AP 4701 Protected Health Information

References:

ORS 192.553 – 192.581
Health Insurance Portability and Accountability Act

Purpose

This procedure establishes areas of responsibility and processes for protecting Protected Health Information (PHI) in compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations and with Oregon Revised Statutes (ORS) and standard best practices.

Designation of a HIPAA Privacy Officer and HIPAA Security Officer

The Director of Risk Management is designated the Rogue Community College (RCC) HIPAA Privacy Officer responsible for overseeing and enforcing HIPAA and applicable ORS compliance college-wide. The Director of Dental Programs is designated as the RCC HIPAA Security Officer assigned to the covered healthcare component. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer coordinate to ensure compliance with HIPAA and applicable ORS.

RCC maintains PHI in 3 different programs.

The RCC Massage Therapy Program and the RCC Dental Assistant Program are subject to the ORS 192.553 – 192.558.

The RCC Dental Hygiene Program is subject to ORS 192.553 – 192.558 in addition to HIPAA, both the Privacy and Security Rule, and is considered a covered healthcare component.

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information, called PHI, in any format by RCC. The Privacy Rule excludes from PHI employment records RCC maintains as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

HIPAA Security Rule

While the HIPAA Privacy Rule safeguards all PHI, the HIPAA Security Rule protects a subset of information covered by the HIPAA Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called electronic protected health information (EPHI). The Security Rule does not apply to PHI transmitted orally or in writing.

Oregon Revised Statute 192.553-192.558

Oregon's PHI rule protects the privacy and security of individuals' health information. The rule aligns with HIPAA but includes state-specific regulations that may impose additional requirements.

Covered Entity

Covered entities are defined in the HIPAA rules as:

- health plans,
- healthcare clearinghouses,
- and healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. The RCC Dental Hygiene Program is considered a healthcare provider.

RCC Covered Transactions

RCC engages in a number of transactions that meet the definition of a covered transaction and are necessary to carry out healthcare-related financial or administrative activities.

Hybrid Entity

The HIPAA Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity." (The activities that make a person or organization a covered entity are its "covered functions.") To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "healthcare components." After making this designation, most of the requirements of the HIPAA Privacy Rule will apply only to the covered healthcare components. A covered entity that does not make this designation is subject in its entirety to the HIPAA Privacy Rule.

RCC is designated as a Hybrid Entity under HIPAA. As such, only RCC-covered healthcare components are required to safeguard PHI in compliance with HIPAA regulations. However, other programs are still subject to ORS.

Protected Health Information

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associates in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present, or future physical or mental health or condition,

- the provision of healthcare to the individual or
- the past, present, or future payment for the provision of healthcare to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Responsibilities and Requirements

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, establish and maintain written responsibilities and processes for handling PHI following HIPAA regulations and ORS as applicable. The RCC HIPAA Privacy Officer will ensure that the responsibilities and processes cover data access, disclosure, transmission, storage, and disposal. The RCC HIPAA Privacy Officer will review and update processes and responsibilities to reflect technological, legislation, and organizational structure changes. The RCC HIPAA Privacy Officer will regularly review and update this administrative procedure to ensure it remains current and effective. The RCC HIPAA Privacy Officer will incorporate lessons learned from incidents and audits into ongoing compliance efforts. The RCC HIPAA Privacy Officer will conduct regular audits, at least annually, to assess compliance with HIPAA responsibilities and processes.

Response to Regulatory Inquiries

The RCC HIPAA Privacy Officer will be the point of contact and will coordinate the response to inquiries from regulatory agencies, such as the Office for Civil Rights (OCR) under the U.S. Department of Health and Human Services (HHS) and the Oregon Health Authority (OHA).

Complaints and Enforcement

If an individual believes their rights under HIPAA or ORS have been violated, they may file a complaint with the RCC HIPAA Privacy Officer, the Secretary of the US Department of HHS (HIPAA only), or the OHA (ORS only).

The complaint must be made in writing, must specify the entity that is the subject of the complaints, and must describe the acts or omissions believed to be in violation of the individual's privacy rights. The complaint must be filed within 180 days of when the individual or the individual's personal representative knew or should have known the act occurred (HIPAA Complaints only).

