Violations of Confidentiality
(formerly "HIPAA Violations Sanctions")

Date: December 21, 2012 **Number:** 1.431 **Status:** Final

Contact Office:
Senior Associate Dean for Clinical Operations
PO Box 800793
Charlottesville, VA 22908
Phone: 434-243-7088
Fax: 434-982-0874

Oversight Executive:
Senior Associate Dean for Clinical Operations
PO Box 800793
Charlottesville, VA 22908
Phone: 434-243-7088
Fax: 434-982-0874

Applies to:
Paid and unpaid employees of the School of Medicine, School of Medicine volunteers, post-doctoral fellows, students enrolled in the School of Medicine's MD and PhD programs, and vendors that are doing business with the School of Medicine and that have access to protected health information.

Reason for Policy:
This policy outlines sanctions for violation(s) of confidentiality of Protected Health Information (PHI).

Policy Statement:
Personnel shall access and use only the Protected Health Information (PHI) that they have a need to know as part of their authorized role-related duties. Federal and institutional guidelines and policies describe measures to safeguard protected health information (PHI). Unauthorized individuals who access, use, and/or disclose PHI, attempt to access PHI, and/or assist others to access PHI when it is not authorized, will be sanctioned appropriately. As outlined in the procedures, a sanction may take the form of verbal counseling, written reprimand, or further disciplinary action, including mandatory leave without pay and/or termination.

Medical Center Policy No. 0021 (Confidentiality of Patient Information) outlines the requirements for confidentiality of patient information. SOM employees shall comply with all provisions of MC Policy No. 0021.

Definition of Terms:

Access – to obtain, open, retrieve, or otherwise handle a patient's Protected Health Information, regardless of its format ("Access").

A *Single Access* is Accessing a single patient's record within a single twenty-four hour period.

A *Multiple Access* is:

- Accessing the records of two or more patients, regardless of the time frame within which the Access occurs; or
- Accessing the same patient's record on more than one occasion within two or more twenty-four hour periods (as measured from the time of the first access).

Authorized Access or Disclosure – Access to or disclosure of Protected Health Information that is necessary to support treatment, payment or business operations, when appropriately authorized by the patient, or as otherwise permitted by law and by SOM and Medical Center policy.

Disclosure or Disclose – the revealing of Protected Health Information, regardless of the format by which the information is made known ("Disclosure" or "Disclose"). With respect to PHI, Disclosure includes revealing the name of a patient, or any other information which would reasonably inform another person of a patient's identity, such as familial status, occupation and job title, address, names of acquaintances, etc. (See Medical Center Policy No. 0021 "Confidentiality of Patient Information")

EMR – electronic medical record used to document clinical care. This excludes MyChart.

HIPAA – Health Insurance Portability and Accountability Act of 1996. It contains provisions for protecting the privacy of patient Protected Health Information (PHI).

MyChart – an online, personalized, secure portal for accessing portions of one's own medical information. A patient may authorize another individual to access his or her MyChart by filing a written proxy in advance of the other individual accessing the patient's MyChart. My Chart is not the same as the EMR.

Protected Health Information (PHI) – All individually identifiable health and billing/payment information about a patient, regardless of its location or

form. Such information is 'individually identifiable' if it includes any one of the identifiers listed in Appendix A of Medical Center Policy 0021.

Violation – Access to, use or Disclosure of PHI for purposes other than those for which the individual is authorized. The following outlines some, but not all, types of violations ("Violations").

a. **Level 1:** An employee carelessly accesses PHI, that he/she has no need to know in order to carry out his/her job responsibilities, or carelessly Discloses information to which he/she has authorized Access. Examples of Level 1 Violations include, but are not limited to:

- Leaving PHI in a public area;
- Misdirecting faxes or emails that contain PHI;
- Discussing PHI that the employee is authorized to have Accessed in public areas where the discussion could be overheard;
- Leaving a computer or portable electronic device (e.g., smartphone, tablet, etc) accessible and unattended with PHI unsecured.

b. **Level 2: A**n employee intentionally accesses PHI without authorization. A Level 2 Violation shall be considered acts of serious misconduct that constitute a serious violation of this policy. Examples of Level 2 Violations include, but are not limited, to:

- Intentional, unauthorized Accessing of a friend's, relative's (including minor child's, adult child's, spouse's, or other family member's), co-worker's, public personality's, or any other individual's PHI (including searching for an address or phone number);
- Intentionally assisting another employee in gaining unauthorized access to PHI;

c. **Level 3:** An employee intentionally Accesses and Discloses PHI without authorization A Level 3 Violation shall be considered misconduct of such a severe nature that a first occurrence normally warrants termination. This is an extremely serious violation of this policy. Examples of Level 3 Violations include, but are not limited to:

- Unauthorized intentional Disclosure of a friend's, relative's (including minor child's, adult child's, spouse's, or other family member's), co-worker's, public personality's, or any other individual's PHI;
- Unauthorized intentional delivery of any PHI to any third party.

