POLICY & PROCEDURE **Assigned Security Responsibility**		**POLICY #2**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 2 v.9 Assigned Security Responsibility	3/1/2014	**5/10/2024**

Purpose

To ensure the designation of the responsible person for overseeing Watershed Health, Inc. (Watershed) obligations to maintain the security of systems and information, including Electronic Protected Health Information (ePHI), in accordance with state and federal privacy and security laws and the Health Insurance Portability and Accountability Act (HIPAA) Regulations.

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 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 will identify a Security Officer who is responsible for the development and implementation of the policies and procedures required by Watershed's Data Governance Policy and the HIPAA Security Rule.

This policy establishes how the Security Officer will serve as the lead for security compliance-related activities and responsibilities, as listed below. The Security Officer is charged with developing, maintaining, and implementing organizational policies and procedures, conducting or directing educational programs, reviewing the performance of those with assigned security responsibilities, and administering reviews and conducting assessments related to the company's security program.

Procedures

1. Appointment of the Security Officer. Watershed's Cybersecurity Oversight Committee will appoint a Security Officer to be responsible for ensuring compliance with security requirements throughout Watershed.
2. Responsibilities of Security Officer. The Security Officer will have the responsibilities set forth in *Appendix 1*: Responsibilities of the Security Officer.
3. Contacting the Security Officer. The Security Officer can be contacted via Watershed's secure email mike.neal@watershedhealth.com (24) hours a day, seven (7) days a week.
4. In the event of an incident, a report must be completed immediately upon becoming aware using the *Security Matter Reporting Form found on the Watershed staff website (staff.watershedhealth.com)*. Incident report submission should follow the steps outlined on the Security Matter Reporting Form.
5. Contact information for the Security Officer will be uploaded to the Watershed staff website and Security Officer changes will be promptly updated to the staff website and communicated to the Workforce.
6. The Security Officer serves as a resource regarding matters of security, and on a periodic basis, either the Security Officer or designee may report the status of security activities to the Watershed Board of Directors.

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)(2) – Standard: Assigned security responsibility.

Internal:

1. Security Policy #6, Security Incidents
2. Reporting and Assessment Form

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

Appendix 1: Responsibilities of the Security Officer

Purpose:

The Security Officer is responsible for Watershed's compliance with state and federal security laws and the HIPAA Security Rules.

Qualifications:

The Security Officer must demonstrate skills, knowledge and experience with the practical and legal requirements relating to security of information in electronic format and with Watershed's information system operations. The Security Officer must be familiar with organizational operations, to include a solid understanding of the IT infrastructure and deployed hardware and software which create, receive, transmit or store information and ePHI, to ensure proper security controls are implemented and effectively protecting those assets. The Security Officer must have the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel. The Security Officer responsibilities will cover administrative, operational, technical (including hardware and software security), physical security issues, and, in consultation with Legal Counsel, legal issues.

Responsibilities:

The Security Officer leads in the development, training and enforcement of information security policies and procedures regarding ePHI, in addition to measures and mechanisms to strengthen prevention, detection, containment, and correction of security violations involving ePHI. He/she will also ensure that the policy/procedure requirements comply with federal and state statutory and regulatory requirements regarding security of ePHI. The Security Officer will be responsible for:

1. Maintaining documented security policies regarding information and ePHI that include:
    a. Administrative Safeguards:
        i. Security Management Process - Implementing processes and procedures for the periodic conduct of risk analysis, risk management activities, information system activity reviews and appropriate sanctions for failure to comply with Watershed security policies and procedures. 45 C.F.R. §164.308(a)(1).
        ii. Workforce Security – Implementing policies and procedures to ensure appropriate access to ePHI, including addressable implementation specifications for authorization and/or supervision, Workforce clearance procedures, and termination procedures for Workforce members. 45 C.F.R. §164.308(a)(3).
        iii. Information Access Management – Implementing policies and procedures consistent with the Privacy Rule for authorization of access to ePHI, including addressable access

authorization and access establishment and modification policies and procedures.[1] 45 C.F.R. §164.308(a)(4).

iv. Workforce training – Implementing a security awareness and training program for all Workforce members. Includes addressable implementation specifications of (a) security reminders, (b) protection from malicious software, (c) log-in monitoring, and (d) password management. 45 C.F.R. §164.308(a)(5).

v. Security Incident policies and procedures – Implementing policies and procedures to address Security Incidents, including an addressable implementation specification of response and reporting. 45 C.F.R. §164.308(a)(6).

vi. Contingency Plan – Implementing policies and procedures for responding to an emergency or occurrence that damages systems containing ePHI, including establishing data backup, disaster recovery, and emergency mode operation plans, and addressable implementation specifications of (a) testing and revision of contingency plans, and (b) assessing the criticality of specific applications and data in support of other contingency plan components. 45 C.F.R. §164.308(a)(7).

vii. Evaluation - Performing a periodic technical and non-technical evaluation that establishes the extent to which Watershed's HIPAA security policies and procedures meet the requirements of the Security Rule. 45 C.F.R. §164.308(a)(8).

