Russell Sage College HIPAA Privacy Use and Disclosure Policy and Procedures

Introduction
HIPAA Privacy Policy and Procedure

Russell Sage College (the College) sponsors a group medical plan, flexible spending account plan, and an employee assistance program, which, for HIPAA purposes, are called “the Plan”. Employees or their dependents may be enrolled in one or more parts of the Plan. Employees of the Colleges’ workforce may have access to the individually identifiable health information of the Plan participants (1) on behalf of the Plan; or (2) on behalf of the College, for administrative functions of the Plan.

In this Policy and Procedure document PHI means information that is created or received by the Plan and 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 to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identity the participant. PHI includes information of persons living or deceased.

It is the Colleges’ policy to comply fully with HIPAA's requirements. To that end, all members of the Colleges’ workforce who have access to PHI must comply with this Privacy Policy, are fully trained in HIPAA’s requirements and will sign appropriate confidentiality agreements. For purposes of this Policy, the Colleges’ workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, work-study students, and other persons whose work performance is under the direct control of the Colleges, whether or not they are paid by the Colleges. The term "employee" includes all of these types of workers.

No third party rights (including but not limited to rights of the Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Colleges reserve the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall not be binding upon the Colleges. This Policy does not address requirements under other federal laws or under state laws.

I. The Plan’s Responsibilities as a Covered Entity

1. Privacy Official and Contact Person

The Director of Human Resources will be the Privacy Official for the Colleges and the Plan. The Privacy Official or a designated assistant will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Colleges’ use and disclosure procedures. The Privacy Official or a designated assistant will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

2. Workforce Training

It is the Colleges’ policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. The Privacy Official or a designated assistant is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the Plan.

3. Technical and Physical Safeguards and Firewalls

The Colleges will establish, on behalf of the Plan, appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and designating specific facsimile machines for the communication of PHI.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

4. Privacy Notice

The Privacy Official or a designated assistant is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights; and
- The Plan's legal duties with respect to the PHI.

The privacy notice will inform participants that the Colleges will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Colleges' complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- no later than April 14, 2004.
- on an ongoing basis, at the time of an individual's enrollment in the Plan, and
- within 60 days after a material change to the notice

The Plan will also provide notice of availability of the privacy notice at least once every three years.

5. Complaints

The Privacy Official or a designated assistant will be the Plan's contact person for receiving complaints.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

6. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with the Colleges' discipline policy, up to and including termination.

7. Mitigation of Inadvertent Disclosures of Protected Health Information

The Colleges shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a use or disclosure of protected health information, either by another employee of the Colleges or an outside consultant/contractor, that is not in compliance with this Policy, the employee must immediately contact the Privacy Official or a designated assistant so that the appropriate steps to mitigate the harm to the participant can be taken.

8. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

Plan Document

The plan document for the Plan includes provisions describing the permitted and required uses and disclosures of PHI by the Colleges for plan administrative purposes. Specifically, the plan document requires the Colleges to:

- not use or further disclose PHI other than as permitted by the plan document or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from agree to the same restrictions and conditions that apply to the Colleges;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan,
- report to the Privacy Official or a designated assistant any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to the Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures as required by law;
- make the Colleges' internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (DHHS) upon request; and
- if feasible, return or destroy all PHI received from the Plan that the Colleges still maintain in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plan document also requires the Colleges to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Colleges agree to those restrictions; and (2) provide adequate safeguards.

10. Documentation Requirements

The Plan's and the Colleges' privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The Plan and the Colleges shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an 'individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years.

II. Policies on Use and Disclosure of PHI

1. Use and Disclosure Defined

The College and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Colleges, or by a Business Associate (defined below) of the Plan.
- Disclosure. For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Colleges.

2. Workforce Must Comply With Colleges' Policy and Procedures

All members of the Colleges' workforce (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and with the Colleges' use and disclosure procedures, which are set forth in this document.

