HIPAA Breach Response and Reporting Policy

Effective Date: February 2020

Policy Statement

The Columbia University Healthcare Component (CUHC) is committed to compliance with all applicable federal and state laws and regulations, including the management of a potential compromise of Protected Health Information (PHI).

Reason(s) for the Policy

This policy establishes the process to investigate and provide required notification in the event of a breach of unsecured PHI.

Primary Guidance to Which This Policy Responds

The HIPAA Breach Notification Rule 45 CFR §§ 164.400-414
Stop Hacks and Improve Electronics Data Security Act “SHIELD ACT”

Responsible University Office & Officer

Privacy Office, Chief Privacy Officer

Revision History

Issued: June 2019
Revised: February 2020

Who is governed by This Policy

All CUHC workforce members

Who Should Know This Policy

All CUHC workforce members

Policy Text

This policy is intended to address the regulatory requirements related to a Breach of Unsecured PHI under HIPAA and the associated procedures. Columbia University’s Electronic Data Security Breach Reporting and Response policy addresses the University’s policy to respond to a potential security incident involving a breach or compromise of electronic systems.

1. Reporting and Investigation of a Potential Breach

   A. Reporting
i. Workforce members shall promptly and without delay report any suspected impermissible use or disclosure under the Privacy Rule that may compromise the privacy or security of Unsecured PHI to the Privacy Office.

ii. To report an actual or potential Breach, contact the Chief Privacy Officer at privacy@cumc.columbia.edu or call (212) 305-7315. The Chief Privacy Officer will obtain the preliminary information and determine the appropriate members of the CUIMC HIPAA Response Team to notify and participate in the investigation.

iii. The CUIMC HIPAA Response Team may include the following representatives:

- Chief Privacy Officer (CPO);
- Chief Information Security officer (CISO);
- Chief Information Officer (CIO);
- Office of General Counsel (OGC);
- Chief Human Resource Officer (CHRO);
- Vice Dean of Faculty Affairs
- Chief Communications Officer;
- Department Chair /Department Administrator;
- Office of Public Safety; and
- Dean of Students – as needed

B. Investigation

i. The CUIMC HIPAA Response Team is responsible for promptly assessing and investigating all potential Breaches of Unsecured PHI. Such investigations shall be conducted in accordance with the requirements of HIPAA and include:

- A collection of all relevant facts;
- A determination as to whether there was a violation of the Privacy Rule;
- The completion of a risk assessment to determine if there is a low probability that the PHI has been compromised, such that a Breach presumption can be refuted; and
- A determination as to whether a Breach exception applies.

ii. Following the investigation and remediation of a potential HIPAA Breach, the CUIMC HIPAA Response Team, which includes the CPO, CISO and OGC will review the incident and determine if an actual Breach of Unsecured PHI occurred.

2. Risk Assessment and Exceptions

A. Presumption

i. If there is an access, acquisition, use or disclosure of Unsecured PHI that is not permitted by the Privacy Rule and which compromises the security or privacy of the PHI, a Breach will be
presumed to have occurred unless CUHC can demonstrate that there is a low probability that
the PHI has been compromised or an exception to the definition of Breach applies.

B. Low Probability of Compromise

i. To determine the probability that PHI has been compromised, a risk assessment shall be
conducted and documented. Documentation of a HIPAA risk assessment is maintained by the
Office of HIPAA Compliance.

ii. A HIPAA risk assessment shall include an assessment of at least the following elements:

• The nature and extent of the PHI involved, including the types of identifiers and likelihood
of re-identification;
• The unauthorized person who used the PHI or to whom the disclosure was made;
• Whether the PHI was actually acquired or viewed; and
• The extent to which the risk to the PHI has been mitigated.

iii. If, after performing the HIPAA risk assessment, the CUIMC HIPAA Response Team determines
that there is a low probability that PHI involved in the incident has been compromised, the
incident is not a Breach and no notification is necessary under HIPAA.

iv. If, after performing the HIPAA risk assessment, the CUIMC HIPAA Response Team determines
that there is more than a low probability that the PHI involved has been compromised, then
the CUIMC HIPAA Response Team shall determine if a Breach exception applies, in accordance
with the exceptions described below.

At the conclusion of a HIPAA Breach risk assessment, a final report will be prepared and
include corrective actions, remediation and sanctions as appropriate.

