Minimum Necessary Rule

Effective Date: May 2019

Policy Statement

Columbia University has established safeguards to limit unnecessary or inappropriate access to, and use or disclosure of, Protected Health Information (PHI). PHI will be used or disclosed when it is necessary to satisfy an approved purpose and in compliance with the Minimum Necessary requirements of the HIPAA Privacy Rule.

Reason(s) for the Policy

To comply with the Minimum Necessary standard for the Use or Disclosure of PHI, as required by the HIPAA Privacy Rule.

Primary Guidance to Which This Policy Responds

HIPAA Privacy Rule 45 CFR § 164.502(b), 164.514(d)

Responsible University Office & Officer

Office of HIPAA Compliance, Chief Privacy Officer

Revision History

Issued: December 2003
Revised: October 2007
December 2009
November 2018
May 2019

Who is governed by This Policy

All Columbia University Healthcare Component (CUHC) workforce members with access to Protected Health Information (PHI)

Who Should Know This Policy

All CUHC workforce members with access to Protected Health Information (PHI)

Exclusions & Special Situations

None

Policy Text

Columbia must make reasonable efforts to limit PHI used, accessed, disclosed or requested to the minimum necessary to accomplish the intended purpose.

1. **When Minimum Necessary Rule Applies**
   The Minimum Necessary Rule applies in three HIPAA circumstances:
   a. When using PHI internally within the Covered Entity
   b. When disclosing PHI to an external party in response to a request (except for treatment-related disclosures)
   c. When requesting PHI from another HIPAA Covered Entity

2. **When the Minimum Necessary Rule Does Not Apply**
   The Minimum Necessary Rule does not apply in the following situations:
   a. Disclosures to or requests by a health care provider for treatment purposes (Note: A provider's internal uses of PHI for treatment <u>are</u> subject to the Minimum Necessary Rule)
   b. Use or disclosure made to the individual to whom the PHI pertains, including in response to a request for access or an accounting
   c. Use or disclosure made pursuant to a valid authorization to release medical information
   d. Disclosures made to the Secretary of the Department of Health and Human Services for the purposes of compliance and enforcement of the HIPAA Privacy and Security Regulations
   e. Use or disclosure of PHI to the extent that such use or disclosure is required by law, complies with and is limited to the relevant requirements of such law
   f. Use or disclosure required for compliance with the HIPAA Privacy Regulation

3. **Access to or Use of PHI by Workforce Members**
   Columbia has identified the persons or groups who require access to PHI to carry out their duties and assigned role-based access to these individuals appropriate to their job functions. These persons or groups may include, but are not limited to, the following categories:
   a. *Physicians* who are employed by Columbia;
   b. *Nursing staff*
   c. Ancillary staff including medical assistants, laboratory staff and others supporting patient care activities
   d. *Administrative staff* including: health information management, business offices, quality, compliance, administration, information systems, human resources and other workforce as need to support the covered entity
   e. *Students*
   f. *Columbia Researchers with approval from the Office of Human Research Protections (OHRP) or (IRB)*

   The list above is not intended to be all-inclusive and may be modified as necessary.
   The Chief Medical Information Officer (CMIO) or their designee is responsible for identifying the persons or groups of workforce members who require access to PHI to carry out their duties and designating the types of PHI needed for each individual or group to carry out their work duties.

4. **This designation should:**
    a. List the job duties of each person or group of workforce members identified;
    b. Identify access granted using a role-based approach, delineating the category or categories of PHI to which each person or group of workforce members requires access and when such access is needed;
    c. Limit the access of each person or groups of workforce members to the Minimum Necessary PHI;
    d. Comply with Information Security policies including, but not limited to; Information Access Management, Workstation Use and Security, Technical Access Controls, Person or Entity Authentication as appropriate; and
    e. Be documented, periodically reviewed and permanently maintained.
    f. Review subsequent designations or changes in access to the Minimum Necessary PHI.
    g. Where the use of the entire medical record is reasonably necessary, the designation must state so explicitly and include a documented justification.

5. **Minimum Necessary designations must be documented**. This includes:
    a. The initial designation for a person or group of workforce members;
    b. Changes or updates to the designation for a person or group of workforce members resulting from:
        - changes in the role or responsibilities of the person or group
        - changes in employment, or
        - changes in technology used or methods in place for limiting access to PHI, including changes in computer systems, applications or the physical environment where PHI is stored; and
    c. Designations for new persons or groups of workforce members.

6. **Disclosures of and Requests for PHI**

    1. Columbia may not disclose an entire medical record unless:
        a. Authorized in writing by the patient or his/her personal representative; **or**
        b. The entire medical record is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the disclosure, which justification should be documented, if appropriate.

    2. The Director of Health Information Management or his/her designee is responsible for developing appropriate procedures to apply the Minimum Necessary standard for disclosures of and requests for PHI. These standards pertain to the following types of disclosures:
        a. Routine and recurring disclosures of and requests for PHI to limit the PHI; and
        b. Non-routine disclosures of and requests for PHI

Responsibilities

All workforce members are required to comply with this policy

- Department Administrators are responsible for identifying any conditions that would have an impact on a workforce member's ability to access and/or disclose the PHI they are authorized to access.

- Department Administrators are responsible for making reasonable efforts to limit the access to PHI necessary to carry out the workforce members job duties, functions and responsibilities.

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 Irving 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.

Protected health information 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
E-mail: HIPAA@cumc.columbia.edu

Health Information Management
Tel: (212) 342-3528
E-mail: ColumbiaDoctors-HIM@cumc.columbia.edu