Anyone who knows or has reason to believe that another person has violated the requirements of HIPAA or applicable ORS as they relate to RCC shall report the matter promptly to the RCC HIPAA Privacy Officer. All alleged violations or reports of violations

of HIPAA or ORS will be investigated, and where appropriate, steps will be taken to remedy the situation.

Employee Training and Awareness

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, develop and implement a comprehensive training program for all employees and students in each of the programs covered by HIPAA or ORS before they are exposed to PHI, including a mandatory annual refresher course. The RCC HIPAA Privacy Officer will provide annual training for college leadership to ensure a top-down commitment to compliance. The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, maintain records of employee and student training for six years from the training date.

Documentation and Recordkeeping

In coordination with the RCC HIPAA Security Officer, the RCC HIPAA Privacy Officer will maintain detailed records of HIPAA and ORS compliance efforts, including policies, procedures, risk assessments, and training records for six years.

Risk Assessment, Analysis, and Management

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer, in coordination with RCC Information Technology (IT), will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the RCC-covered healthcare component. In coordination with IT, the RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will develop and implement security measures to reduce risk and vulnerabilities to a reasonable level. The RCC HIPAA Privacy Officer will review and update risk assessments to adapt to changes in the college environment.

The RCC HIPAA Privacy Officer will take reasonable steps to identify and prioritize the risks to the confidentiality, integrity, and availability of EPHI. As approved by the RCC HIPAA Privacy Officer, a documented risk analysis process shall be used to identify, define, and prioritize potential risks and vulnerabilities to EPHI. The risk analysis shall include, where appropriate, the judgments used, such as assumptions, defaults, and uncertainties, and explicitly state and document them.

Each RCC-covered healthcare component shall update the risk analysis annually. In addition to the risk analysis updates that RCC completes, the risk analysis shall be updated when environmental or operational changes arise that impact the confidentiality, integrity, or availability of EPHI.

The documented risk analysis results shall be reviewed by the RCC HIPAA Privacy Officer, the RCC HIPAA Security Officer, and RCC Senior Leadership.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer, in coordination with IT to protect the confidentiality, integrity, and availability of EPHI, will implement security measures designed to reduce the risks to EPHI to a reasonable and appropriate level. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer, in coordination with IT, will implement a Risk Management process that will be conducted annually and will be based on a documented process that is used as a basis for the selection and implementation of the security measures.

The RCC HIPAA Privacy Officers' and the RCC HIPAA Security Officers' strategies for managing risk shall be proportionate with the risks to and sensitivity of EPHI. The RCC HIPAA Privacy Officers' and the RCC HIPAA Security Officers' security measures shall reasonably protect the confidentiality, integrity, and availability of EPHI, and the risk will be managed continuously.

The results of the risk management process shall be documented in writing, reviewed by RCC's HIPAA Privacy Officer, the RCC's HIPAA Security Officer, and RCC Senior Leadership, and maintained by RCC.

Periodic and Compliance Audits and Monitoring

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, monitor system logs and reports for unusual or unauthorized activities. The RCC HIPAA Privacy Officer will take corrective actions based on audit findings.

The RCC HIPAA Privacy Officer will conduct internal audits to assess the college's overall HIPAA compliance at least every 90 days or sooner if necessary. The RCC HIPAA Privacy Officer will independently consider engaging external auditors to assess HIPAA compliance if necessary.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer, in coordination with RCC IT, will take reasonable and appropriate steps to ensure that EPHI Systems have the appropriate hardware, software, or procedural auditing mechanisms installed on them to enable the review of information system activity. The RCC HIPAA Privacy Officers risk analysis shall determine the level and type of auditing mechanisms that will be implemented on EPHI Systems.

For each EPHI System, the RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall maintain and follow a specific procedure for conducting information systems activity review, including review of information systems activity and review of auditable events. These procedures shall identify the information systems activity to be reviewed and the auditing mechanism to be used to capture the information systems activity. The audit results shall be retained for six years.