3. Access to PHI is Limited to Certain Employees

The following employees ("employees with access") have access to PHI:

- Vice President of Finance and Administration
- Chief Information Officer
- Budget Analyst; and

Employees of

- Human Resources Department
- Finance and Business Services
- MIS
- Purchasing Department

These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the more detailed use and disclosure procedures.

4. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

a. Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

   - eligibility and coverage determinations including coordination of benefits and adjudication (e.g., claim administration) or subrogation of health benefit claims;
   - risk adjusting based on enrollee status and demographic characteristics; and
   - billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

b. Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities; reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and
- business management and general administrative activities.

5. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Colleges' "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in Policy II-8 "Disclosures of PHI Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

6. Mandatory Disclosures of PHI: to Individual and Department of Health and Human Services (DHHS)

A participant's PHI must be disclosed as required by HIPAA in two situations:

- The disclosure is to the individual who is the subject of the information (see Policy III-1) "Access to Protected Information and Request for Amendment")
- The disclosure is made to DHHS for purposes of enforcing of HIPAA.

7. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Colleges' use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Colleges' Privacy Official or a designated assistant. Permitted are disclosures:

- about victims of abuse,
- neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes,
- for public health activities, for health oversight activities;
- about decedents;
- for cadaver organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety:
- for specialized government functions, and
- that relate to workers' compensation programs.

8. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

9. Complying With the "Minimum Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the minimum necessary to accomplish the purpose of the use or disclosure.

The minimum-necessary standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization,
- disclosures made to the DOL;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

a. Minimum Necessary When Disclosing PHI. The Colleges will not allow disclosures of PHI except for Payment and Health Care Operations, (see Permitted Uses and Disclosures: Payment and Health Care Operations, (Policy II-4)), which are not subject to the minimum necessary standard and those listed above in Complying With Colleges' Policy and Procedures (Policy II-9), which are not subject to the minimum necessary standard.

b. Minimum Necessary When Requesting PHI. If the Colleges make requests for disclosure of PHI from business associates for purposes of Payment or Health Care Operations, the Colleges will attempt to limit PHI to the minimum necessary amount required for validation that the PHI received is only PHI of the Colleges' employees or their covered dependents.

Any unanticipated requests for PHI must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

10. Disclosures of PHI to Business Associates

Employees with access may disclose PHI to the Plan's business associates and allow The Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees with access must contact the Privacy Official or a designated assistant and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a the Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

11. Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

- Any of the following numbers

        - Social Security
        - Medical record
        - account and health plan beneficiary numbers
        - Certificate, license
        - Vehicle ID or plate
        - URL or IP addresses
        - Device identifiers
        - Biometric identifiers
        - Full face or comparable images
- Names
- Geographic units
- Dates
    - Month/day relating to any individual including birth, treatment
- Ages over 89
- Phone, fax numbers
- E-mail addresses
- Any other unique identifiers

III. Policies on Individual Rights

1. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the Colleges that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan, or
- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

2. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, they may extend the period by 30 days, provided that they give the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official or a designated assistant may impose reasonable production and mailing costs for subsequent accountings.

3. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Colleges, the requests are reasonable.

However, the Colleges shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official or a designated assistant has responsibility for administering requests for confidential communications.

4. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. The Colleges are not required to honor such requests. The Privacy Official or a designated assistant is charged with responsibility for administering requests for restrictions.

IV. Use and Disclosure Procedures

1. Procedures for Use and Disclosure of PHI

Procedure

Uses and Disclosures for the Plan's Own Payment Activities or Health Care Operations. An employee may use and disclose a Plan participant's PHI to perform the Plan's own payment activities or health care operations.

