UNIVERSITY of VIRGINIA HEALTH SYSTEM

Vice President and Chief Executive Officer of the Medical Center

MEDICAL CENTER POLICY NO. 0021

A. SUBJECT: Confidentiality of Patient Information

B. EFFECTIVE. DATE: January 1, 2013 (R)

C. POLICY:

"Protected Health Information," or "PHI," consists of all individually identifiable health and billing/payment information about a patient regardless of its location or form. Health information is "individually identifiable" if it includes any one of the identifiers listed in Appendix A. Protected Health Information ("PHI") may not be disclosed except when necessary to support treatment, payment or business operations, when authorized by the patient, or as otherwise permitted or required by law. Every person employed or otherwise providing services, or receiving training, in any capacity by or within the Medical Center that includes access to Protected Health Information, including all persons involved in healthcare education and research (collectively, "Personnel"), must comply with this requirement.

Physical, administrative and technical safeguards to be used for protecting PHI are contained in the Medical Center Corporate Compliance and Privacy Office Website (http://www.healthsystem.virginia.edu/pub/ccpo/privacy-office), and through hyperlinks provided in Medical Center Policy No. 0227 "Protection of Electronic Information and Information Systems." The original paper or microfilm chart may not be removed from Medical Center premises for any reason or under any circumstances, unless legally required. All individual-use electronic devices that store and/or transmit PHI over the Internet must be authenticated and encrypted using a Medical Center approved method of authentication and encryption to limit access to authorized recipients. (See also Medical Center Policy No. 202 "Internet and Intranet Access/ Usage").

D. PROCEDURE:

1. Personnel shall access and use only the PHI that they have a need to know as part of their authorized role-related duties.

2. Users of devices that store and/or transmit PHI shall follow the technical guidelines for encryption published at https://www.healthsystem.virginia.edu/technology/departments/health-system-technology/teams/information-security/guidelines/encryption.html.

3. All agreements with vendors of services and goods, where the vendor needs access to PHI, must include security and confidentiality provisions ("business associate" terms). Supply Chain Management is responsible for inclusion of business associate terms in agreements with vendors. (See Medical Center Policy No. 0189 "Medical Center Procurement Guidelines")

4. If confidential patient information needs to be stored off University of Virginia owned/leased premises, Personnel shall contact the University of Virginia Medical Center Facilities Services Business Manager who will coordinate the contacts between the requesting department and a vendor that has been contracted for record storage.

5. All Personnel will receive education upon first association with the Medical Center as well as during annual retraining regarding their roles in maintaining confidentiality of PHI. Each manager is responsible for implementing this policy and for developing department specific procedures required for safeguarding protected health information, as well as for ensuring that his/her employees are informed and educated as to their responsibilities under this policy. All such implementation and procedures shall conform to this policy and related confidentiality policies, including those referenced at the end of this policy.

6. Duty to Report Violations of Patient Confidentiality:

    a. All Personnel shall promptly (and in any event within twenty four hours) report any alleged, apparent or potential violations of confidentiality of PHI to both the manager/designee of the relevant area and the Corporate Compliance and Privacy Officer for investigation and follow up. For purposes of this subsection, "violations of patient confidentiality" shall mean any unauthorized acquisition, access, use or disclosure of protected health information.

    b. The Corporate Compliance and Privacy Officer shall:

        i. develop and implement policies and procedures for assessing each report to determine whether a notification of breach must be given to affected patients, the media and the Secretary of HHS, under the HITECH Act Rule on Breach Notification for Unsecured Protected Health Information, and

        ii. perform and document an assessment of each report and make any required notifications.

    c. In addition to reporting alleged, apparent, or potential violations of patient confidentiality to the Corporate Compliance and Privacy Officer, managers shall use a Quality Report (QR) to document reports. QR forms used for this purpose are to be forwarded to the Quality Office for review and a determination by that Office as to the appropriate action to be taken, if any, for quality assurance purposes. Managers shall also confer with the Human Resources Employee Relations Office, as necessary, for assistance in the reporting of, and follow up to, reports of patient confidentiality violations.

    d. Human Resources, the Quality Office, the Corporate Compliance and Privacy Office, and HSTS Security Office shall cooperate as required so as to ensure an appropriate and timely institutional response to reports of alleged patient confidentiality violations. Patient and family complaints regarding patient confidentiality shall be handled as required by Medical Center Policy No. 0070 "Patient Concerns and Grievances".