C. Exceptions to Definition of Breach

i. The following are exceptions to the definition of Breach and are not considered a Breach of
Unsecured PHI:

• The unintentional acquisition, access, or use of PHI by a Workforce member or person
acting under the authority of CUHC or a Business Associate, if such acquisition, access, or
use was made in good faith, within the scope of the person’s authority, and does not result
in further use or disclosure in a manner not permitted by the Privacy Rule.
• The inadvertent disclosure of PHI by a person authorized to access PHI at CUHC or a
Business Associate to another person authorized to access PHI at CUHC or the same
Business Associate, or Organized Health Care Arrangement in which CUHC participates
• CUHC has a good faith belief that the unauthorized person to whom the impermissible
disclosure was made, would not reasonably have been able to retain the information.

ii. If no exception applies and a determination was made that there is more than a low
probability that the PHI involved has been compromised, the incident is a Breach and CUHC
must comply with the Breach notification requirements under the Privacy Rule and the procedures described below.

3. Breach Notification Requirements

If the CUIMC HIPAA Response Team confirms a HIPAA Breach of Unsecured PHI has occurred, the CUHC must provide notification, as described below, to:

- The Affected Individual(s)
- The Secretary for Health and Human Services, Office for Civil Rights
- To the media (in certain circumstances)

A. Individual Notice. If a Breach of Unsecured PHI is determined to have occurred, CUHC must notify each individual whose Unsecured PHI has been, or is reasonably believed by CUHC to have been, accessed, acquired, used, or disclosed as a result of such Breach (“Affected Individual”).

i. Method of Notification. Notification to Affected Individuals shall be provided by CUHC through one of the following methods:

- **Written Notice** by first-class mail to the Affected Individual at his/her last known address; or
  - If CUHC knows the Affected Individual is deceased and has the address of the next of kin or personal representative of the individual, written notice by first-class mail to either the next of kin or personal representative;

- **Electronic Mail** if the Affected Individual has agreed to receive such notices electronically and has not withdrawn his/her agreement to notice by electronic mail; or

- **Substitute Notice** if written notice is returned as undeliverable or CUHC has insufficient or out-of-date contact information. CUHC must provide substitute notice of the Breach in accordance with the following:
  - If CUHC has insufficient or out-of-date contact information for ten (10) or more Affected Individuals, CUHC shall:
    - Post a conspicuous notice on the home page of its website for a minimum of ninety (90) calendar days; or
    - Provide the notice for publication in major print or broadcast media where the Affected Individuals likely reside.
  - Regardless of the form of substitute notice, CUHC must include a toll-free phone number that remains active for at least ninety (90) days where Affected Individuals can learn if their information was involved in the Breach.
If CUHC has insufficient or out-of-date contact information for fewer than ten (10) Affected Individuals, CUHC may provide substitute notice through an alternative form of written, telephone, or other means of communication.

- **Under urgent circumstances**, CUHC may provide notice to Affected Individuals by telephone or other means, as appropriate. However, such notice shall be provided in addition to notification by either written or electronic form.

ii. **Content and Timing of Notification.** Notice must be provided without unreasonable delay and in no case later than sixty (60) days following the Discovery of a Breach. All notifications to Affected Individuals shall include, at a minimum:

- A brief description of the Breach;
- Date of the Breach and date of Discovery, if known;
- A description of the types of PHI that were involved in the Breach (e.g., full name, social security number, date of birth, diagnosis);
- The steps Affected Individuals should take to protect themselves from potential harm;
- A brief description of what CUHC is doing to investigate the Breach, mitigate the harm to Affected Individuals, and prevent further Breaches; and
- Contact information for Affected Individuals to ask questions or learn more information, which shall include a toll-free number, an e-mail address, website, or postal address.

B. **Media Notice**

i. If a Breach affects more than five-hundred (500) Affected Individuals who are residents of a particular State or jurisdiction, CUHC shall also be required to provide notice to prominent media outlets serving the State or jurisdiction.

ii. Such notice to the media shall be provided without unreasonable delay and in no case later than sixty (60) calendar days following the Discovery of a Breach.

iii. The notice to the media must include the same information required for the notice to the Affected Individuals, described above.

