

Policy Title Documentation

Department County Manager's Office

Chapter 5

Section 5

Policy 2

Effective Date Wednesday, December 18, 2019

POLICIES & PROCEDURES

1. GENERAL

It is the policy of Ramsey County to create and keep all documentation required by the HIPAA Security Rule, including required documentation on actions, activities, and assessments; and to do so in a manner that complies with the HIPAA Security Rule specifications on time limits, availability, and updates. Included immediately below and throughout this set of policies and procedures 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. § 164.316 \(b\) Documentation \(in Security Rule\)](#)

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 Documentation to its HIPAA Health Care Components and its other personnel who support HIPAA compliance. When security documentation is required for purposes other than HIPAA, Ramsey County applies other policies as set forth in Ramsey County's Administrative Policy Manual.

2. TIME LIMITS (Required)

It is the policy of Ramsey County to retain all documentation required by the Security Rule, including policies and procedures, in written form for six (6) years after the retirement date; including revisions and outdated materials, accurately labeled with effective dates and revision dates. When documentation is created or updated, effective dates are used at the top and a record of revision history is kept at the bottom. The revision history includes a log of each revision date and corresponding description of the change, including old documentation reference numbers as applicable. Current policies and procedures are kept on the County Administrative Procedure Manual in Chapter 5 - Information Technology, Section 5-1 (Updated HIPAA Security Policies and Procedures). Current other documentation required by the Security Rule on actions, activities, and assessments are kept by the HIPAA Security Official in binders/folders that are accessible to the workforce that supports HIPAA security. Similarly, out-of-date policy and procedure provisions and other documentation is kept in binders/folders by the HIPAA Security Official that are accessible to the workforce that supports HIPAA security. Out-of-date policy and procedure provisions and other documentation is kept at least six (6) years from the date it was last in effect. Periodic purge efforts managed and logged by the HIPAA Security Official destroys documentation after it is at least six years old and is no longer of any value to the workforce that supports HIPAA Security.

3. AVAILABILITY (Required)

It is the policy of Ramsey County to make all documentation required by the Security Rule available to those persons responsible for implementing Security Rule policies and procedures. HIPAA Security Rule Policies and Procedures are available on the Administrative Policy Manual electronic portal for access by the workforce of Ramsey County HIPAA Health Care Components and other Ramsey County personnel who support HIPAA compliance. Notice is provided from time to time regarding the existence of the Administrative Policy Manual and requirements for access and review. Other required Security Rule documentation is kept by the HIPAA Security Official in binders/folders that are accessible to the workforce that supports HIPAA security; and the HIPAA Security Official provides periodic notice to the workforce that supports HIPAA security of such documentation and its required use. Notices include language that requires the workforce that supports HIPAA security to access and use such documentation on a regular basis and when required by security planning, implementation, and response. Notices are kept by the HIPAA Security Official to demonstrate compliance with this Policy on Documentation. To further document compliance, the HIPAA Security Official will migrate at a future date HIPAA Security Rule Policies and Procedures and other required documentation to the ComplyPAK software, where individual access and use by workforce members can be logged.

4. UPDATES (Required)

It is the policy of Ramsey County to review documentation periodically, and update it as needed, in response to environmental and/or operational changes affecting the security of electronic Protected Health Information. Whenever the HIPAA Security Official becomes aware of an environmental or operational change that affects the security of electronic Protected Health Information, he/she takes appropriate steps to make corresponding changes to the HIPAA Security Policies and Procedures and other required documentation. In addition, the HIPAA Security Official performs periodic reviews across the entire scope of HIPAA Security Policies and Procedures and other required documentation. As changes are made, appropriate notices are sent out to the appropriate members of the workforce that support HIPAA security. To demonstrate compliance with this Policy on Documentation and the HIPAA Security Rules, the HIPAA Security Official maintains a log that is readily accessible to auditors that shows all periodic reviews conducted and specific changes implemented in response to environmental and operational changes, as described above.

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 is a new policy

APPROVAL

John Siqveland

Data Board Chair

December 16, 2019

Revision History Date Wednesday, December 18, 2019

[← Assigned Security Responsibility](#)

[Back](#)

[Workforce Security >](#)
