center Policy 0253 "Verification for Release of Patient Information".

D. PROCEDURE:

1. Identifying red flags: the following are relevant "red flags," or indicators of possible identity theft (this list is not intended to be inclusive and may change from time to time):

   a. notification by a patient or patient's representative that an identity theft may have occurred;

   b. a complaint or question from a patient or patient's representative based on the patient's receipt of a bill for products or services which the patient denies that he/she (or his/her family member) received, or a notice of insurance benefits paid (or denied) for health products or services that were never received;

Exhibit OO12.x

c. records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient;

d. suspicious documentation, or documentation that appears to be altered or forged;

e. documents that contain information that does not match the characteristics of the presenting patient as to such factors as age, gender, race, demographic information (i.e., address or telephone number), insurance information or where appropriately requested, social security number;

f. identification or other information provided by the patient, family or visitors which does not match the identification provided on a prior visit;

g. notifications from third party payors of potential identity theft;

h. information provided by a patient that matches information submitted by another patient as to date of birth, social security number, medical record number, insurance, or demographic information;

i. a complaint or question from a patient about information added to a credit report by a health care provider or insurer;

j. a notice or inquiry from a law enforcement agency or an insurance fraud investigator concerning possible identity theft

2. Detecting and responding to red flags to prevent and mitigate identity theft

    a. When a red flag is detected that involves a patient, staff will immediately report the incident to the manager or administrator on call. The manager or administrator on call will then notify the Medical Center Corporate Compliance and Privacy Office ("Compliance") of the incident.

    b. Responsibilities of Compliance. When a red flag incident is reported, Compliance shall:

        i. coordinate an investigation of the red flag incident, which may include, but would not be limited to, interviewing the patient, reviewing the patient's registration and scheduling history; reviewing the patient's billing records, reviewing the patient's medical records, and determining any other points of contact between the patient and the Medical Center;

        ii. notify all appropriate areas, including Health Information Services and the University Physicians Group billing department and the Medical Center's Patient Financial Services or Continuum Home Health billing department so that they may place a hold on the patient's account pending outcome of an investigation;

        iii. ascertain what additional actions may be needed to determine whether an identity theft has occurred, and alert appropriate areas to carry out those actions. As appropriate, Compliance may also contact and/or cooperate with law enforcement agencies and/or investigators for third party payors;

Exhibit OO12.x

iv. report to the Medical Center CEO as to the outcome of the investigation of any identity theft incidents, making recommendations for preventing their recurrence.

3. Annual Report

The CEO of the Medical Center, or his/her designee who is at the level of senior management, shall report to the University Comptroller any significant incidents involving identity theft and shall also identify and bring to the Comptroller's attention any processes that increase the risk of identity theft.

SIGNATURE:

R. Edward Howell

R. Edward Howell, CEO, UVA Medical Center

DATE: 3/21/14

Medical Center Policy No. 0286 (R)
Approved March 2009
Revised March 2014
Reviewed March 2012
Approved by Special Advisor to CEO
Approved by Medical Center Administration