



Human Resources

MEDICAL CENTER HUMAN RESOURCES POLICY NO. 707

A. SUBJECT: Violations of Confidentiality

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

C. POLICY:

The University of Virginia Medical Center strictly maintains the privacy and confidentiality of certain data pertaining to patients, employees and business information (“Confidential Information”). All Medical Center employees are held to the same performance expectations concerning Confidential Information, and are subject to corrective measures for violating those expectations (“Violations of Confidentiality” or “Violations”).

Those corrective measures for Violations that are applicable to full-time, part-time and flex employees who have successfully completed their probationary periods are set forth in [Medical Center Human Resources Policy No.701 “Standards of Performance”](#) and the performance improvement counseling process described therein. Violations of Confidentiality involving Medical Center management, Unit-Based Pool, Medical Center Pool, temporary and contract employees are not subject to the progressive performance improvement counseling process but are subject to corrective measures referenced in other applicable policies, procedures, and contracts.

Violations of Confidentiality which also involve violations of other Medical Center policies and/or applicable performance standards may be subject to additional corrective measures beyond those described in this Policy.

D. DEFINITIONS:

1. **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*)

(SUBJECT: Violations of Confidentiality)

2. **Authorized Access or Disclosure** – Access to or Disclosure of Confidential Information that is necessary to support treatment, payment or business operations, or as is otherwise permitted by law and Medical Center policy.
3. **Confidential Information** – any information in the custody of the Medical Center regardless of its form (oral, paper, electronic) or storage media, that constitutes medical records or other Protected Health Information (PHI), or proprietary Medical Center financial or other business-related information, including human resources records, payroll records, and legal advice documents.
4. **Disclosure** – the revealing of Confidential 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”](#))
5. **EMR** – electronic medical record used to document clinical care. This excludes MyChart.
6. **HIPAA** – the Health Insurance Portability and Accountability Act, which contains provisions for protecting the privacy of a patient’s health information (PHI).
7. **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. MyChart is not the same as the EMR.
8. **Protected Health Information (PHI)** – Protected Health Information consists of all individually identifiable health and billing/payment information about a patient regardless of its location or form. ([Medical Center Policy No. 0021 “Confidentiality of Patient Information”](#))
9. **Violations of Confidentiality (“Violations”)** – Access to, or use or Disclosure of, Confidential Information for purposes other than those for which an individual is authorized.

E. PROCEDURE:

1. Each employee must report all actual or suspected Violations promptly (and in any event within twenty-four hours) to his/her manager/designee of the relevant area.
2. All reports of Violations shall be appropriately investigated by the relevant area manager/designee. In addition, managers shall report any Violation involving PHI to the Corporate Compliance and Privacy Officer for investigation. ([Medical Center Policy No. 0021 “Confidentiality of Patient Information”](#)). Managers shall report Violations that do not involve PHI to senior management as determined by an individual manager to be necessary and appropriate.
3. Prior to any formal Performance Improvement Counseling, a predetermination meeting with a staff employee alleged to have engaged in a Violation shall be conducted to ensure the employee

(SUBJECT: Violations of Confidentiality)

has had an opportunity to address any issue(s) ([Medical Center Human Resources Policy No 701 “Employee Standards of Performance”](#)). This meeting is held to review the facts and provide the employee an opportunity to respond to the issues or explain any mitigating circumstances.

Supervisors and managers must consult with the Medical Center’s Human Resources, Employee Relations Office on all alleged Violations.

4. Any employee(s) responsible for a Violation shall be subject to corrective action based on the level of the Violation.
5. To ensure consistency and uniformity, the School of Medicine has also adopted a similar policy regarding performance expectations and Violations involving PHI applicable to paid and unpaid employees of the School of Medicine, School of Medicine volunteers, students enrolled in the School of Medicine’s MD and PhD programs, and School of Medicine business associates.
6. Levels of Violations; Corrective Measures:

a. **Level 1: Careless Access or Disclosure of Confidential Information**

This occurs when an employee carelessly Accesses Confidential Information 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

Examples include, but are not limited to:

- Leaving Confidential Information in a public area;
- Misdirecting faxes or emails that contain Confidential Information;
- Discussing Confidential Information 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 Confidential Information unsecured.

Corrective Measures:

Corrective action for a Level 1 Violation shall, in most instances, follow the progressive counseling process as outlined in the Standards of Performance ([Medical Center Human Resources Policy No. 701 “Employee Standards of Performance”](#)) and shall result in an informal counseling with appropriate retraining mandated. Multiple careless unintentional Violations (Level 1) shall be subject to progressive disciplinary action up to and including termination.

b. **Level 2: Intentional Access to Confidential Information without Authorization**

This occurs when an employee intentionally Accesses Confidential Information without authorization.