- Disclosures must comply with the minimum necessary standard (Procedure IV-9). (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10),

Disclosures for Another Entity's Payment Activities. An employee may disclose a Plan participant's PHI to another covered entity or health care provider to perform the other entity's payment activities. Disclosures may be made under the following procedures:

- Disclosures must comply with the minimum necessary standard (Procedure IV-9). (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

Disclosures for Certain Health Care Operations of the Receiving Entity. An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are subject to the following:

- Disclosures must comply with the minimum necessary standard (Procedure IV-9). (Under that procedure, if the disclosure is not recurring, the disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in "Disclosures of PHI Pursuant to an Authorization" (Policy II-8) has been received, an employee may not use a participant's PHI for the payment or operations of the Colleges' "nonhealth" benefits (e.g., disability, workers' compensation, and life insurance). If an employee requires a participant's PHI for the payment or health care operations of non-Plan benefits, follow these steps:

- Obtain an Authorization Form. First, contact the Privacy Official or a designated assistant to determine whether an Authorization Form for this type of use or Disclosure Form is on file. If no form is on file, request an appropriate Authorization Form from the Privacy Official or a designated assistant. Employees shall not attempt to draft Authorization Forms. All authorizations for use or disclosure for non-Plan purposes must be on a form approved by the Privacy Official.
- Disclosures must comply with the minimum necessary standard (Procedure IV-9).
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

Questions? Any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official or a designated assistant.

2. Mandatory Disclosures of PHI: to Individuals and DHHS

Procedure

- Request From Individual. Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own PHI, the employee must follow the procedure for "Disclosures Pursuant to Individual Authorization" (Policy IV-4) and "Disclosures to Individuals Under Right to Access Own PHI" (Policy II-6).
    - Request From DHHS. Upon receiving a request from a DHHS official for disclosure of PHI, the employee must take the following steps:

        - Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
        - Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

3. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

Procedure

- Disclosures for Legal or Public Policy Purposes. An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described in the following section, "Legal and Public Policy Disclosures Covered", must contact the Privacy Official or a designated assistant. Disclosures may be made under the following procedures:

    - The disclosure must be approved by the Privacy Official.
    - Disclosures must comply with the "Minimum-Necessary Standard" (Policy II-9)
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

Legal and Public Policy Disclosures Covered

a. Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

- The individual agrees with the disclosure; or
- The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

b. For Judicial and Administrative Proceedings, in response to:

- An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order): and
- A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

To a Law Enforcement Official for Law Enforcement Purposes, under the following conditions:

- Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
- Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
- Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.
- Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
- Information that constitutes evidence of criminal conduct that occurred on the Colleges' premises.

To Appropriate Public Health Authorities for Public Health Activities, as authorized by law.

To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

To a Coroner or Medical Examiner about Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

For Cadaver Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

For Specialized Government Functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.

For Workers' Compensation Programs, only to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

4. Disclosures of PHI Pursuant to an Authorization

Procedure

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required under these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
Verify that the authorization form is valid. Valid authorization forms are those that:

- Are properly signed and dated by the individual or the individual's representative;
- Are not expired or revoked;
- Contain a description of the information to be used or disclosed;
- Contain the name of the entity or person authorized to use or disclose the PHI;
- Contain the name of the recipient of the PHI ;
- Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
- Contain a statement regarding the possibility for a subsequent re-disclosure of the information.
  All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

5. Disclosure of PHI to Business Associates

Definition of Business Associate

Business Associate is an entity or person who:

- performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration including claim review assistance; data analysis, underwriting including vendor selection processes, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management. accreditation, or financial services, where the performance of such services involves giving the business associate access to PHI.

Procedure

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a business associate must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees with access must contact the Privacy Official or a designated assistant and verify that a business associate contract is in place. The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the business associate contract.

- Disclosures must comply with the "Minimum-Necessary Standard" (Procedure IV-9).(Under that procedure, each recurring disclosure will be subject to a separate policy to address the minimum-necessary requirement, and each non-recurring disclosure must be approved by the Privacy Official.)
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

6. Requests for Disclosure of PHI from Spouse, Family Member or Friend

The Plan and Colleges will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend will be able to access PHI.

- If an employee receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child, or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
- Once the identity of a parent or personal representative is verified, then follow the procedure for "Individual's Request for Access" (Procedure V-1)
- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Mandatory Disclosures of PHI: to Individuals and DHHS" (Policy II-6)

.

7. Disclosures of De-Identified Information

De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers as outlined in HIPAA regulations.

