

HIPAA Security Rule



POLICY & PROCEDURE Policies and Procedures		POLICY #19
SUPERCEDES POLICY:	EFFECTIVE:	LAST REVIEWED:
Privacy and Security Compliance Program Exhibit EE, Documentation Retention and Storage	3/1/2014	5/10/2024

Purpose

To address the requirement to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements contained in the Health Insurance Portability and Accountability Act (HIPAA) Regulations, 45 C.F.R. §164.316(a).

Consult with Legal Counsel for any applicable state security or breach laws with respect to matters governed by this policy and procedure to determine any additional requirements. Other federal laws may also apply.

Applicability

All Watershed Health, Inc. (Watershed) Workforce members are responsible for awareness of this policy and adherence to the given direction and guidance.

Definitions

For definitions of capitalized terms or phrases, please refer to *Privacy, Security and Breach Notification Glossary*.

Policy

It is the policy of Watershed to develop, implement, modify (when needed or appropriate), and retain Policies and Procedures and to work to assure that Watershed’s Workforce members comply with those Policies and Procedures.

Procedures

1. The Security Officer or designee is responsible for the development and implementation of policies and procedures and to maintain them in written form (paper and/or electronic).
2. Changes to policies and procedures. If Watershed changes its policies and procedures, the changes will be documented and implemented as follows:
 - a. **Flexible Approach.** Watershed will use security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as specified in the HIPAA Security Rule. In deciding which security measures to use, Watershed must take into account the following factors:

HIPAA Security Rule

-
- i. Its size, complexity and capabilities;
 - ii. Its technical infrastructure, hardware, and software security capabilities;
 - iii. The costs of security measures; and
 - iv. The probability and criticality of potential risks to Electronic Protected Health Information (ePHI).
 - b. **Addressable specifications.** Watershed will decide what addressable implementation specifications are reasonable and appropriate based on size, complexity, capabilities, technical infrastructure, hardware and software security capabilities, cost, and risk analysis results.
 - i. Watershed will implement addressable implementation specifications determined to be reasonable and appropriate. If implementing an addressable implementation specification is not reasonable and appropriate, Watershed will:
 - (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
 - (2) Implement an equivalent alternative measure, if reasonable and appropriate.
 - (3) Ensure the documentation of the decision and alternative measures are retained in accordance with *Security Policy #20, Documentation*.
3. The Security Officer or designee will ensure that Watershed's policies have been reasonably designed to consider the size and type of activities undertaken by Watershed with respect to ePHI.
 - a. If the review does not result in changes to the policies and procedures, the documents will be updated to reflect the annual review.
 - b. If the review results in changes to the policies and procedures, a revised version of the policy will be created, and the previous version will be deactivated and electronically stored in a central location, upon the approval date of the new version, and in accordance with the retention requirements.
 4. Watershed will monitor and assure that any necessary revisions are made to Watershed's Security Policies and Procedures in a timely manner following changes in Watershed's organization, operations, or technology capabilities and, as needed, following a Security Incident and/or an impermissible use or disclosure of PHI.
 5. The Security Officer or designee will properly document and implement any changes to policies and procedures as necessary, in accordance with *Security Policy #20, Documentation*.
 6. Annually, the President or designee will review and accept the policies and procedures by formal processes approved by Watershed, date all accepted policies and procedures, and include the name or role of the accepting person or body.
 7. Watershed will retain the policies and procedures and make them available in accordance with *Security Policy #20, Documentation*.

HIPAA Security Rule

Enforcement

Violations of this policy will result in imposition of sanctions in accordance with Watershed sanctions policy. This may include suspension or loss of the violator's use privileges, with respect to Watershed's information systems, termination of employment or volunteer, intern, contractor status with Watershed. Additional civil, criminal and equitable remedies may apply.

Documentation

The Security Officer or designee is responsible for ensuring this version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by Watershed for a period of at least 6 years plus the current year from the date of creation or the date when last in effect, whichever is later.

References

Regulatory Authority:

1. 45 C.F.R. §164.306(a) General requirements.
2. 45 C.F.R. §164.316(a) Standard: Policies and procedures.

Internal:

1. Security Policy #20, Documentation

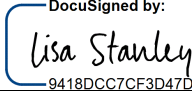
External:

1. [Current Administrative Simplification Regulations](#)
2. HHS Guidance – [Guidance on Risk Analysis Requirements under the HIPAA Security Rule](#)
3. Refer to *NIST CSF Subcategory & Control Mapping* at the end of this document

HIPAA Security Rule



Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	<div>DocuSigned by:  9418DCC7CF3D47D...</div>
(Printed Name)	(Date)	(Signature)

REVISION HISTORY			
Date	Author	Version	Comments
3/1/2014	Arthur Grant	1.0	Implemented
2/19/2015	Lisa Stanley	2.0	Reviewed
2/23/2016	Lisa Stanley	3.0	Reviewed
1/30/2017	Lisa Stanley	4.0	Reviewed
3/3/2018	Lisa Stanley	5.0	Reviewed
9/3/2019	Lisa Stanley	6.0	Reviewed
3/18/2020	Lisa Stanley	7.0	Reviewed
11/13/2020	Scott Snodgrass	8.0	Reviewed and updated by Privacy & Security Officer
11/11/2021	Lisa Stanley	8.0	Reviewed
5/20/2022	Lisa Stanley	8.0	Reviewed
5/15/2023	Nicole Montagnet	9.0	Reviewed and updated by Privacy & Security Officer
5/10/2024	Nicole Montagnet	9.0	Reviewed

NIST CSF Subcategory & Control Mapping

Policies and Procedures			
HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.316		ID.BE-1: The organization’s role in the supply chain is identified and communicated	NIST SP 800-53 Rev. 4 CP-2, SA-12
164.316		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	NIST SP 800-53 Rev. 4 CP-2, SA-12
164.316		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	NIST SP 800-53 Rev. 4 PM-11, SA-14
164.316		ID.GV-1: Organizational information security policy is established	NIST SP 800-53 Rev. 4 PM-1, PS-7
164.316		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
164.316		ID.RA-3: Threats, both internal and external, are identified and documented	NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
164.316(a)		ID.RA-4: Potential business impacts and likelihoods are identified	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
164.316(a)		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16