Policy Title Workforce Security
Department County Manager's Office
Chapter 5
Section 5
Policy 4
Effective Date Wednesday, December 18, 2019

POLICIES & PROCEDURES

1. General

It is the policy of Ramsey County to ensure that all members of its workforce have appropriate access to electronic protected health information (PHI) and to prevent workforce members from inappropriate, unauthorized access to electronic PHI, according to HIPAA regulations on workforce security. Included immediately below and throughout this document are references and links to HIPAA regulations, which are hereby incorporated and made part of this document, and therefore must be read as part of this Policy.

Key HIPAA Regulations (incorporated by reference):

- **45 C.F.R. § 164.308(a)(3)(i) Workforce Security (Required)**
- **45 C.F.R. § 164.308(a)(3)(ii)(A) Workforce Authorization and/or Supervision (Addressable)**
- **45 C.F.R. § 164.308(a)(3)(ii)(B) Workforce Clearance Procedure (Addressable)**
- **45 C.F.R. § 164.308(a)(3)(ii)(C) Establish Termination Procedures (Addressable)**

As a HIPAA Hybrid Entity, Ramsey County designates its HIPAA Health Care Components in accordance with HIPAA regulations, as set forth in Ramsey County's Administrative Policy Manual. Ramsey County applies this Policy on Workforce Security to its HIPAA Health Care Components and its other personnel who support HIPAA compliance. When workforce security procedures are required for purposes other than HIPAA, Ramsey County applies other policies as set forth in Ramsey County's Administrative Policy Manual.

To implement this Policy, Ramsey County uses procedures to ensure workforce members have appropriate access to electronic PHI; but only to the extent required for each workforce member to accomplish assigned job duties. Access privilege levels are assigned no higher than necessary to accomplish job duties; and must be appropriately approved and communicated. Appropriate access levels are determined according to job descriptions. Access privilege levels must be approved by managers in consultation with the HIPAA Security Official, communicated to workforce members, and documented in personnel files and other HIPAA Security documentation under the control of the HIPAA Security Official. By receiving communications from managers on assigned privilege levels, workforce members are empowered to identify and report unintended, incidental access to unauthorized electronic PHI. Documentation of assigned privilege levels, along with documentation demonstrating that access privilege levels correlate with job descriptions, is available for review through the HIPAA Security Official.

To implement this policy, Ramsey County also implements the following related sub-policies and procedures:

2. Authorization and/or Supervision (Addressable)

It is the policy of Ramsey County to carefully manage and document the authorization process for workforce members who need access to electronic PHI, in accordance with HIPAA regulations at **45 C.F.R. § 164.308(a)(3)(i) Workforce Security** (Required). The following procedures describe this authorization process.

First, all workforce members are assigned to organizational units, as shown on Ramsey County organizational charts, and receive supervision from the designated manager/supervisor. When access to electronic PHI is needed to perform job responsibilities, an access request form is used by managers/supervisors to submit requests for access to information systems, including electronic PHI. The access request form identifies the manager/supervisor submitting the form, the name and other identifying information for the workforce member who needs access, a description of the information and/or level of access needed including a specific notation referencing electronic PHI when applicable, and an area for sign off by the HIPAA Security Official or designee to show if, when, and how the requested access has been granted. Additional approval/sign off may be needed for certain applications. When using access request forms, it is important that the manager/supervisor, the workforce member, and the HIPAA Security Official all have an understanding of the Ramsey County HIPAA Health Care Component ("HCC") and whether the access request involves PHI or not, based on the most current version of the HCC. This is made clear on the request form by the manager/supervisor. It also is confirmed during review by the HIPAA Security Official. Before a request for access to electronic PHI is granted, a call is made or an email is sent by the HIPAA Security Officer or designee to the manager/supervisor making the request, to verify the request is in fact authorized. After authorized access privilege levels have been properly configured as described on the access request form, and before the new level of access is made available to the workforce member, the account is tested under the direction of the HIPAA Security Official. As part of the process, the access request form, along with related documentation, is saved in a manner that it is accessible to both the HIPAA Security Official or designee as part of a master list or index of all requests for access to electronic PHI and also accessible to the requesting manager/supervisor as part of the employee/contractor record. To ensure that managers/supervisors perform these required procedures, performance criteria for managers/supervisors include adherence to these procedures.

These procedures follow the standard implementation specifications in HIPAA rules for workforce security authorization. If the HIPAA Security Official ever determines that an alternative measure is needed, the Security Official will document why the standard implementation specification is not a reasonable and appropriate safeguard, as well as the equivalent alternative measure to be implemented instead.

3. Workforce Clearance Procedure (Addressable)

It is the policy of Ramsey County to carefully manage and document the workforce clearance process to determine whether all workforce members' access to electronic PHI is appropriate, in accordance with HIPAA regulations at **45 C.F.R. § 164.308(a)(3)(ii)(A) Workforce Clearance** Procedure (Addressable). The following procedures describe this workforce clearance process.

First, all workforce members are assigned to organizational units, as shown on Ramsey County organizational charts, and receive supervision from the designated manager/supervisor. When access to electronic PHI is needed to perform job responsibilities, an access request form is used by managers/supervisors to submit requests for access to information systems, including electronic PHI. Prior to authorizing access to electronic PHI for a workforce member, the manager/supervisor carefully reviews the job description and documents the level of access needed to complete assigned job responsibilities. This is documented on the access request form as well as the personnel file kept by the manager/supervisor. The manager/supervisor also confirms that the workforce member has the correct/appropriate professional credentials to receive the access levels being requested; and that the workforce member does not have a negative disciplinary record regarding improper use or disclosure of PHI such that providing access to the workforce member would create significant risk for Ramsey County.