Privacy by Design

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will integrate privacy considerations into designing and developing new systems, processes, and technologies involving EPHI. The RCC HIPAA Privacy Officer will conduct privacy impact assessments during the planning phase of new initiatives.

Privacy Impact Assessments (PIA)

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will conduct privacy impact assessments for new projects, systems, or processes involving EPHI. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will evaluate the potential impact on privacy and implement necessary safeguards.

Data Minimization

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will apply the principle of data minimization, collecting and storing only the minimum necessary PHI for the intended purpose. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will regularly review data storage practices to identify and eliminate unnecessary data.

Data Safeguards

RCC must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing PHI before discarding them, securing medical records with lock and key or passcode, and limiting access to keys or passcodes.

Access Controls and Physical Security

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will implement access controls to restrict access to EPHI based on the principle of least privilege.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will regularly review and update user access permissions. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will monitor and audit user access to EPHI systems. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will implement physical security measures to safeguard areas where EPHI is stored. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will control physical access to servers, data centers, and other locations where EPHI is processed or stored.

Data Classification

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will classify data based on sensitivity and apply appropriate security controls accordingly. The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will communicate data classification policies to employees to ensure consistent handling of PHI.

Automatic Logoff

Electronic sessions will be terminated when feasible, and employees and students will be logged out of EPHI Systems after a number of minutes to be determined by the RCC HIPAA Privacy Officer, requiring the user to be identified and authenticated again to regain access and continue the session. The log-out time is set to 5 minutes or less.

The RCC HIPAA Privacy Officer will determine when it is not reasonable or appropriate to implement electronic automatic logoff mechanisms on certain EPHI Systems and approve equivalent alternative mechanisms (e.g., screen/session locking, screensaver implemented after a period of time).

RCC employees and students will be instructed to terminate electronic sessions on EPHI Systems when such sessions are completed and to log off from or lock their workstations or other EPHI Systems when their work or classes are completed or when they expect to be away from their workstations or other EPHI System for an extended period of time (e.g., for lunch, meetings, breaks).

Employee and Student Exit Procedures

The RCC HIPAA Privacy Officer will work with the RCC HIPAA Security Officer to develop and implement procedures for managing access to PHI when employees and students leave the college. The RCC HIPAA Privacy Officer will work with the RCC HIPAA Security Officer to promptly revoke access rights and collect any college property, including electronic devices containing EPHI, from departing employees and students.

Medical Device Security

In coordination with IT, the RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will implement security measures for medical devices storing or transmitting PHI and will regularly assess and update the security of medical devices to address vulnerabilities.

Mobile Device Management

In coordination with IT, the RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will establish policies and procedures for securing mobile devices that may access or store PHI and implement mobile device management solutions to enforce security settings and remotely wipe devices in case of loss or theft.

Secure Data Disposal

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer, in coordination with IT, will establish procedures for the secure disposal of electronic and physical media containing PHI.

Documentation Retention and Disposal

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer will implement procedures for the secure retention and disposal of PHI in accordance with HIPAA regulations and applicable ORS. The RCC HIPAA Privacy Officer will ensure that electronic and physical records are securely stored, archived, and, when appropriate, permanently deleted. RCC must maintain its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented for six years from the date of creation or last effective date, whichever is later.

For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed is acceptable as a disposal method.

RCC may, but is not required to, hire a business associate to appropriately dispose of PHI on its behalf. In doing so, RCC must enter into a contract or other agreement with the business associate that requires that business associate to appropriately safeguard the PHI through disposal.

Privacy Practices Notice

Each RCC-covered healthcare component, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe how the RCC-covered entity may use and disclose PHI. The notice must state the RCC-covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and the RCC-covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the RCC-covered entity. RCC-covered entities must act in accordance with their notices. The Privacy Rule also contains specific distribution requirements for direct treatment providers, all other healthcare providers, and health plan. The privacy practices notice is maintained by the RCC HIPAA Privacy Officer.