Procedures:

Each employee must report all alleged, apparent, or potential Violations within no more than twenty-four hours to both his/her supervisor/designee and the Corporate Compliance and Privacy Officer for investigation and follow up. Any report of a Violation shall be investigated appropriately by the area supervisor/designee, the SOM Human Resources designee, and the Corporate Compliance and Privacy Officer.

Upon receiving report of a possible HIPAA violation, the Corporate Compliance and Privacy Officer will work with the appropriate senior associate deans and SOM Human Resources designee to conduct a confidential investigation of the alleged Violation. They are:

- Senior Associate Dean for Clinical Affairs – for events related to clinical faculty
- Senior Associate Dean for Education – for events related to medical or graduate students
- Senior Associate Dean and Chief Operating Officer – for events related to any other individuals to whom this policy applies

A reasonable effort will be made during the investigation to include interviews of any person who may have knowledge of the event.

The Senior Associate Deans are responsible for recommending the appropriate sanctions to the Vice President and Dean. Results of the investigation and decision will be documented in writing and records retained in the employee's official personnel file. Individuals may appeal the decision in accordance with existing policies and procedures. The Vice President and Dean, or designee, will review any sanction involving suspension, dismissal, or termination before it is implemented, and retains final authority concerning sanctions.

In the event of a possible Violation involving both School of Medicine and Medical Center and /or University of Virginia Physicians Group (UPG) personnel, the investigation must be coordinated and any corrective actions or sanctions must be consistent among the organizations. The appropriate School of Medicine Senior Associate Dean, the appropriate Medical Center Chief, and the appropriate UPG Director shall cooperate and collaborate with University, SOM, UPG, and Medical Center Human Resources and with the Corporate Compliance and Privacy Officer in reaching a determination of the matter.

The Corporate Compliance and Privacy Officer shall provide an annual report of all Violations to the Vice President and Dean of the School of

Medicine and the Vice President and Chief Executive Officer of the Medical Center.

The following will serve as guidelines for appropriate sanctions in circumstances where it has been determined that a Violation has occurred.

Virginia law requires the reporting of specific matters related to licensed or certified healthcare practitioners to the Virginia Department of Health Professions (DHP). For all individuals who are licensed or certified by any of Virginia's Health Regulatory Boards, all Level 2 and 3 Violations of HIPAA or Virginia law will be reported to DHP.

Paid and unpaid employees, post-doctoral fellows, volunteers

- A *Level 1* Violation shall result in verbal counseling; a written letter of counseling; and/or retraining. Multiple careless unintentional Level 1 Violations involving Disclosure and / or Multiple Access shall be subject to progressive disciplinary action up to and including termination.
- A *Level 2* Violation shall result in performance warning with a three-day leave without pay in most instances and required retraining for the first Level 2 Violation. Disciplinary action up to and including termination may be taken for multiple Level 2 Violations, and for those Level 2 Violations where access was obtained under false pretenses.
- *Level 3* Violations, in most cases, shall result in immediate termination of employment, non-paid or volunteer assignment.

Corrective action for Violations involving paid employees shall involve the appropriate dean and shall follow the process outlined in the Standards of Conduct for University and classified staff. When faculty are involved, the appropriate Senior Associate Dean shall be consulted, and the faculty shall have the rights outlined in relevant faculty policies and grievance procedures. The services of a non-paid or volunteer may be terminated at will if recommended.

Students enrolled in the School of Medicine's MD or PhD programs, and students enrolled in dual degree programs (MD/MBA, MD/MPH, MD/CR)

- A *Level 1* Violation shall result in verbal counseling; a written warning in the student's file; and/or retraining. . Careless unintentional Level 1 Violations involving Disclosure and / or Multiple Access shall be subject to progressive disciplinary action up to and including termination from the program of study.

- A *Level 2* Violation shall result a written reprimand in the student's file and retraining. The student will be suspended from the program of study for three days and/or terminated from the program of study.
- *Level 3* Violations, in most cases, shall result in immediate termination from the program of study.