7. Appropriate corrective action will be taken regarding violations of this policy and other Medical Center Policies on confidentiality of PHI, including mitigation of any known harmful effect. Employee sanctions, which may include suspension or termination of employment as well as reporting to an applicable licensing board or other agency for serious misconduct, will be implemented as appropriate. (See Medical Center Human Resources Policy No. 707 "Violations

of Confidentiality"; see also School of Medicine Policy No. 1.431)

8. No retaliatory action will be taken against any person who files a complaint, participates in any proceeding, or otherwise engages in reasonable, good faith opposition to practices in violation of applicable privacy laws.

9. The Corporate Compliance and Privacy Officer shall develop and implement policies regarding PHI and handle complaints in coordination with those responsible under Medical Center Policy No. 0070 "Patient Concerns and Grievances". The Corporate Compliance and Privacy Officer shall also maintain a log of complaints received and their disposition.

   The Corporate Compliance and Privacy Office will report regarding patient confidentiality violations and other matters concerning confidentiality of patient information through the Health Information Management Subcommittee to the Quality Committee, to the Corporate Compliance Steering Committee, and to the Vice President and CEO of the Medical Center, the Associate Vice President for Hospital and Clinics Operations, and the Chief Information Officer.

10. A Notice of Privacy Practices was implemented effective April 14, 2003 describing uses and disclosures of, and patient rights and healthcare providers' duties regarding PHI. The Notice may be accessed at http://www.virginia.edu/uvaprint/HSC/pdf/030463.pdf and shall be posted at appropriate locations. The Notice shall be provided to all patients on the date of first service delivery, or as soon as reasonably practicable thereafter in emergency treatment situations. A good faith effort shall be made to obtain written acknowledgement of receipt of the Notice, except in emergency treatment situations. If acknowledgement is not obtained, the good faith effort and reasons why the acknowledgement was not obtained shall be documented.

SIGNATURE:

R. Edward Howell, CEO, UVA Medical Center

DATE: 12/21/12

Medical Center Policy No. 0021 (R)
Approved January 1984
Revised August 1990, May 1991, November 1994, November 1996, September 1999, November 2002, February 2004, September 2005, September 2007, December 2008, September 2009, March 2011, June 2011, December 2012
Approved by (Interim) Chief Technology and Health Information Officer
Approved by Medical Center Administration

Related confidentiality policies (non-inclusive list):
- Medical Center Policy No. 0193 – Electronic Mail (E-mail)
- Medical Center Policy No. 0194 - Faxing of Patient Information
- Medical Center Policy No. 0092 - Release of Patient's Protected Health Information

(SUBJECT: Confidentiality of Patient Information)

- Medical Center Policy No, 0163 - Access to Electronic Medical Records and Institutional Computer Systems
- Medical Center Policy No. 0084 - Health Information Request for Non-Patient Care Usage
- Medical Center Policy No. 0244 - Electronic Medical Record Access Auditing
- Medical Center Policy No. 0245 - Minimum Necessary Use and Disclosure of Protected Health Information
- Medical Center Policy No. 0251 - Use and Disclosure of Protected Health Information for General Fundraising Purposes
- University Policy – IRM-015 - Electronic Storage of Highly Sensitive Data

(SUBJECT: Confidentiality of Patient Information)

APPENDIX A: De-identification Standard

Health information is considered not individually identifiable if:

1. The following identifiers of the patient, and of relatives, employers or household members of the patient (collectively, the "individual"), are removed:

    a. Names;

    b. All geographic subdivisions smaller than a State, including street address, city, county, precinct and zip code, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

        i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
        ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

    c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

        i. Telephone numbers;
        ii. Fax number;
        iii. Electronic mail addresses;
        iv. Social security numbers;
        v. Medical record numbers;
        vi. Health plan beneficiary numbers;
        vii. Account numbers;
        viii. Certificate/license numbers;
        ix. Vehicle identifiers and serial numbers, including license plate numbers;
        x. Device identifiers and serial numbers;
        xi. Web Universal Resource Locators (URLs);
        xii. Internet Protocol (IP) address numbers;
        xiii. Biometric identifiers, including finger and voice prints;
        xiv. Full face photographic images and any comparable images; and
        xv. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual; and

2. The Medical Center has no actual knowledge that the remaining information could be used to identify the individual.