Notice Distribution

An RCC-covered healthcare provider with a direct treatment relationship with individuals must have delivered a privacy practices notice to patients as follows:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery).
- By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice.
- In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.
- RCC-covered entities, whether direct or indirect treatment providers, must supply notice to anyone on request. An RCC-covered entity must also make its notice electronically available on any website it maintains for customer service or benefits information.

Acknowledgment of Notice Receipt.

An RCC-covered healthcare provider with a direct treatment relationship with individuals must make a good faith effort to obtain a written acknowledgment from patients of receipt of the privacy practices notice. RCC must document the reason for failing to obtain the patient's written acknowledgment. RCC is relieved of the need to request acknowledgment in an emergency treatment situation.

Patient Consent Management

The RCC HIPAA Privacy Officer will establish processes for obtaining and managing patient consent for using and disclosing their PHI. The RCC HIPAA Privacy Officer will communicate the purposes for which consent is sought and allow patients to make informed decisions.

Patient Education

The RCC HIPAA Privacy Officer will develop educational materials for patients to inform them about their rights under HIPAA and how their PHI is used and protected. The RCC HIPAA Privacy Officer will work with impacted departments to provide clear and accessible information about how patients can exercise their rights and report privacy concerns.

Patient Rights

The RCC HIPAA Privacy Officer will educate employees and students about patient rights under HIPAA, including the right to access, amend, and restrict the use of their PHI. The RCC HIPAA Privacy Officer will establish processes for responding to patient requests promptly.

Communication with Patients

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, develop procedures for communicating with patients regarding their rights under HIPAA. The RCC HIPAA Privacy Officer will establish clear channels for patients to request access to their PHI, amendments to their records, and information about how their PHI is used and disclosed.

Confidential Communications Requirements

RCC-covered healthcare providers must permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the RCC-covered entity typically employs.

Any RCC-covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Secure Messaging

The RCC HIPAA Privacy Officer will ensure using secure messaging systems for PHI communication. The RCC HIPAA Privacy Officer will provide guidelines on the appropriate use of messaging platforms and the secure exchange of information.

Alternate Communication Methods

If communicating with patients or other entities, the RCC HIPAA Privacy Officer will establish secure and HIPAA-compliant alternative methods, such as encrypted email or secure patient portals.

Electronic Health Record (EHR) Security

If RCC uses EHR systems, the RCC HIPAA Privacy Officer will implement additional security measures to protect electronic health records. The RCC HIPAA Privacy Officer will work with RCC IT regularly to update and patch EHR systems to address security vulnerabilities.

Disclosures

Permitted Uses and Disclosures

RCC is permitted, but not required, to use and disclose PHI without an individual's authorization for the following purposes or situations:

- To the individual (unless required for access or accounting of disclosures);
- Treatment, Payment, and Healthcare Operations;
- Opportunity to Agree or Object;
- Incident to an otherwise permitted use and disclosure;

- Public Interest and Benefit Activities; and
- Limited Data Set for the purposes of research, public health, or healthcare operations.

RCC-covered healthcare components may rely on professional ethics and best judgments to decide which permissive uses and disclosures to make.

Public Interest and Benefit Activities.

The Privacy Rule permits the use and disclosure of PHI, without an individual's authorization or permission, for 12 existing national priority purposes as outlined in the HIPAA Privacy Rule. These disclosures are permitted, although not required, by the Privacy Rule in recognition of the important uses of health information outside of the healthcare context. Specific conditions or limitations apply to each public interest purpose, striking a balance between the individual privacy interest and the public interest need for this information.

Authorized Uses and Disclosures

RCC must obtain the individual's written authorization for any use or disclosure of PHI not for treatment, payment, healthcare operations, or otherwise permitted or required by the Privacy Rule. RCC may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting authorization except in limited circumstances.

An authorization must be written in specific terms. It may allow the use and disclosure of PHI by RCC or a third party.

All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

Required Disclosures

RCC must disclose PHI in only two situations:

- to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and
- to HHS when it is undertaking a compliance investigation or review, or enforcement action.

