Columbia College Health Plan

HIPAA POLICIES AND PROCEDURES

EFFECTIVE DATE OF LAST UPDATE: AUGUST 2018

TABLE OF CONTENTS

Introduction

As directed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health and Human Services ("HHS") has issued health privacy regulations. The privacy rules protect the privacy of health information about individuals by restricting the ways in which most group health plans, doctors, hospitals, and other "Covered Entities" can use and disclose health information about individual plan participants or patients ("Participants"). This health information is referred to as "Protected Health Information" or "PHI." The purpose of these HIPAA Privacy Policies and Procedures (this "Privacy Policy") is to comply with the regulations issued by the HHS under HIPAA, the Health Information Technology for Economic and Clinical Health Act ("HITECH") as found in the American Recovery and Reinvestment Act of 2009 ("ARRA") and regulations issued thereunder (the "Privacy Rule"). Modifications to the Privacy Rule are expected from time to time, some of which may require amendment of this Privacy Policy. If any provision of this Privacy Policy is inconsistent with HIPAA or a more restrictive applicable state privacy law (to the extent not preempted), this Privacy Policy will be interpreted to comply with such law.

Columbia College sponsors certain group health plans (including medical, dental, and health savings account plans) (referred to herein as the "Health Plan(s)") for its employees, that are subject to the HIPAA Privacy Rules. Columbia College is referred to herein as the "College" or, the "Employer."

All PHI will be treated as confidential and subject to these policies. All representatives of the Health Plan, and all members of the Employer workforce, including any agents or independent contractors performing work for the Employer on behalf of the Health Plan, are expected to maintain the privacy and security of any PHI they receive in accordance with these policies.

The unauthorized disclosure of PHI by any employed member of the Health Plan or the Employer's workforce, as applicable, can subject the Health Plan or the Employer to civil and criminal fines, as well as contractual damages. As such, these policies should be circulated and understood by all members of the Employer's workforce that have access to PHI.

Definitions

"**Authorization**" means an Individual's specific written permission allowing the Health Plan or Business Associates to use and disclose PHI for purposes other than those described in *Use and Disclosures of PHI*.

"**Breach**" means the unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of such information.

"**Designated Record Set**" or "**DRS**" means a group of records maintained by or for a Covered Entity that is: (1) the medical records and billing records about participants maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the Covered Entity to make decisions about participants. The term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Health Plan. Designated Record Sets do <u>not</u> include the following: peer review information, quality assurance information, performance improvement information, case management information, reviews by experts, attorney-client privileged materials, documents created in anticipation of litigation, incident reports, compliance information and investigations, risk management materials, complaints, investigation of complaints, and their disposition; personnel records; and any records, documents, or information that were not used to make decisions about the individual.

"**HHS**" means the United States Department of Health and Human Services.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, and the implementation regulations thereunder.

"**HITECH Act**" means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) which modifies HIPAA by establishing new privacy and security obligations and limitations on those parties that exchange or access PHI (*i.e.*, covered entities and business associates).

Individual" means an individual who is covered by a Health Plan and to whom the PHI pertains, and includes a person who qualifies as a Personal Representative in accordance with 45 C.F.R. §164.502(g). Individual includes a decedent previously covered by a Health Plan.

"**Individually Identifiable Health Information**" means information created or received by the Health Plan that relates to the past, present, or future physical or mental health or condition of a Participant, the provision of health care to a Participant, or the past, present, or future payment for the provision of health care, and that identifies the Participant, or with respect to which there is a reasonable basis to believe the information can be used to identify the Participant.

"**NIST**" means the National Institute of Standards and Technology.

"**Participant**" means the Employer's covered employee under the Health Plan who is the subject of the PHI that the Health Plan receives by or on behalf of its Participant, and includes a person who qualifies as a Personal Representative in accordance with 45 C.F.R. §164.502(g).

"**Personal Representative**" means, as specifically defined by state law, a person who has the authority to act on behalf of a Participant in making decisions related to the Participant's health care and/or health claim adjudication processes.

"**Protected Health Information**" or "**PHI**" means Individually Identifiable Health Information maintained or transmitted in any form or medium.

