Privacy and Information Security Sanction Policy

Effective Date: November 2018

Policy Statement

All workforce members, including faculty, staff, and students, are expected to comply with the organization's Privacy and Information Security policies and the HIPAA Rules. Workforce members shall be subject to sanctions up to and including termination for failure to comply with the established policies and procedures or the HIPAA Rules.

Violations of Privacy or Information Security policies and procedures or the HIPAA Rules will result in an appropriate sanction to be determined on a case by case basis, depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper use or disclosure of PHI, and other relevant considerations.

Reason(s) for the Policy

The purposes of this policy are (1) to provide a framework of appropriate and consistent sanctions for violations of Privacy and Information Security policies and procedures and the HIPAA Rules and in line with any related Human Resource disciplinary policies and (2) to inform workforce members of CUHC's sanction policy, which will be enforced against workforce members in violation of the organization's Privacy and Information Security policies or the HIPAA Rules.

Primary Guidance to Which This Policy Responds

45 C.F.R. §§ 164.308(a)(1)(ii)(C), 164.530(e)(1)

Responsible University Office & Officer

Office of HIPAA Compliance, Chief Privacy Officer
Human Resources, Chief Human Resources Officer
Office of Faculty Affairs, Vice Dean for Faculty Affairs
CUMC Information Security Office, Chief Information Security Officer

Schools:
CUMC Medical, Dental, Nursing and Public Health, Student Dean(s)

Revision History

Issued: December 2003
Revised: October 2007
February 2010
November 2011
November 2012
November 2015
November 2018

Who is governed by This Policy

All CUHC workforce members

Who Should Know This Policy

All CUHC workforce members

Policy Text

1. Investigation

   The Privacy or Security Officer will investigate reported violations of Privacy and Information Security policies and procedures or the HIPAA Rules with the assistance of the workforce member's department, Legal Affairs/General Counsel, and others as deemed necessary. Investigations may include interviews of complainant, patients or staff, review of work schedules, auditing electronic information systems, medical information reviews, and other related processes or documents.

   If it is confirmed that a violation has occurred, the findings of the investigation, with a recommendation in accordance with this policy, including potential mitigating factors, will be forwarded to the Ad-Hoc Privacy Sanctions Committee to make the final determination of appropriate sanction(s).

   The Ad-Hoc Privacy Sanctions Committee will include the Privacy Officer, Chief Human Resources Officer, Faculty Affairs or Student Dean and the department administrator as appropriate. Office of General Counsel will provide the committee with legal and regulatory guidance, including advice on the potential financial and legal exposure associated with any disciplinary decision.

2. Sanctions as a result of a violation of CUHC Information Security or Privacy policies or procedures or the HIPAA Rules shall be imposed consistently across the organization. Sanctions shall be appropriate to the severity of the infraction and may take into account aggravating and mitigating factors, including but not limited to the following**:**
   - unintentional vs. deliberate violation
   - good faith vs. harmful intent
   - workforce member promptly reported the breach or violation when detected/identified and cooperated with the investigation
   - number of individuals affected
   - potential risk to the individuals affected and Columbia
   - repeated vs. first such violation by the workforce member

3. Sanction Guidelines

   To assist in determining the significance and impact of a violation, four (4) categories of potential violations, with examples of violations and appropriate disciplinary actions for each category, are identified below. This is not an exhaustive list. Review the relevant Privacy and Information Security policy or procedure for additional information.

CATEGORY	EXAMPLE VIOLATIONS	EXAMPLE DISCIPLINARY ACTIONS
Category 1 **Unintentional violation caused by carelessness, lack of adequate training or human error**	Accidental or Inadvertent Violation • Fax, mail or email to the wrong patient • Leaving paper documents unsecured • Verbal discussions in inappropriate places	• Mandatory remedial education course • Verbal or written warning • Note: *A second occurrence of such a violation or a single occurrence that results in the misdirection of numerous patient records should be treated as a Category 2 violation*
Category 2 **Violations attributed to poor job performance or failure to understand/follow policies**	Failure to Comply with Privacy and Information Security policies and procedures: • Releasing PHI without proper patient authorization • Failure to log off of an IT application • Failure to safeguard portable devices • Sharing user ID and/or passwords • Transmitting PHI using an unsecured method • Improper disposal • Failure to report a privacy or security violation • Leaving detailed PHI on an answering machine • Discussing PHI in a public area inside or outside of CUHC without legitimate business reason • Failure to register an information system for certification • Research conducted on human subjects without IRB approval	• Written warning • Mandatory remedial education course • Note: *A second occurrence of such a violation or a single occurrence that results in the misdirection of or risk to numerous patient records should be treated as a Category 3 violation*
Category 3 **Intentional violation due to curiosity or failure to understand access/authorization**	Deliberate or purposeful violation without harmful intent: • Unauthorized access of PHI without harmful intent • Unauthorized access of CUHC records without a business need, without harmful intent • Sending PHI to the wrong address or patient	• Final written warning • Mandatory remedial education course • Suspension • Termination, depending on the circumstances