Remote Work Policies

The RCC HIPAA Privacy Officer will work with RCC-covered healthcare components to develop and implement procedures for remote employees accessing PHI. The RCC HIPAA Privacy Officer will ensure that remote work environments meet the same security standards as on-site locations. RCC does not currently have remote work environments that access EPHI.

Telehealth Security

RCC does not provide Telehealth Services.

Business Associate Contracts

When RCC uses a contractor or other non-RCC student or employee to perform "business associate" services or activities, HIPAA requires that RCC include certain protections for the information in a business associate agreement (in certain circumstances, governmental entities may use alternative means to achieve the same protections). In the business associate contract, RCC must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates. Moreover, RCC may not contractually authorize its business associate to use or disclose PHI that would violate HIPAA.

In coordination with the RCC HIPAA Security Officer and RCC Contract and Procurement, the RCC HIPAA Privacy Officer will maintain a current list of business associates with PHI access. The RCC HIPAA Privacy Officer will ensure all business associates sign and adhere to a HIPAA-compliant Business Associate Agreement. The RCC HIPAA Privacy Officer will work with RCC Contract and Procurement to review and update business associate agreements at least annually.

Third-Party Vendor Management

The RCC HIPAA Privacy Officer will develop and implement a vendor management program for third-party service providers that handle EPHI. The RCC HIPAA Privacy Officer will assess the HIPAA compliance of third-party vendors and regularly review their security practices. Before engaging with new vendors, the RCC HIPAA Privacy Officer will conduct security assessments to ensure they meet HIPAA compliance requirements. The RCC HIPAA Privacy Officer will regularly review and update vendor security assessments as part of the ongoing vendor management process.

Cloud Service Providers

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer, IT, and RCC Contract and Procurement, evaluate the HIPAA compliance of cloud service providers that store or process EPHI. The HIPAA Privacy Office will work with RCC Contract and Procurement to ensure that appropriate agreements, such as Business Associate Agreements, are in place with cloud service providers.

IT Security

In coordination with the RCC HIPAA Security Officer and IT, the RCC HIPAA Privacy Officer will develop, implement, and review a documented process for guarding against,

detecting, and reporting malicious software that poses risks to PHI. RCC's malicious software prevention, detection, and reporting procedures shall include:

- Anti-virus software installed and updated on PHI Systems.
- Procedures for RCC students and employees to report suspected or confirmed malicious software.
- Plan for recovering from malicious software attacks.
- Process to examine electronic mail attachments and downloads before they can be used on PHI Systems.

RCC employees and students shall not bypass or disable anti-virus software installed on EPHI Systems unless properly authorized.

RCC will provide annual training and awareness to covered RCC employees and students about guarding against, detecting, and reporting malicious software.

The RCC HIPAA Privacy Officer will, in coordination with the RCC HIPAA Security Officer and IT, develop, implement, and review a documented process for monitoring login attempts to EPHI Systems and reporting login discrepancies.

RCC will provide training and awareness annually and as needed to covered RCC employees and students regarding the procedures for monitoring login attempts and reporting discrepancies regarding their access or login attempts.

Incident Reporting

RCC shall include, as appropriate, in its documented process for promptly identifying security incidents, the following:

- Risk analysis of PHI Systems, as outlined in RCC's Risk Analysis operational specification.
- Based on the risk analysis, identify what events constitute a security incident in the context of RCC's and the RCC covered healthcare component's operations.
- Process for identifying a security incident.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall organize a Security Incident Response Team (SIRT), which is primarily responsible for security incident reporting and response, in coordination with IT if RCC IT systems are involved in the breach. They will perform an investigation when evidence shows that a security incident has occurred and will respond promptly to the security incident. RCC shall document its process for promptly responding to security incidents.

The SIRT will consist of the following positions:

- RCC Director of Risk Management
- Director of Dental Programs
- Chief Information Officer

- Director, Athletics, Fitness and Recreation Programs

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall include, as appropriate, in its documented process for promptly reporting security incidents, a procedure for RCC students and employees to report a security incident to the RCC HIPAA Privacy Officer. An RCC student or employee will not prohibit or otherwise attempt to hinder or prevent another RCC student or employee from reporting a security incident to the SIRT and shall cooperate fully with security incident investigations.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall include training and awareness for covered RCC students and employees, as appropriate, in its documented process for promptly identifying, reporting, tracking, and responding to security incidents in accordance with RCC's and the RCC covered healthcare component's security policies and procedures.

The RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall mitigate, to the extent practicable, harmful effects of security incidents that are known to the RCC-covered entity and document those security incidents and their outcomes.

When performing a risk assessment, the RCC HIPAA Privacy Officer and the RCC HIPAA Security Officer shall assess the probability that the EPHI has been compromised based on considerations that include at least the following four factors:

- the nature and extent of the PHI involved, including the types of identifiers and the 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.

Documentation of Breaches

RCC-covered entities and business associates, where applicable, have the discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the PHI has been compromised.

There are three exceptions to the definition of "breach."

- The first exception applies to the unintentional acquisition, access, or use of PHI by an RCC student, employee, or person acting under the authority of an RCC-covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at an RCC-covered entity or business associate to another person authorized to access PHI at the RCC-covered entity or business associate, or organized healthcare arrangement in which the RCC-covered entity

participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception applies if the RCC-covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

The RCC HIPAA Privacy Officer will document any breaches of PHI, including the nature of the breach, the individuals affected, and the corrective actions taken. The RCC HIPAA Privacy Officer will report breaches to the college, law enforcement, affected individuals, and HHS.

Following a breach of unsecured PHI, RCC-covered entities must notify affected individuals, the Secretary of HHS, and, in certain circumstances, the media. In addition, business associates must notify RCC-covered entities if a breach occurs at or by the business associate.

Individual Notice

RCC must notify affected individuals after discovering a breach of unsecured PHI. RCC entities must provide this individual notice in written form by first-class mail or email if the affected individual has agreed to receive such notices electronically. If RCC has insufficient or out-of-date contact information for ten or more individuals, RCC must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. RCC must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If RCC has insufficient or out-of-date contact information for fewer than ten individuals, RCC may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach; the steps affected individuals should take to protect themselves from potential harm, a brief description of what RCC is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for RCC or business associates, as applicable.

Concerning a breach at or by a business associate, while RCC is ultimately responsible for ensuring individuals are notified, RCC may delegate the responsibility of providing individual notices to the business associate. RCC and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of RCC and which entity has a relationship with the individual.

Media Notice

In addition to notifying the affected individuals, if RCC experiences a breach affecting more than 500 residents of a state or jurisdiction, RCC is required to notify prominent media outlets serving the state or jurisdiction. RCC may notify appropriate media outlets serving the affected area through a press release. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. It must include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), RCC must notify the Secretary of HHS of breaches of PHI. RCC will notify the Secretary of HHS by visiting the HHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, RCC must notify the Secretary of HHS without unreasonable delay and in no case later than 60 days following a breach. If a breach affects fewer than 500 individuals, RCC may notify the Secretary of HHS of such breaches annually. Reports of breaches affecting fewer than 500 individuals are due to the Secretary of HHS no later than 60 days after the end of the calendar year in which the breaches are discovered.

Post-Incident Review

The RCC HIPAA Privacy Officer will conduct a thorough post-incident review after a PHI breach or security incident to identify lessons learned and areas for improvement. The RCC HIPAA Privacy Officer will update policies and procedures based on insights gained from the post-incident review.

Continuous Improvement

In collaboration with impacted departments, IT, Contract and Procurement, the RCC HIPAA Privacy Officer will establish a process for continuous improvement of HIPAA compliance efforts. The RCC HIPAA Privacy Officer will regularly review and update procedures in response to technology, regulations, or college structure changes. The RCC HIPAA Privacy Officer will stay informed about updates to HIPAA regulations and adjust practices accordingly.

Legal Updates

The RCC HIPAA Privacy Officer will stay informed about changes to healthcare and privacy laws that may impact HIPAA compliance. The RCC HIPAA Privacy Officer may seek legal advice to ensure ongoing compliance with evolving legal requirements.

Rescinds Procedure Number: None

Approved: September 5, 2024