viii. Business Associate Agreements and Other Arrangements –Implementing procedures for ensuring satisfactory assurances are received from business associates, and for ensuring that the documentation requirements for such assurances are met. 45 C.F.R. §164.308(b).

b. Physical Safeguards: Managing the physical requirements related to ePHI.

i. Facility Access Controls – Implementing policies and procedures to limit physical access to ePHI systems and the facilities where they are housed, while ensuring proper access is allowed. Includes addressable implementation specifications for facility security plans, access control and validation procedures, maintenance records and contingency operations. 45 C.F.R. §164.310(a)(1).

ii. Workstation Use –Establishing procedures to ensure proper functions to be performed on workstations that can access ePHI, the manner in which those functions are performed, and the physical attributes of the area(s) of the workstations. 45 C.F.R. §164.310(b).

[1] If a Health Care Clearinghouse is part of the entity, the Health Care Clearinghouse must implement policies and procedures that protect its ePHI from unauthorized access by the larger organization. This is a required implementation specification for the Information Access Management Standard. 45 C.F.R. §164.308(a)(4).

iii. Workstation Security – Implementing safeguards for the prevention of unauthorized physical access to workstations processing ePHI while ensuring appropriate access. 45 C.F.R. §164.310(c).

iv. Device and Media Controls – Implementing procedures governing receipt and removal of hardware and Electronic Media that contain ePHI (i) into and out of remote work areas; (ii) into and out of a facility; and (iii) movement around a facility. Includes proper disposal of ePHI and/or the hardware or Electronic Media on which it is stored, proper media re-use, and two addressable implementation specifications for accountability for the movements of hardware and Electronic Media, and creating a retrievable, exact copy of ePHI, when needed, before movement of equipment. 45 C.F.R. §164.310(d).

c. Technical Safeguards:

i. Access Controls – Implementing technical policies and procedures for ePHI systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Procedures Section 4(a)(3), including unique user identification, emergency access procedures, and two addressable implementation specifications: automatic logoff and encryption/decryption. 45 C.F.R. §164.312(a).

ii. Audit Controls – Implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. 45 C.F.R. §164.312(b).

iii. Integrity – Implementing policies and procedures to ensure data integrity is maintained and ePHI is not changed or destroyed in an unauthorized manner. Includes an addressable implementation specification to use electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. 45 C.F.R. §164.312(c).

iv. Person or Entity Authentication – Implementing procedures to verify that the person or entity seeking access to ePHI is the one claimed before access is granted. 45 C.F.R. §164.312(d).

v. Transmission Security – Implementing technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Includes two addressable implementation specifications: integrity controls and encryption. 45 C.F.R. §164.312(e).

d. Organizational Requirements:

i. Business Associate Contracts or Other Arrangements – Ensuring that the regulatory requirements are included in Watershed business associate agreements or other arrangements. 45 C.F.R. §164.314(a).

ii. Group Health Plans – if the Security Officer also serves as the Security Officer for one or more Group Health Plan(s) sponsored by Watershed, then 45 C.F.R. §164.314(b) specifies requirements for the group health plan(s) and the plan document(s). 45 C.F.R. §164.314(b).

e. Policies and Documentation Requirements:

i. Policies and Procedures – requirements for implementation and modification of reasonable and appropriate HIPAA security policies and procedures. 45 C.F.R. §164.316(a).

ii. Documentation – Requirements for the maintenance of written HIPAA security policies and procedures and written documentation of actions, activities, or assessments required by the Security Rule, including requirements for retaining documents and length of retention, making documentation available, and updating documentation. 45 C.F.R. §164.316(b).

2. The Security Officer oversees and/or performs on-going security monitoring of organization information systems that maintain, create, receive or transmit ePHI.
3. The Security Officer is responsible for directing or conducting periodic risk analyses/assessments as systems or processes involving ePHI change or new ones are added and is responsible for obtaining sign-off from appropriate management for acceptance of residual risks relating to ePHI.
4. The Security Officer will conduct functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with the Security Rule requirements.
5. The Security Officer will oversee and collaborate with the Chief Technology Officer, or designee, to ensure technical testing of the environment to assess general safeguard and control effectiveness, including vulnerability assessments, penetration tests, and evaluating Workforce susceptibility to social engineering and other forms of human deception, is conducted at least annually, or more often, if needed, due to significant changes in organizational information security posture.
6. The Security Officer will evaluate and recommend new information security technologies and counter-measures against threats to information or privacy.
7. The Security Officer ensures ongoing compliance with the HIPAA Security Rule through suitable training/awareness programs and periodic security audits regarding ePHI.

Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	DocuSigned by: Lisa Stanley 9418DCC7CF3D47D...
(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	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Assigned Security Responsibility

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(2)	🟦	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)(2)	🟦	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)(2)	🟪	PR.AT-2: Privileged users understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(2)	🟪	PR.AT-4: Senior executives understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(2)	🟪	PR.AT-5: Physical and information security personnel understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(2)	🟨	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
164.308(a)(2)	🟥	RS.CO-1: Personnel know their roles and order of operations when a response is needed	NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8