	• Posting PHI to a social media account without written authorization using the CUMC HIPAA Media Authorization form	
Category 4 **Intentional violations causing patient or organizational harm**	Willful unauthorized disclosure of and/or access to PHI with malicious or harmful intent: • Unauthorized disclosure of PHI for identity theft, fraud, or other intent to use or sell for personal or financial gain • Unauthorized access of PHI to use against the patient in a dispute, legal proceeding or to otherwise extort, embarrass or humiliate a patient	• Termination

In addition, these guidelines apply to all categories of sanctions:

- The mandatory remedial education course must be completed within 7 days of the issuance of sanction and the transgressor must score at least 90% on the examination.
- A subsequent violation after receiving a final written warning should result in termination.
- No penalty involving dismissal or other serious sanctions may become effective except in accordance with the provisions of the University's Code of Academic Freedom and Tenure
- The sanctions imposed may be one or more from the relevant category.
- In addition to any sanctions imposed, the workforce member may be reported to the appropriate licensing board, if required and as appropriate. Reports to law enforcement also may be warranted and appropriate depending on the nature of the violation.

4. Documentation of sanctions will be maintained by the Privacy Officer and reported to the relevant entity's Compliance or Risk Committee, as required. Documentation of sanctions may be maintained for a minimum of six years.

5. Workforce members are prohibited from retaliating against a workforce member who acts in good faith to report a practice they believe is unlawful, in accordance with the Columbia University Non-Retaliation Policy. In addition, no sanction may be applied against a workforce member on the basis that he/she:

   - Believes in good faith that CUHC has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by CUHC potentially endangers one or more patients, workers, or the public, and the disclosure of PHI is to:
     - A Health Oversight Agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of CUHC;

- An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professionals standards or misconduct by CUHC; or
- An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the employee with regard to potential privacy violations or other misconduct.

- Is the victim of a criminal act and discloses PHI to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the criminal act and the PHI disclosed is limited to the following:
  - Name and address;
  - Date and place of birth;
  - Social Security number;
  - ABO blood type and Rh factor;
  - Type of injury;
  - Date and time of Treatment;
  - Date and time of death, if applicable; and
  - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Individuals who are suspected of retaliating against a workforce member will be subject to disciplinary action up to and including termination.

Note: When a student is the subject of a Privacy or Information Security investigation the designated Student Dean will be notified and participate in the investigation and, if required, determine the appropriate sanction for the student.

Responsibilities

Office of HIPAA Compliance, Office of Information Security, Human Resources, Faculty Affairs, and General Counsel

- Educate workforce members about policy
- Investigate policy violations
- Establish sanctions in consultations with HR, OGC, PU and CISO

Definitions

Columbia University Healthcare Component (CUHC) – Columbia University is a Hybrid Entity that has designated as its Healthcare Component (the **Columbia University Healthcare Component)** Columbia University Medical Center and the other colleges, schools, departments and offices of the University to the extent that they (i) provide treatment or health care services and engage in Covered Transactions electronically or (ii) receive Protected Health Information to provide a service to, or perform a function for or on behalf of, the Columbia University Healthcare Component.

HIPAA Rules means the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and related regulations.

Protected Health Information (PHI) is individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium (includes paper and oral communication). (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.

Workforce includes employees, faculty, staff, students, residents, volunteers, trainees, and other individuals at or affiliated with CUHC, whose work is under the direct control of CUHC, regardless of whether they are paid by CUHC.

Contacts

Karen Pagliaro-Meyer
Privacy Officer, Office of HIPAA Compliance
Tel: (212) 305-7315
Email: kpagliaro@columbia.edu

William L. Innes
Chief Human Resource Officer, Human Resources
Tel: (212) 305-9789
Email: William.innes@columbia.edu

Dionida Ryce
Assistant Vice President for Academic Appointments
Tel: (212) 305-9589
Email: dxr2101@cumc.columbia.edu

Anne L. Taylor, MD
Vice Dean for Academic Affairs
Tel: (212) 305-4993
Email: ataylor@columbia.edu