Privacy Complaint Policy

Effective Date: November 2018

Policy Statement

Columbia University Healthcare Component (CUHC) has established a process for a patient to file a privacy complaint. The patient also has a right to file a complaint related to a privacy policy without alleging a violation of their rights.

Columbia University 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).

Reason(s) for the Policy

To outline the mechanism for individuals to report complaints regarding privacy practices; including the process to respond to a complaint.

Primary Guidance to Which This Policy Responds

HIPAA Privacy Rule § 164.530 Administrative requirements

Responsible University Office & Officer

Office of HIPAA Compliance, Chief Privacy Officer

Revision History

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

Who is governed by This Policy

All Columbia University Healthcare Component (CUHC) workforce members

Who Should Know This Policy

All CUHC workforce members

Exclusions & Special Situations

None

Policy Text
Each privacy complaint is promptly investigated and the individual is provided with a written response regarding the resolution of the complaint. In addition, the Privacy Officer shall assure that an individual that files a complaint is not retaliated against for filing such complaint.

1. **Patient Privacy Complaint**
   Patients should be directed to the HIPAA Compliance website or provided with the patient complaint form.
   
   - Any workforce member that becomes aware of a privacy complaint shall promptly report this information to the Office of HIPAA Compliance
   - The patient is informed of the process to file a complaint in the Notice of Privacy Practices
   - The Privacy Officer or their designee will investigate a complaint and provide a written response to the patient within 30 days

2. **Mitigating the effect of a loss or an unauthorized access, use or disclosure of PHI**
   The Privacy Officer or their designee will:
   
   - Review the circumstances or the alleged unauthorized access, use or disclosure;
   - Advise management staff as necessary
   - Determine the extent to which Columbia University can mitigate the effect or potential harm from an unauthorized access, use or disclosure
   - Make recommendations to management, review and revise policies if necessary, and/or recommend other corrective action as appropriate
   - Coordinate with the Information Security Officer (ISO) and General Counsel to determine if additional actions including regulatory reporting is required

3. **Loss or Theft of PHI**
   - If PHI is stolen (i.e., a laptop containing PHI stolen from an office etc.), the employee who initially discovers the loss or is made aware of the theft is responsible for reporting the incident to Public Safety immediately.
     
     - Public Safety will notify the Information Security and/or Privacy Officer.
     - If police or other law enforcement authorities are notified of the theft, a copy of the report will be included when submitted to the Privacy Officer to assist with the HIPAA breach risk assessment requirement.
   
     - If PHI is accidentally lost (i.e., records transported from one place to another are dropped and some pages blow away, etc.) the workforce member who lost or misplaced the documents is responsible for reporting the incident to the Privacy Officer immediately.
     
     - Each loss or theft will be promptly investigated and additional reporting, notification or corrective actions will be coordinated by the Privacy Officer, when indicated.

4. **Safeguards to prevent unauthorized access, use or disclosure of PHI**
   - Each department is responsible for establishing procedures for the disposal of PHI
including ePHI to minimize the risk of inadvertent disclosure. Refer to the Columbia Administrative Sanitation and Disposal of Information Resources Policy

- Continuously evaluate physical security and privacy including locked doors and cabinets where PHI is stored.
- Assure that all workforce members have their ID card visible at all times
- Continuously monitor authorized access control to sensitive areas including reviewing the list of those authorized to access secure areas.
- Limit the disclosure of information to meet the purpose and always utilize a departmental cover sheet when faxing PHI. In addition, workforce members should verify recipient fax number and document confirmation of receipt.
- Refrain from leaving detailed messages on patients’ answering machines, the message should include the minimum necessary; e.g. calling from Columbia University and a call back number for the patient to return the call.

5. **Organized Health Care Arrangement (OHCA)**

- Columbia participates in an OHCA with NewYork Presbyterian Hospital and Weill Cornell Medicine to permit the sharing of patient information for treatment, payment and healthcare operations at each of the organizations.
- The Privacy Officer will inform the appropriate Privacy Officer if Columbia receives a complaint that involves a hospital patient, employee or program.

**Responsibilities**

The Privacy Officer is responsible for:

- Investigating and responding to a complaint in a timely manner but no more than thirty (30) days
- Assuring all complaints are documented including the complaint disposition
- Assuring all documents related to complaints are maintained for a minimum of six years

**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.

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

*Hybrid Entity* – A single legal entity (i) that is a Covered Entity (ii) whose business activities include both Covered and non-Covered functions and (iii) that designates health care components within the Hybrid Entity as more particularly described in Section 164.103
**Protected Health Information (PHI)** is individually identifiable health information:

(1) Except as provided in section (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 communications).

(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.

**Contacts**

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

**Cross References to Related Policies**

[HIPAA Privacy Rule and Patient Rights Policy](https://www.hipaa.cumc.columbia.edu/)

**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)