C. **Notice to the Secretary**

i. CUHC must notify the Secretary of HHS regarding a Breach of Unsecured PHI in accordance with the following requirements. CUHC will electronically submit a breach report form on the HHS website.
• If a Breach affects five-hundred (500) or more individuals, CUHC must notify the Secretary without unreasonable delay and in no case later than sixty (60) calendar days following the Discovery of the Breach. Notice to the Secretary shall be provided at the same time that CUHC provides notice to Affected Individuals.

• If a Breach affects fewer than five-hundred (500) individuals, CUHC shall include the Breach in an annual report to the Secretary. The annual report must be submitted to the Secretary no later than sixty (60) days after the end of the calendar year in which the Breach occurred.

D. Notice to New York Regulators

i. CUHC must notify the New York Attorney General, New York Department of State, and Division of State Police of the Breach if:

• New York residents are to be notified of a Breach; and/or
• CUHC is required to notify the Secretary of HHS of the Breach.

ii. The notice must describe the timing, content, and distribution of notices to individuals and include the approximate number of affected individuals and a copy of the template notice sent to affected individuals.

iii. Notice of the Breach may be provided to all three entities online via the Data Breach Reporting Form on the New York Attorney General website.

iv. Such notice shall be made within five (5) business days of notifying the Secretary of HHS, if applicable, and without delaying notice to affected New York residents.

E. Notice to Consumer Reporting Agencies

i. If more than five thousand (5,000) New York residents are to be notified of the Breach at one time, CUHC must also notify the consumer reporting agencies on the Attorney General’s list of the Breach.

ii. The notice must describe the timing, content and distribution of the notices to individuals and the approximate number of affected individuals. Such notice shall be made without delaying notice to affected New York residents.

4. Breaches by Business Associates

A. Business Associates of CUHC are required to notify CUHC of Breaches that they experience.

i. If a Business Associate reports a potential Breach to a Workforce member, the Workforce member shall promptly and without delay forward such notification to the Privacy Office.

ii. The CUIMC HIPAA Response Team shall determine if the potential Breach constitutes a Breach of Unsecured PHI that requires notification under HIPAA and this Policy.
iii. If notification is required, the CUIMC HIPAA Response Team/Privacy Officer shall provide any required notifications to Affected Individuals, the Secretary of HHS, and the media, all in accordance with the procedures outlined above.

5. Law Enforcement Delay

A. If a Law Enforcement Official informs CUHC that a notification, notice, or posting required under the Privacy Rule would impede a criminal investigation or cause damage to national security, the following procedures shall apply:

i. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

ii. If the statement is made orally, CUHC shall:

- Document the statement, including the identity of the official making the statement, and
- Delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. State Law Requirements

A. In addition to assessing and meeting any notification obligations under HIPAA, the CUIMC HIPAA Response Team shall determine if notice is required under applicable state data protection laws and regulations. Even where notification is not required under HIPAA, notice may be required under applicable state law. CUHC shall meet its notification obligations in the event of a breach under applicable state law.

7. Administrative Requirements

A. New hire and annual training informs Workforce members of the definition of a HIPAA Breach in addition to CUHC’s Breach notification responsibilities.

B. CUHC HIPAA Privacy and Information Security Sanction Policy will address Workforce Members who do not comply with this Policy, including the obligation to promptly report a potential HIPAA Beach to the Privacy Office.

C. All documentation including the HIPAA Breach Risk Assessment, notifications and Breach reports will be maintained by the Privacy Office for a minimum of six (6) years.

Definitions

Breach - the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

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 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.

**Discovery** – the first day that a Breach is known, or by exercising reasonable diligence would have been known by CUHC (which includes members of its Workforce or agents, other than the person committing the Breach).

**Protected Health Information (PHI)** - individually identifiable health information:
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).

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.

**Unsecured Protected Health Information** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under section 13402(h)(2) of Public Law 111-5.

**Workforce** - employees, volunteers, trainees and other persons whose conduct, in the performance of work for CUHC, is under the direct control of CUHC, whether or not they are paid by CUHC.

**Contacts**
To report a potential breach of PHI:
Privacy Office
Email: privacy@cumc.columbia.edu

To report a potential breach of other Sensitive Data at CUIMC:
CUIMC IT Information Security Office
Email: security@cumc.columbia.edu

Cross References to Related Policies
[Electronic Data Security Breach Reporting and Response Policy]