

HIPAA Security Rule



POLICY & PROCEDURE Information Access Management		POLICY #4
SUPERCEDES POLICY:	EFFECTIVE:	LAST REVIEWED:
Privacy and Security Compliance Program Exhibit N, Information Access Management	3/1/2014	5/10/2024

Purpose

To implement and maintain policies and procedures for authorizing and controlling access to electronic Protected Health Information (ePHI) and the processes surrounding how that access is granted and modified.

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

Watershed’s Supervisors/Managers, in conjunction with the Human Resources Department and Security Officer, or designee, are responsible for ensuring the establishment and modification of access to ePHI, including:

- a. **Access Authorization (Addressable).** Watershed will implement procedures for granting access to ePHI through access to a Workstation, transaction, program, process, or other mechanism.
- b. **Access Establishment and Modification (Addressable).** Watershed will implement procedures to establish, document, review, and modify a Workforce member's right of access to a Workstation, transaction, program, or process.

Procedures

1. Access Authorization.

HIPAA Security Rule



-
- a. Supervisors/Managers are responsible for ensuring that Workforce members under their direct supervision comply with the following requirements:
 - i. Use the ePHI only for purposes authorized by Watershed.
 - ii. Not disclose ePHI unless authorized to do so.
 - b. Workforce members will not be granted access to a system/application, workstation, transaction, program, or process unless they have a need for access.
 - c. Workforce members will be granted only the minimum access necessary to perform job functions requiring such access to a system/application, workstation, transaction, program, or process.
2. The following protocol will be used to determine a new Workforce member and existing Workforce member's initial right of access:
- a. New Hire Checklist will be used for onboarding new and modifying existing Workforce members.
 - i. Workforce members will not be granted access to ePHI unless they have a need for access.
 - ii. Workforce members will be granted only the minimum access necessary to perform duties requiring such access to ePHI.
 - iii. Access should be limited to necessary tasks, such as read-only, read and copy, read and edit by adding a new entry and should consider access to a Workstation, transaction, program, process, or other mechanism.
3. Access Establishment and Modification.
- a. Should Supervisor/Manager determine that an access permission change is necessary, this would be reviewed by the Security Officer or designee, considering the principles of least privilege, need-to-know, and separation of duties in deciding the new access permissions.
 - b. If a Workforce member's duties, role, function, or responsibilities change, the access permissions of that Workforce member will be re-evaluated. All modifications and reasons for modifications will be documented via the access control inventory.
 - i. Supervisors/Managers are responsible for ensuring that any additions or changes are submitted to the Security Officer, or designee, using the approved system.
 - c. Termination procedures and required documentation are described in *Security Policy #3, Workforce Security*.
4. Access Review
- a. All accounts (including user, privileged, system, shared, and seeded accounts) and privileges (e.g. user-to-role assignments, user-to-object assignments) will be reviewed quarterly. Any required modifications or adjustments shall follow the procedures above.

HIPAA Security Rule



5. Responsibilities.

- a. Watershed's Human Resources Department, in consultation with the Security Officer, Privacy Officer, system owner, and other appropriate individuals, is responsible for developing appropriate Access Authorization Levels and Personnel Clearance Levels, as described in *Security Policy #3, Workforce Security* and *Privacy Policy #30, Minimum Necessary Uses, Disclosures, and Requests*.

6. All Watershed's Workforce members shall be trained regarding appropriate access to ePHI, including the awareness of information access controls.

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. §164.308(a)(4)(i) – Standard: Information access management.
2. 45 C.F.R. §164.308(a)(4)(ii)(B) – Access authorization.
3. 45 C.F.R. §164.308(a)(4)(ii)(C) – Access establishment and modification.

Internal:

1. Security Policy #3, Workforce Security
2. Security Policy #21, Mobile Device Security
3. Security Policy #22, Data Governance and Data Classification
4. Privacy Policy #30, Minimum Necessary Uses, Disclosures, and Requests

HIPAA Security Rule



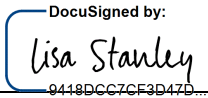
External:

1. [Current Administrative Simplification Regulations](#)
2. 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
5/4/2023	Nicole Montagnet	9.0	Reviewed and updated by Privacy & Security Officer
5/10/24	Nicole Montagnet	9.0	Reviewed

HIPAA Security Rule



NIST CSF Subcategory & Control Mapping

Information Access Management: Access Authorization & Access Establishment and Modification			
HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(4)(ii)(A)		ID.AM-4: External information systems are catalogued	NIST SP 800-53 Rev. 4 AC-20, SA-9
164.308(a)(4)		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders	NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
164.308(a)(4)(ii)		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
164.308(a)(4)(ii)		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
164.308(a)(4)		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	NIST SP 800-53 Rev. 4 PM-1, PS-7
164.308(a)(4)		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
164.308(a)(4)		PR.AC-1: Identities and credentials are managed for authorized devices and users	NIST SP 800-53 Rev. 4 AC-2, IA Family
164.308(a)(4)(i)		PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
164.308(a)(4)		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
164.308(a)(4)(ii)(B)		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7
164.308(a)(4)		PR.DS-5: Protections against data leaks are implemented	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
164.308(a)(4)		PR.DS-7: The development and testing environment(s) are separate from the production environment	NIST SP 800-53 Rev. 4 CM-2

HIPAA Security Rule



HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(4)		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	NIST SP 800-53 Rev. 4 AC-3, CM-7
164.308(a)(4)		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14