UNIVERSITY of VIRGINIA HEALTH SYSTEM

Vice President and Chief Executive Officer of the Medical Center

MEDICAL CENTER POLICY NO. 0227

A. SUBJECT: Protection of Electronic Information and Information Systems

B. EFFECTIVE DATE: July 1, 2011 (R)

C. POLICY:

The Medical Center will use reasonable and appropriate administrative, technical and physical safeguards for the protection of electronic information and information systems. Electronic information includes all data stored, accessed, displayed, and transmitted using the Health System and University computer networks. The Electronic Information Security Plan developed and maintained by Health System Computing Services (HSCS) communicates standards and procedures for implementing electronic information safeguards (information security controls). HSCS coordinates and collaborates with University Information Technology and Communications (ITC) to develop University-wide policies and implement same as applicable to the Medical Center. All Medical Center departments and other organizational units and all persons, regardless of employer ("users"), having access to the Medical Center's electronic information are required to comply with all relevant policies, standards and procedures, unless specifically exempted in writing by the Medical Center's Chief Information Officer.

Any electronic information security incident, such as a misuse by authorized users, unauthorized access, computer viruses, worms, hacking, information system failure, or theft, must be reported in accordance with the Computer Security Incident Report procedure.

D. PROCEDURE:

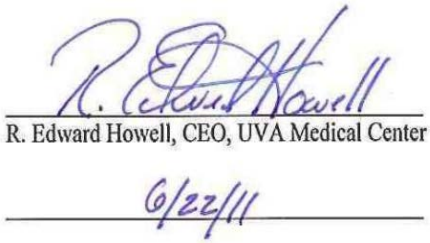
1. Users accessing Medical Center electronic information shall comply with all Medical Center and University requirements applicable to Medical Center information security, including but not limited to the standards, policies, and procedures at: https://www.hsts.virginia.edu/services/procedures, and the applicable guidelines at http://www.hsts.virginia.edu/services/it-security, unless specifically exempted in writing by the Medical Center's Chief Information Officer. Users accessing Medical Center electronic information must complete all education requirements applicable to Medical Center information security.

(SUBJECT: Protection of Electronic Information and Information Systems)

2. When a user becomes aware of an electronic information security incident he/she must immediately notify his/her manager and complete a Computer Security Incident Report. This report is made by accessing the following website: http://www.hsts.virginia.edu/procedures/incident-management .

   Electronic information security incidents include, but are not limited to, misuse by authorized users, unauthorized access, electronic identity theft such as theft of social security numbers, computer equipment theft, computer viruses, worms, hacking, and information system failures.

SIGNATURE:



R. Edward Howell, CEO, UVA Medical Center

6/22/11

DATE:

Medical Center Policy No. 0227 (R)
Approved December 1, 2003
Revised March 2007, June 2010, June 2011
Approved by (Interim) Chief Technology and Health Information Officer
Approved by Medical Center Administration

Related Policies:

Medical Center Policy No. 0021 - Confidentiality of Patient Information
Medical Center Policy No. 0163 - Access to Electronic Medical Records and Institutional Computer Systems
Medical Center Policy No. 0235 - Compliance Code of Conduct
University Policy - IRM-015 – Electronic Storage of Highly Sensitive Data