Examples of Level 2 Violations

(SUBJECT: Violations of Confidentiality)

Examples include, but are not limited, to:

- Intentional, unauthorized Access to a friend's, relative's (including minor child, adult child, spouse, or any other family member), co-worker's, public personality's, or any other individual's PHI;
- Intentionally assisting another employee in gaining unauthorized Access to PHI;
- Intentional, unauthorized Access to Human Resource or payroll records.

Corrective Measures:

A **Level 2 Violation involving PHI** shall be considered serious misconduct and shall, in most instances, result in performance warning ([see Medical Center Human Resources Policy No. 701 "Employee Standards of Performance"](#)) with a three (3) day suspension without pay for the first Level 2 Violation involving PHI and disciplinary action up to and including termination for multiple Level 2 Violations, and for those Level 2 Violations where access was obtained under false pretenses. .

Level 2 Violations involving Confidential Information other than PHI are also considered serious instances of misconduct, with the appropriate disciplinary action determined upon consideration of such factors as the personal or economic harm such Violation may have caused to another individual, or the economic or other business-related harm such Violation may have caused to the Medical Center. Therefore, depending upon its impact, the Violation may result in performance warning ([see Medical Center Human Resources Policy No. 701 "Employee Standards of Performance"](#)) with a three day suspension without pay for the first Level 2 Violation and disciplinary action up to and including termination for multiple Level 2 Violations and for those Level 2 Violations where Access was obtained under false pretenses.

c. Level 3: Intentional Disclosure of Confidential Information

This occurs when an employee intentionally discloses Confidential Information without authorization.

Examples of Level 3 Violations:

Examples include, but are not limited to:

- Unauthorized intentional Disclosure of a friend's, relative's (including minor child, adult child, spouse, or any other family member), co-worker's, public personality's, or any other individual's PHI to any third party, including a parent or family member and including the posting of PHI to a social network, regardless of privacy setting
- Unauthorized intentional delivery of any Confidential Information to any third party.

Corrective Measures:


Disciplinary action for **Level 3 Violations involving PHI** in most cases shall result in immediate termination of employment.

(SUBJECT: Violations of Confidentiality)

Level 3 Violations involving Confidential Information other than PHI are extremely serious instances of misconduct, with the appropriate disciplinary action determined upon consideration of such factors as the personal or economic harm such Violation may have caused to another individual, or the economic or other business-related harm such Violation may have caused to the Medical Center. Therefore, depending upon its impact, the Violation may result in performance warning ([see Medical Center Human Resources Policy No. 701 "Employee Standards of Performance"](#)), with a three day suspension without pay, or termination.

7. Violations involving PHI and corrective actions shall be reported to the applicable licensing board or other agency as appropriate.
8. In the event of a Violation involving the Medical Center, School of Medicine and/or UPG personnel, any investigation must be coordinated and corrective actions or sanctions must be consistent based on the facts. The appropriate member of senior management on behalf of the Medical Center and the appropriate Senior Associate Dean on behalf of the School of Medicine, and/or the appropriate UPG director shall cooperate and collaborate with Medical Center Human Resources, University Human Resources, UPG Human Resources, and the Medical Center Corporate Compliance and Privacy Officer in reaching a determination of the matter.
9. The Graduate Medical Education (GME) Office has adopted a similar policy regarding Violations involving PHI that is applicable to all GME Trainees.
10. The Medical Center Corporate Compliance and Privacy Officer shall provide an annual report of all Violations involving PHI to the Vice President and Chief Executive Officer of the Medical Center and the Vice President and Dean of the School of Medicine.

SIGNATURE:



R. Edward Howell, CEO, UVA Medical Center

DATE:

12/21/12

Medical Center Human Resources Policy No. 707 (R)
Approved June 2007
Revised September 2009, June 2010, December 2012
Approved by Chief Human Resources Officer
Approved by Medical Center Administration

(SUBJECT: Violations of Confidentiality)

See related Medical Center Confidentiality policies (non-inclusive list):

- [Medical Center Policy No. 0021 “Confidentiality of Patient Information”](#)
- [Medical Center Policy No. 0084 “Health Information Request for Non-Patient Care Usage”](#)
- [Medical Center Policy No. 0193 “Electronic Mail \(E-mail\)”](#)
- [Medical Center Policy No. 0194 “Faxing of Patient Information”](#)
- [Medical Center Policy No. 0163 “Access to Electronic Medical Records and Institutional Computer Systems”](#)
- [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”](#)

Other policies:

- [School of Medicine Policy No. 1.431 HIPAA Violations Sanctions](#)
- [University of Virginia Policy IRM-015 Electronic Storage of Highly Sensitive Data](#)