UNIVERSITY of VIRGINIA HEALTH SYSTEM

Vice President and Chief Executive Officer of the Medical Center

MEDICAL CENTER POLICY NO. 0163

A. SUBJECT: Access to Electronic Medical Records and Institutional Computer Systems

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

C. POLICY:

This policy applies to information contained in the electronic medical record (EMR), to billing systems containing protected health information, to those other Medical Center or departmental systems containing identifiable patient information, and to any and all other computer systems used at the Medical Center (collectively, "institutional systems").

Access to the EMR and to other institutional systems shall be granted only to those Covered Persons who have a legitimate need to know or to access such information for their work or training. Users of information in the EMR obtained *via* access to institutional systems shall also follow the guidelines contained in Medical Center Policy No. 0021 "Confidentiality of Patient Information".

D. PROCEDURE

1. Health Information Services in collaboration with the Health Information Management Subcommittee ("HIMS") in collaboration with Health System Technology Services ("HSTS"; formerly known as Health System Computing Services or "HSCS") shall grant access to institutional systems only to those Covered Persons who require such access for their work or training, and HSTS shall assign to each such person an access code or password. No Covered Person shall disclose access codes or passwords to any other person, nor shall anyone use another person's access code or password to access any institutional systems. Any person who has reason to believe that his/her access code or password, or that of another person, has been compromised shall report such occurrence to his/her supervisor and the HSTS Information Security Office. Automatic logoffs after a defined period of no activity will occur for institutional computer systems containing patient information. The timeout standards are located at https://www.healthsystem.virginia.edu/technology/departments/health-system-technology/teams/information-security/guidelines/automatic_logoff.html. All users shall log off all systems after completing their work.

2. Within forty eight (48) hours of a manager's/ supervisor's receipt of notification of a Covered Person's change of job duties, termination of employment, or termination of trainee status, the manager/supervisor shall notify the appropriate Human Resources office to initiate notification to the HSTS Information Security Office of the impending change (see also Medical Center Human Resources Policy No. 405 "Separation from Employment"; Medical Center Policy No. 0004 "Medical Center Identification"). The appropriate Human Resources office shall, within three (3)

business days of such notification, alert HSTS Information Security to take whatever timely action is required to ensure that such Covered Person's access to institutional systems is consistent with his/her change in status. If, due to an employee's termination, or for security reasons, immediate termination of access to institutional systems is required, managers/supervisors shall immediately (i.e., within 24 hours) notify the HSTS Information Security Office to take all necessary measures. Medical Center managers shall follow additional requirements set forth in Medical Center Human Resources Policy No. 405 "Separation from Employment". Additionally, at least annually, managers and supervisors shall use the Supervisor Review Application to review and verify the status of Covered Persons within their respective departments or areas to ensure that access to institutional systems continues to be appropriate to each Covered Person's role or function.

3. Managers and supervisors shall immediately report to the HSTS Information Security Office any violations of this policy, and other compromises of access security, including compromises of sign-on/passwords or access codes. HSTS Information Security Office shall take corrective action as appropriate and shall notify the Compliance and Privacy Office of the violation and of any action taken. The Compliance and Privacy Office, in conjunction with the appropriate supervisor and Human Resources, shall investigate the violation.

4. If temporary access to institutional systems is necessary for a person not directly employed by the Medical Center, the University Physicians Group, School of Medicine or another entity (such as a contract vendor), a requesting manager or supervisor shall obtain from such person/s a confidentiality and security agreement incorporating the relevant requirements of this policy; if the person requiring access to institutional systems is a contract vendor, or employed by a contract vendor, a requesting manager or supervisor shall also confirm with Procurement that any required Business Associate Agreement has been executed.

5. This policy does not apply to a patient's access to his/her medical record via patient portal (e.g Epic, MyChart). Covered Persons with approved access may retrieve and view their own EMR, consistent with Medical Center Policy No. 0021 "Confidentiality of Patient Information".

6. Contact information for the HSTS Information Security Office may be found at https://www.healthsystem.virginia.edu/technology/departments/health-system-technology/teams/information-security.

SIGNATURE:

R. Edward Howell, CEO, UVA Medical Center

DATE: 6/20/13

Medical Center Policy No. 0163 (R)
Approved March 1995
Revised March 1996, April 1999, November, 2002, November 2004, June 2007, September 2010,

(SUBJECT: Access to Electronic Medical Records and Institutional Computer Systems)

March 2012, September 2012, June 2013
Reviewed October 1998
Approved by Interim Chief Technology and Health Information Officer
Approved by Medical Center Administration
Related Medical Center Policies:

Medical Center Human Resources Policy No. 701 "Employee Standards of Performance and Conduct"
Medical Center Policy No. 0227 "Protection of Electronic Information and Information Systems"

Related University Policies:

a. Administrative Data Access Policy for University of Virginia
b. University Financial and Administrative Policies
c. Faculty Handbook