Effective Date: January 9, 2018

Policy Statement

The Columbia University Healthcare Component (CUHC) has established a process for individuals to file complaints if they feel their rights have been violated. An individual also has a right to file a complaint about the organization's privacy policies and procedures even without alleging the violation of a right.

CUHC will mitigate, to the extent possible, any harmful effect that is known or resulting from an unauthorized or improper access, use or disclosure of Protected Health Information (PHI).

Each privacy complaint shall be promptly investigated, and the individual shall be provided with a response regarding the resolution of the complaint if contact information is provided. In addition, the Privacy Officer shall assure that no workforce member or other person who files a complaint is retaliated against for filing such complaint.

Reason(s) for the Policy

The purpose of this policy is to outline CUHC's process for individuals to submit complaints regarding CUHC's privacy practices. The policy also describes how CUHC will address such complaints.

Primary Guidance to Which This Policy Responds

HIPAA Privacy Rule 45 CFR § 164.530(d)(1)

Responsible University Office & Officer

Office of HIPAA Compliance, Privacy Officer

Revision History

Issued: December 2003
Revised: September 2008
           September 2012
           November 2017
           January 2018

Who is governed by This Policy

All CUHC workforce members
Who Should Know This Policy

All CUHC workforce members

Exclusions & Special Situations

None

Policy Text

1. Patient Privacy Complaints
The patient is informed of the process to file a complaint in the Notice of Privacy Practices. Patients may be directed to the HIPAA Compliance website or provided a copy of the patient Privacy Rights Complaint Form.

   • Any faculty or staff member that becomes aware of a privacy complaint shall report this information to the Office of HIPAA Compliance promptly
   • The Privacy Officer or his/her designee will investigate a complaint and provide a written response to the individual within 30 days

2. Mitigating the effect of a loss or an unauthorized access, use or disclosure of PHI
The Privacy Officer or his/her designee shall carry out the following mitigation activities:

   • Review the circumstances surrounding unauthorized access, use or disclosure;
   • Notify others at CUHC as necessary
   • Determine the extent to which CUHC can mitigate the effects of any potential harm from the unauthorized access, use or disclosure
   • Make recommendations to management, review and revise policies and procedures if necessary, and/or take action as appropriate
   • Coordinate with the Columbia University Medical Center Chief Information Security Officer (CISO) and General Counsel to determine if additional actions, including regulatory reporting, are required

3. Loss or Theft of PHI

   • If PHI is stolen (e.g., a laptop containing PHI is stolen from an office), the employee who initially discovers the loss or is made aware of the theft is responsible for reporting the incident to Public Safety as soon as possible after learning of the loss.

       • Public Safety will notify the CISO or Privacy Officer, who shall coordinate incident response together
       • If police or other law enforcement authorities are notified of the theft, and they take a report, the report or a copy should be included with the written report submitted to the Privacy Officer to assist with HIPAA breach risk assessment requirements

   • If PHI is accidentally lost (e.g., records transported from one place to another are dropped and some pages blow away) the workforce member who lost or misplaced the documents is responsible for reporting the incident to the Privacy Officer as soon as possible after discovering the loss. The Privacy Officer shall coordinate mitigation efforts
4. **Safeguards to prevent unauthorized access, use or disclosure of PHI**

Each department is responsible for adhering to the [Sanitization and Disposal of Information Resources Policy](#) and/or establishing procedures for the disposal of PHI, including ePHI, to minimize the risk of inadvertent disclosure. Refer to the Columbia Administrative [Sanitization and Disposal of Information Resources Policy](#)

The Privacy Officer or his/her designee shall ensure safeguards are in place to prevent unauthorized access, use or disclosure of PHI. A few examples of such safeguards include:

- Continuously evaluate physical security, including locked doors and cabinets
- Assure that all workforce members have their ID card visible at all times and that authorized access into sensitive areas is monitored
- To mitigate sensitive or confidential information sent by fax in error, limit the information to the minimum necessary to meet its purpose and always utilize a departmental cover sheet as your first page
- Refrain from leaving detailed voicemail messages when calling patients; the message should only state that you are calling from Columbia University and provide a call back number for the patient to return your call

**Responsibilities**

The Privacy Officer is responsible for:

- Ensuring all complaints will be documented, along with the complaint disposition and response
- Ensuring all documents related to complaints will be maintained for six years
- Ensuring reasonable steps are taken to mitigate improper uses and disclosures of PHI, including theft and loss of PHI

**Definitions**

*Columbia University Healthcare Component* – 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.

*Covered Entity* – (i) a health plan, (ii) healthcare clearinghouse, or (iii) healthcare provider that transmits any health information in electronic form in connection with a Covered Transaction.

*Protected Health Information* – Information about a patient, including demographic information, that may identify a patient, which relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present or future
payment for the provision of health care to a patient.

**Contacts**

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

Chief Information Security Officer  
Tel: (212) 342-0268  
Email: security@cumc.columbia.edu

**Cross References to Related Policies**

**HIPAA Privacy Rule and Patient Rights**  

**Non-Retaliation Policy**  

**Web Address**

[https://www.hipaa.cumc.columbia.edu/](https://www.hipaa.cumc.columbia.edu/)

**Appendix**

**Privacy Rights Complaint Form**

[https://www.hipaa.cumc.columbia.edu/patient-hipaa-forms](https://www.hipaa.cumc.columbia.edu/patient-hipaa-forms)