"**Responsible Employee**" means an employee (including a contract, temporary, or leased employee) of Employer whose duties (i) require that the employee have access to PHI to perform administrative functions on behalf of a Health Plan, or (ii) make it likely that they will receive or have access to PHI on behalf of a Health Plan. Any other employee (other than a designated Responsible Employee) who creates, uses, discloses, or receives PHI on behalf of a Health Plan will be treated as a Responsible Employee under the Privacy Policy, even though their duties do not (or are not expected to) include creating, using, disclosing, or receiving PHI.

"**Secretary**" means the Secretary of HHS, or designee.

"**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"**Unsecured PHI**" 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 in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

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

Designation of HIPAA Privacy Official

Purpose:

To designate a Privacy Official with the assigned responsibilities of executing, and maintaining policies and procedures to ensure the Health Plan's and Employer's continuing compliance with the HIPAA Privacy Rule.

Policy:

The College's Vice President and General Counsel shall act as the Privacy Official. The Privacy Official shall have overall responsibility for developing, establishing and maintaining the HIPAA Privacy Policies and Procedures, as well as developing any future amendments or revisions to such policies.

Duties and Responsibilities of the Privacy Official:

- Oversee activities related to the development, implementation, maintenance of, and adherence to the policies set forth in these Policies and Procedures.
- Ensure that the Health Plan documents have been amended to allow Responsible Employees to perform functions on behalf of the Health Plans in accordance with this Privacy Policy.
- Provide HIPAA training and guidance to the Responsible Employees.
- Receive any complaints or inquiries about privacy matters, and respond to such complaints or inquiries.
- Document all complaints or inquiries received and ensure complaints are investigated.
- Regularly monitor changes to privacy laws and regulations to help ensure the Health Plan and the Employer continues to conform to applicable law and the standards of confidentiality and privacy.

Privacy Official Contact:

For all required HIPAA notification purposes as set forth below, the Privacy Official may be contacted at the following:

Columbia College
General Counsel Office
1001 Rogers Street
Columbia, MO 65216
573-875-7806 (phone)
generalcounsel@ccis.edu (email)

Right to Receive Notice of Privacy Practices

Purpose:

To ensure that the Health Plan is fulfilling its obligations related to providing Individuals with the Health Plan's notice of privacy practices which indicates the Health Plan's uses and disclosures of the Individual's PHI.

Policy:

The Health Plan shall provide each Individual with a "Notice of Privacy Practices" (the "Notice"), which details how PHI may be used or disclosed by the Health Plan and each Individual's rights related to such PHI.

Procedure:

1. The Health Plan will notify Individuals of the Health Plan's permissible uses and disclosures of PHI and of the Individuals' rights and the Health Plan's legal duties with respect to PHI. The terms of the Notice will also describe the use and disclosure of PHI by Business Associates on behalf of the Health Plans.

2. The Notice will be provided to each Individual at the time of enrollment. Each covered dependent of a Covered Individual will be deemed to have received a copy of the Notice if the Notice is provided to the Covered Individual.

3. The Notice must be revised whenever there is a change to the uses and disclosures, Individuals' rights, the Health Plans' duties, or other privacy practices stated in the Notice. Whenever there is a material change to the Notice, a revised Notice will be distributed to all current Individuals within sixty (60) days of the revision to the Notice.

4. At a minimum, once every three (3) years, the Health Plan will mail Individuals a copy of the Notice.

5. If an Individual agrees, delivery of the Notice may be electronic, provided that the agreement has not been withdrawn. If a Responsible Employee becomes aware that electronic delivery has failed, a paper copy must be provided to the Individual. All Individuals may obtain a paper copy of the current Notice by making a request to the Privacy Officer, even if such Individual previously agreed to receive an electronic notice.

6. The Privacy Officer must maintain a copy of each version of the Notice for a period of at least six (6) years from the date last in effect.

Notification of Breach of Unsecured PHI

Purpose:

To standardize the process to be followed in the event of any incident of the impermissible acquisition, access, use, or disclosure of PHI in compliance with applicable laws and regulations.

Policy:

If any Responsible Employee becomes aware of any actual or suspected unauthorized use or disclosure of Unsecured PHI, they must immediately notify the Privacy Official. The Privacy Official will immediately take steps to determine if there has been a Breach, and if there has been a Breach, to mitigate any harmful effects of the Breach and initiate notification procedures in accordance with this Policy.