Procedure

- Obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.
- The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

8. Verification of Identity of Those Requesting Protected Health Information

a. Verifying Identity and Authority of Requesting Party. Employees with access must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

b. Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:
   - Request a form of identification from the individual. Employees with access may rely on a valid driver's license, passport or other photo identification issued by a government agency.
   - Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity

of the individual requesting access to the PHI, contact the Privacy Official or a designated assistant.
- Make a copy of the identification provided by the individual and file it with the individual's designated record set.
- If the individual requests PHI over the telephone verify the Social Security Number of the individual.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

c. Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:
- Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent, unless the child is a student at The Sage Colleges, in which case FERPA privacy guidelines apply.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements" (Policy I-10).

d. Request Made by Personal Representative. When a personal representative requests access to an individual's PHI, the following steps should be followed:
- Require a copy of appropriate documentation such as a valid power of attorney. If there are any questions about the validity of this document, seek review by the Privacy Official or a designated assistant.
- Make a copy of the documentation provided and file it with the individual's designated record set.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

e. Request Made by Public Official. If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" (Policy II-6) or "Permissive Disclosures of PHI" (Policy II-7); the following steps should be followed to verify the official's identity and authority):
- If the request is made in person, request presentation of an agency identification badge, other official credentials or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
- If the request is in writing, verify that the request is on the appropriate government letterhead.
- If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal contact the Legal Department.
- Obtain approval for the disclosure from the Privacy Official or a designated assistant.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

9. Complying With the "Minimum-Necessary" Standard

a. Procedures for Disclosures of PHI

- PHI may be disclosed when Plan participants or their covered dependents ask employees for assistance with claim inquiries and/or appeals to the Plan. The types of information likely to be disclosed are bills, physician statements, or a carrier's explanation of benefits. The employees with access must inform employees or their covered dependents of the necessity of signing an Authorization Form before any discussion of PHI. The Authorization Form must describe how PHI will be used and to whom it will be disclosed and it will advise employees and their dependents of their rights regarding the disclosure of PHI.
- For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

b. Procedures for Requests of PHI

- The Colleges will not share PHI for any reason other than those listed in the following section entitled "Exceptions". All other health information which is disclosed will be de-identified
- For any unauthorized requests for PHI, contact the Privacy Official, who will determine the necessity of the request and ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Exceptions

The minimum necessary standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to an individual authorization;
- Disclosures made to DHHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

10. Documentation Requirements

Procedure

Documentation. Employees with access shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants.
- When a disclosure of PHI is made:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - a brief description of the PHI disclosed;
  - a brief statement of the purpose of the disclosure; and
  - any other documentation required under these Use and Disclosure Procedures.
- Individual authorizations.

11. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to the Plan of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this policy. As a result, if an individual becomes aware of a disclosure of PHI either by an employee of the Colleges or an outside consultant/contractor that is not in compliance with the policies and

procedures set forth in this manual, the individual should immediately contact the Privacy Official. The Privacy Official will take appropriate steps to mitigate any potential harm to the individual.

V. Procedures for Complying With Individual Rights

1. Individual's Request for Access

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the Colleges that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Procedure

Request From Individual, Parent of a Minor Child, or Personal Representative. Upon receiving a request from an individual, parent of a minor child, or an individual's representative for disclosure of an individual's PHI, the employee with access must take the following steps.

- Require a written request
- Follow the procedures for verifying the identity of the individual, parent of a minor child or personal representative set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
- Review the disclosure request to determine whether the PHI requested is held in the individual's designated record set. See the Privacy Official or a designated assistant if it appears that the requested information is not held in the individual's designated record set. No request for access may be denied without approval from the Privacy Official.
- Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, certain requests by inmates, information compiled during research when the individual has agreed to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.
- Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30- or 60-day period of the reasons for the extension and the date by which the Colleges will respond.
    - A Denial Notice must contain (1) the basis for the denial, (2) a statement of the individual's right to request a review of the denial, if applicable, and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.
    - Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
    - Individuals have the right to receive a copy by mail, e-mail or in person at Human Resources. Individuals also have the right to inspect the information.

- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements" Policy I-10

2. Individual's Request for Amendment

Procedure

Request From Individual, Parent of Minor Child or Personal Representative. Upon receiving a request from an individual, parent of a minor child, or a personal representative for amendment of an individual's PHI held in a designated record set, the employee with access must take the following steps:

a. Follow the procedures for verifying the identity of the individual, parent of a minor child or personal representative set forth in “Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).

b. Review the disclosure request to determine whether the PHI at issue is held in the individual's designated record set. See the Privacy Official or a designated assistant if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Official.

c. Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (Policy III-1). See the Privacy Official or a designated assistant if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official.

d. Review the request for amendment to determine whether the amendment is appropriate - that is, determine whether the information in the designated record set is accurate and complete without the amendment.

e. Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Colleges will respond.

f. When an amendment is accepted make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form. Provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.

g. When an amendment request is denied, the following procedures apply:

- All notices of denial must be prepared or approved by the Privacy Official or a designated assistant. A Denial Notice Form must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement: (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
- If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the Denial Notice Form of the request; the individual's statement of disagreement, if any; and the Colleges’ rebuttal/response to such statement of disagreement, if any,

with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

3. Processing Requests for an Accounting of Disclosures of PHI

Procedure

Request From Individual, Parent of a Minor Child, or Personal Representative. Upon receiving a request from an individual, parent of a minor child or a personal representative for an accounting of disclosures, the employee with access must take the following steps:

- Follow the procedures for verifying the identity of the individual, parent of a minor child or personal representative set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
- Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Colleges will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by the Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the Plan is not required to account for any disclosures made prior to April 14, 2004.) The accounting does not have to include disclosures made:
  - to carry out treatment, payment and health care operations,
  - to the individual about his or her own PHI,
  - incident to an otherwise permitted use or disclosure,
  - pursuant to an individual authorization,
  - for specific national security or intelligence purposes,
  - to correctional institutions or law enforcement when the disclosure was permitted without an authorization, and,
  - as part of a limited data set.
- If any business associate of the Plan has the authority to disclose the individual's PHI, then the Privacy Official or a designated assistant will contact the business associate and obtain a written accounting of the business associate's disclosures.
- The accounting must include the following information for each reportable disclosure of the individual's PHI:
  - the date of disclosure;
  - the name (and if known, the address) of the entity or person to whom the information was disclosed;
  - a brief description of the PHI disclosed; and
  - a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
- If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official or a designated assistant for more guidance.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

4. Processing Requests for Confidential Communications

Request From Individual, Parent of a Minor Child, or Personal Representative. Upon receiving a request from an individual, parent of a minor child or an individual's representative to receive communications of PHI by alternative means or at alternative locations, the employee with access must take the following steps:

- Require a written request.
- Follow the procedures for verifying the identity of the individual, parent of a minor child or personal representative set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
- If a request will not be accommodated, the employee with access must contact the individual to explain why the request cannot be accommodated.
- All confidential communication requests that are approved must be signed by the Privacy Official.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10).

5. Processing Requests for Restrictions on Uses and Disclosures of PHI

Request From Individual, Parent of a Minor Child, or Personal Representative. Upon receiving a request from an individual, parent of a minor child or a personal representative to restrict access to an individual's PHI, the employee with access must take the following steps:

- Follow the procedures for verifying the identity of the individual, parent of a minor child or personal representative set forth in "Verification of Identity of Those Requesting Protected Health Information" (Procedure IV-8).
- The employee with access must submit a written request to the Privacy Official to restrict access.
- The Plan is not required to honor requests for restriction on the use and disclosure of PHI.
- If a request will not be accommodated, the employee with access must contact the individual to explain why the request cannot be accommodated.
- All requests for limitations on use or disclosure of PHI that are approved must be approved by the Privacy Official.
- All business associates that may have access to the individual's PHI must be notified of any agreed-to restrictions. The business associate must be notified in writing and a written confirmation of the associate's agreement must be filed.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation Requirements" (Policy I-10)

Revised July 2024