Corrective action for Violations involving students shall involve the Senior Associate Dean for Education. For events involving medical students, the procedures outlined in the Academic Standards and Achievements Policy of the Student Handbook shall be followed. For events involving graduate students, the Associate Dean for Graduate and Medical Scientist Programs will consult with the Dean of the Graduate School of Arts and Sciences throughout the investigation, and the two will make a recommendation to the Vice President and Dean of the School of Medicine regarding the final outcome.

<u>Vendors</u>

- A *Level 1* Violation may result in a verbal warning; written correspondence regarding the Violation; and/or a request that vendor representatives be certified that they have retrained for HIPAA privacy.
- A *Level 2* Violation may result in written correspondence regarding the Violation; a request that vendor representatives certify that they have retrained in HIPAA privacy; a request that the company assign a new representative(s) to conduct its business with the institution; and/or suspension of activity with the business associate for a period of time to be determined.
- A *Level 3* Violation will result in written correspondence regarding the Violation; a request that the company assign a new representative(s) to conduct its business with the institution; suspension of activity with the vendor for a period of time to be determined; and/or termination of the relationship with the vendor.

Corrective action for Violations involving vendors shall involve the Senior Associate Dean and Chief Operating Officer and the Director of Procurement Services, and shall include review of the vendor's contract.

Related Documents:

UVa Medical Center Privacy Policies (including Confidentiality of Patient Information, Medical Center Policy 0021) are listed on this page:
https://www.healthsystem.virginia.edu/intranet/privacyoffice/Policies.cfm

Violations of Confidentiality, Medical Center Policy 707
http://www.healthsystem.virginia.edu/docs/manuals/policies/mc_hr/A70A3D38-110A-2E68-144F9953684D9285/A70A415E-110A-2E68-147F39AD7114F1FD/A70ACD51-110A-2E68-14198F7DF61229C2

SOM Required HIPAA Privacy Training
http://www.medicine.virginia.edu/administration/office-of-the-dean/administration/school-policies/Required-HIPAA-Privacy-Training-_Jan-2006_.pdf

Delegation of Dean's Authority
http://www.medicine.virginia.edu/administration/office-of-the-dean/administration/school-policies/Violations%20of%20Confidentiality%20DELEGATION%20-3-15-13.pdf/view

HIPAA
http://www.hhs.gov/ocr/privacy/index.html

UVa Code of Ethics
http://www.virginia.edu/statementofpurpose/uethics.html

Research Misconduct
https://policy.itc.virginia.edu/policy/policydisplay?id='RES-004'

Responsibility of the Principal Investigator in Human Subject Research (contained in "IRB-HSR Research Guidance")
http://www.virginia.edu/vpr/irb/hsr/for_researchers.html

Student Health Center Confidentiality
http://www.virginia.edu/studenthealth/NSConfidentiality.html

Ethics in Computer Usage
http://www.itc.virginia.edu/policy/ethics.html

University Administrative Data Access Policy
http://itc.virginia.edu/policy/admindataaccess.html

Responsibilities for Computing Devices Connected to the University of Virginia Network
http://www.itc.virginia.edu/policy/netdevices/

Policy on Disciplinary Suspension or Termination of Academic Faculty
http://www.virginia.edu/provost/docs_policies/disciplinary.html

Grievance Policy for Academic Faculty (tenured, tenure-track, and academic non-tenure-track faculty)
http://www.virginia.edu/facultysenate/gpolicy2002.html

Grievance Procedure for Administrative General Faculty
http://www.virginia.edu/provost/docs_policies/grievance.html

Grievance Procedure for Classified Staff
http://www.edr.state.va.us/grievance.htm

Grievance Procedure for Students
http://www.medicine.virginia.edu/education/medical-students/ome/advoc

Grievance Procedure for Residents (under "Policies & Manuals)
http://www.medicine.virginia.edu/education/graduate-md/GME/housestaff-page

UVA Policy: Authorization of Volunteers in the Workplace
https://policy.itc.virginia.edu/policy/policydisplay?id=HRM-001

SOM Policy: Volunteers in Research
http://www.healthsystem.virginia.edu/internet/about/sompolicies/Volunteers-in-Research--REV-12-04-06-.pdf

Next Scheduled Review: October 2015

Revision history: Implemented July 23, 2007; revised 7/1/10, 12/21/12

Approved:

Steven T. DeKosky, MD — December 21, 2012 Date