There are 3 exceptions to the definition of Breach:

(i) Any unintentional acquisition, access or use of PHI by a Responsible Employee or individual acting under the authority of a covered entity or a business associate if such access or use was made in good faith and within the scope of authority and does not result in a further unauthorized use or disclosure;

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information is not further used or disclosed in an impermissible manner; and

(iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Any unauthorized use or disclosure of PHI that does not meet one of the "breach" exceptions is presumed to be a "Breach" unless the Plan can demonstrate (through a written risk assessment) that there is a "low probability that the PHI has been compromised." The 4 factors that must be considered in making this determination include: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. The Plan may consider other factors (as appropriate), but the risk assessment must be documented, thorough, completed in good faith and the conclusions reached must be reasonable.

Procedure:

1. Any Responsible Employee who becomes aware of any actual or suspected unauthorized acquisition, access, use, or disclosure of Unsecured PHI (i.e., unencrypted PHI) must immediately notify the Privacy Official.

2. The Privacy Official will immediately take steps to determine if there has been a Breach, and if there has been a Breach, to mitigate any harmful effects of the Breach and initiate the notification procedures in accordance with the following procedures:

a. Upon receipt of a report of a potential Breach, the Privacy Official shall immediately begin investigating the incident and perform a risk assessment to determine whether the impermissible acquisition, access, use, or disclosure of the Unsecured PHI constitutes a Breach because it compromises the privacy or security of the PHI. In investigating the incident, the Privacy Official may take the following steps:

i. Contact and interview the Responsible Employee who reported the incident; and

ii. Contact and interview any other person involved in the incident.

b. In assessing whether an incident constitutes a reportable Breach, the Privacy Official must consider the four factors listed above in the policy section.

3. Following the Privacy Official's risk assessment, if it is determined that an exception applies or that the impermissible acquisition, access, use, or disclosure does not constitute a Breach, such determination should be documented and no further action is required.

4. If it is determined that the impermissible acquisition, access, use, or disclosure of PHI does constitute a Breach, then the Privacy Official should notify each affected Individual in writing by first class mail at the last known address of the Individual, or if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

a. If the Individual is deceased and the Health Plan has the address of the next of kin or Personal Representative of the Individual, written notification by first class mail shall be made to the next of kin or the Personal Representative of the Individual.

b. If there is insufficient or out-of-date contact information to provide written notice, a substitute notice reasonably calculated to reach the Individual shall be provided. Substitute notice need not be provided if there is insufficient contact information for the next of kin or Personal Representative.

- If fewer than ten (10) Individuals require substitute notice, then substitute notice may be provided by an alternative form of written notice, telephone or other means.

- If ten (10) or more Individuals require substitute notice, then substitute notice shall be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the website of the Health Plan or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside. A toll-free telephone number should be provided that remains active for at least ninety (90) days where an Individual can learn whether such Individual's Unsecured PHI was included in the Breach.

c. Emergency Notice – If the Health Plan determines that urgent notice is necessary because of possible imminent misuse of Unsecured PHI, the Health Plan may provide information to Individuals by telephone or other means, as appropriate. However, written notification still must be provided to the Individual.

5. Following the discovery of a Breach of Unsecured PHI, the Health Plan shall also notify HHS in accordance with the following.

- Breaches Involving 500 or More Individuals – For Breaches of Unsecured PHI involving 500 or more Individuals, the Health Plan shall provide notice to HHS simultaneously with the notifications to Individuals through the HHS website.

- Breaches Involving Less than 500 Individuals – For Breaches of Unsecured PHI involving less than 500 Individuals, the Privacy Official shall maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide notice to HHS through the HHS website.

6. Following a Breach of Unsecured PHI involving more than 500 residents of a state or jurisdiction, the Health Plan shall notify the prominent media outlets serving the state or jurisdiction. The timing of the notification and content of the notification shall be the same as for notification to affected Individuals.

7. To the extent feasible, all notices of a Breach provided by the Health Plan should include:

- A brief description of what happened, including the date of the Breach, if known, and date of the discovery;

- A description of the types of Unsecured PHI that were involved in the Breach (such as name, Social Security Number, date of birth, home address, account number, diagnosis, or other information);

- The steps affected Individuals should take to protect themselves from harm as a result of the Breach;

- A brief description of what the Health Plan is doing to investigate the Breach, to mitigate losses and to protect against further Breaches; and

- Contact procedures for Individuals to ask questions or obtain additional information, including a toll-free number, e-mail address, web site or postal address.