Access levels also are reviewed/revalidated by managers/supervisors on an ongoing basis. At least annually, the manager/supervisor reviews the job description to verify that the current level of access is required to complete assigned job responsibilities or request a change in access levels; and also reviews the work history and disciplinary record of the workforce member for improper use or disclosure of PHI. This revalidation is often done to coincide with employee performance reviews, updates to job descriptions, HIPAA training, and/or other events during the year that make good triggers for re-validating access to electronic PHI. Documentation on the revalidation process is created and kept by managers/supervisors in their personnel files. A copy or a confirmation of each revalidation also is sent to the HIPAA Security Official for the purpose of maintaining a master index of each initial clearance and revalidation performed, as required by HIPAA regulations.

These procedures follow the standard implementation specifications in HIPAA rules for workforce clearance procedures. If the HIPAA Security Official ever determines that an alternative measure is needed, the Security Official will document why the standard implementation specification is not a reasonable and appropriate safeguard, as well as the equivalent alternative measure to be implemented instead.

4. Establish Termination Procedures (Addressable)

It is the policy of Ramsey County to terminate access to electronic PHI when it is no longer needed and to establish and maintain procedures to ensure appropriate and timely termination of access to electronic PHI, in accordance with HIPAA regulations at **45 C.F.R. § 164.308(a)(3)(ii)(A) Establish Termination Procedures** (Addressable). The following procedures describe how access is terminated and how related processes are managed.

First, all workforce members are assigned to organizational units, as shown on Ramsey County organizational charts, and receive supervision from the designated manager/supervisor. When employment or other contractual arrangements are terminated for workforce members (including business associates), the exit/termination process for the workforce member includes termination of access to electronic PHI, as well as a discussion of privacy and security topics regarding electronic PHI (as discussed at the end of this Section). More specifically, when termination of a workforce member is anticipated in advance, the manager/supervisor is required to and does complete an access termination form, similar in content to the access request form discussed above in this Policy at Section 2. However, instead of requesting access be turned on, this form requests that access to electronic PHI be disabled. Whenever possible, this form is submitted by the manager/supervisor in advance and includes a particular date/time for the request to become effective. This allows the HIPAA Security Official or designee to schedule the access termination. When it is not possible for a manager/supervisor to submit this form in advance, the form and transmittal documents can indicate "URGENT STATUS" to receive immediate attention from and action by the HIPAA Security Official or designee. Because access is being terminated rather than activated, the verification step for the request access form (to verify submission by a manager/supervisor) does not apply. At the same time as when termination of access is requested to take effect, the supervisor/manager also recovers and takes control of all Ramsey County-owned devices used by the employee/contractor to access electronic PHI. This provides a second level of protection against unauthorized access to electronic PHI.

When a workforce member requires a change in access levels, the same basic procedure for access termination is used; except that the request for termination of access is accompanied by a corresponding request for access to a different level of information. In other words, the old access is terminated, and the new access is activated. Both of the procedures described above can be followed separately, or a change request form can be used that consolidates both procedures. Either way, the new access request requires the same verification of authorization as described above in this Policy at Section 2.

The exit process for workforce members with access to electronic PHI includes a discussion of HIPAA privacy and security topics regarding electronic PHI. The discussion asks specific questions about whether the workforce member has experienced or has knowledge of any unauthorized access to electronic PHI; whether the workforce member has any complaints with regard to procedures for managing the privacy and security of electronic PHI; whether the workforce member is aware of any weaknesses and procedures that could lead to a potential security incident or data breach; and whether the workforce member is aware of any electronic PHI on any external devices. The discussion also includes open questions about ideas or suggestions for improving procedures for protecting the privacy and security of electronic PHI.

These procedures follow the standard implementation specifications in HIPAA rules for access termination procedures. If the HIPAA Security Official ever determines that an alternative measure is needed, the Security Official will document why the standard implementation specification is not a reasonable and appropriate safeguard, as well as the equivalent alternative measure to be implemented instead.

APPLICABILITY

The workforce of Ramsey County HIPAA Health Care Components (including employees, volunteers, students, and interns); and other Ramsey County personnel who support HIPAA compliance.

GENERAL INFORMATION

N/A

AUTHORITY

This policy and the procedures herein were prepared under the authority of the County Manager, as delegated to the Data Board. This policy complies with:

- The Health Insurance Portability and Accountability Act (P.L.104-191), as amended ("HIPAA"); the Health Information Technology for Economic and Clinical Health Act OF 2009 ("HITECH"); and the corresponding implementation rules of both Acts, which are officially known as Administrative Simplification rules codified at 45 C.F.R. §§ 160-164 (more commonly referenced as "HIPAA Rules" and/or "HIPAA regulations").

DEFINITIONS

Please see **Policy 6.1.1, Master List of HIPAA Definitions**.

RESPONSIBILITIES

Please see **Policy 5.5.1.3, Assigned Security Responsibility**.

LINKS AND RESOURCES

See links in policy text above.

CONTACTS / SUBJECT MATTER EXPERTS

Ramsey County HIPAA Security Official

REVISION HISTORY

Date	Brief description of change
12/18/2019	This policy replaces the HIPAA Workforce Security provisions that are part of the *Login and Access Security, Maintenance and Reporting* policy and procedure document found in Chapter 5, Section 5, Subsection 2, Policy ODP-S005 and Procedure ODP-S005. That policy will remain in effect as written but only to the extent it contains other HIPAA requirements and/or addresses requirements under other laws.

APPROVAL

John Siqveland

Data Board Chair

December 16, 2019
Revision History Date Wednesday, December 18, 2019