8. All notifications required pursuant to this policy, except as otherwise indicated, must be made without unreasonable delay and in no event later than sixty (60) days after the Breach is discovered, unless sooner notification is required under applicable state law. A Breach shall be treated as discovered by the Health Plan as of the first day on which such Breach is known, or by exercising reasonable diligence would have been known to any Responsible Employee (other than the person committing the Breach).

9. If a law enforcement official states that notification would impede a criminal investigation or cause damage to national security, the Health Plan shall:

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

- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification no longer than 30 days from the date of the oral statement, unless a written statement is submitted during such 30 day period.

10. The Privacy Official must retain documentation of Breach investigations, risk assessments, and notifications provided under this policy. Such documentation must be maintained for a period of at least six (6) years from the date created.

Right to File a Complaint

Purpose:

To provide a process for individuals to complain about the Health Plan's privacy practices and compliance with HIPAA and for the Health Plan and its representatives to respond to those complaints.

Policy:

1. The Health Plan has a procedure by which individuals can submit written complaints regarding the Health Plan's privacy practices and how the Health Plan will respond to such complaints.

2. An Individual who believes the Health Plan has violated his or her privacy rights may file a complaint with the Health Plan or with the Secretary. To file a complaint with the Health Plan, the individual may send a written complaint to the Privacy Official. Neither the Health Plan nor the Employer may penalize or retaliate against any individual for filing a complaint.

3. The Health Plan shall review the allegations in any complaint; determine its validity; and require the Employer to impose any sanctions upon Responsible Employees found to have violated these Policies and Procedures.

4. Within thirty (30) days of receiving the complaint, the Privacy Official shall begin reviewing the allegations in the complaint; following that, the Privacy Official shall determine its validity, and impose any sanctions upon individuals found to have violated these Policies and Procedures.

Procedure:

1. When a Responsible Employee receives a written complaint about the Health Plan's use or disclosure of PHI, the must immediately forward it to the Privacy Official who will follow and document the standard process for handling these complaints; the Privacy Official will timely begin reviewing and investigating the allegations in the complaint; the Privacy Official will then determine the complaint's validity; and the Privacy Official will take any corrective action and/or impose any sanctions upon individuals found to have violated these Policies and Procedures.

2. Documentation of complaints and their disposition must be maintained for a period of six (6) years from the date of the complaint.

Risk Analysis and Risk Management

Purpose:

To establish, manage, and implement a risk analysis and risk management process for the Health Plan.

Policy:

The Employer will establish and maintain appropriate risk analysis and management processes, and review procedures to reduce its privacy and security risk.

Procedure:

Risk Analysis

1. The Health Plan will conduct periodic assessments of potential risks, threats, and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI ("ePHI") that the Health Plan is entrusted with.

2. The Security Official, or designee, shall be responsible for conducting periodic risk analyses. Such responsibility includes establishing a plan and procedures for the conduct of such analyses.

3. Risk analyses must be conducted periodically, but at least once each year.

4. The Security Official shall model the risk analysis process on that recommended by the NIST.

5. In conducting a risk analysis, the Security Official shall consider the following:

    a. How does PHI flow through the Health Plan?

    b. What are the less obvious sources and external sources of PHI?

    c. What are the human, natural, and environmental threats to information systems that contain PHI?

6. The results of risk analyses shall be considered by management when making decisions, in order to help reduce the Health Plan's overall risk and to comply with HIPAA and other applicable laws and regulations.

7. All risk analyses shall be documented.

Risk Management Process

1. The Health Plan's and the Employer's risk management process, as applicable, shall be under the direct control and supervision of the Security Official, and shall involve legal counsel and information technology personnel.

2. The risk management process shall incorporate business and information-technology "best practices," along with the recommendations of the NIST.

3. The risk management process shall identify, analyze, prioritize, and minimize identified risks and threats to information privacy, security, integrity, and availability. The nature and severity of various risks and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.

4. The results of the risk management process shall be considered by management when making decisions, in order to help reduce the overall risk and to comply with HIPAA and other applicable laws and regulations.

5. The results of the risk management process shall be documented.

Risk Management Implementation

1. The Security Official shall develop and implement a plan, procedures, and a timetable for the implementation of the risk management process in all its aspects.