POLICY & PROCEDURE **Security Evaluation**		**POLICY #8**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 8 v.9 Security Evaluation	3/1/2014	**5/10/2024**

Purpose

To perform periodic technical and nontechnical evaluations, based initially upon the standards implemented, and subsequently in response to environmental or operational changes affecting the security of Electronic Protected Health Information (ePHI), and to establish the policy and procedures by which Watershed Health, Inc. (Watershed) will perform periodic technical and non-technical evaluations under 45 C.F.R. §164.308(a)(8).

Watershed will continually assess potential risks and vulnerabilities, including individually identifiable health information in its possession, and ensure the confidentiality, integrity, and availability of all electronic information the created, received, maintained, or transmitted as also required at 45 C.F.R. §164.306(a)(1).

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 conduct initial technical and nontechnical evaluations. After the initial evaluations, subsequent periodic ongoing evaluations will be conducted to identify environmental and operational changes affecting the security of ePHI. These operational and environmental changes include, but are not limited to, technology changes, organizational changes, business process changes, and regulatory changes.

At least annually and in response to identified environmental and operational changes affecting the security of ePHI, Watershed will conduct evaluations of its information security safeguards to demonstrate and document compliance with its security policies and procedures, based on the

standards implemented under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The policies and procedures apply to all ePHI that Watershed creates, receives, maintains, or transmits, with specific emphasis on data classifications as described in *Security Policy #22, Data Governance and Data Classification*.

Procedures

1. Procedures for identifying and evaluating environmental or operational changes (known hereinafter as an "evaluation").
    a. On a quarterly basis, Watershed, under the direction of the Security Officer, or designee, will conduct an evaluation to identify any environmental or operational changes to Watershed.
    b. The evaluation may include consideration of the following elements:
        i. Regulatory changes affecting Watershed;
        ii. Information system or technology revisions and deployments;
        iii. Major workforce changes;
        iv. Leadership and/or governance structure alterations;
        v. Business model adjustments;
        vi. Mergers and Acquisitions;
        vii. Policy and procedural modifications not driven by regulatory changes;
        viii. New or changed administrative, physical, or technical safeguards.
    c. The results of annual evaluations will be communicated to Senior Management.
        i. If indicated by the identification of environmental or operational changes, a technical or non-technical evaluation, possibly out-of-annual cycle, as described below will be conducted.
        ii. A Risk Analysis will be reviewed or conducted, as appropriate, in accordance with *Security Policy #1, Security Management Process*.
    d. Where results do not indicate the need for an immediate out-of-cycle evaluation, any environmental or operational change information gathered in the quarterly review will be retained and included in an annual technical evaluation, annual risk analysis, and biennial non-technical evaluation.
2. Procedures for Conducting Non-Technical Evaluations.
    a. An initial non-technical evaluation will examine Watershed's Security Policies and Procedures to determine the extent to which the policies and procedures comply with the requirements of the HIPAA Security Rule. Non-technical evaluations will include inspections, reviews, interviews, workshops, and compliance gap analyses as appropriate.

b. The policies and procedures and other required documentation will be reviewed to establish that documentation is, at a minimum, consistent with each Implementation Specification of the HIPAA Security Rule; all documentation is complete, has been formally approved; and the documentation has been disseminated to the Workforce members responsible for implementing the policies and procedures.

   i. Documentation reviews and interviews will be conducted with appropriate Watershed Workforce members to determine the level of implementation, addressing how well the documented procedures are being communicated, enforced, and practiced.

   ii. Reviews will consider whether the existing practices are reasonable and appropriate to meet Watershed's obligations under the Security Rule, at a minimum. Process steps will include, but not be limited to:

      (1) Review of latest Security Policies and Procedures for correctness and completeness.

      (2) Inspection and analysis of training, incident, and media logs for compliance.

c. An analysis of the results will be prepared and presented to management detailing the current level of compliance across all process steps utilized.

   i. A remediation plan will be developed to resolve all gaps in compliance. The plan will prioritize remediation activities, assign tasks and responsible parties, and establish dates for expected completion.

   ii. The Security Officer or designee will oversee completion of remediation activities, assigning resources as necessary to complete the tasks, and ensure consistent progress to completion.

   iii. The Security Officer or designee will report progress to the Board of Directors as requested.

d. Subsequent Non-Technical Evaluations will be conducted at least bienially utilizing the processes described sections a – c, above, ensuring a repeatable, sustainable practice of evaluation.

e. As identification and evaluation of operational or environmental conditions reviews dictate, the Security Officer or designee will direct additional evaluations to identify the effect of these changes on current policies and procedures.

3. Procedures for Conducting Technical Evaluations.

   a. Watershed will perform technical evaluations annually at a minimum. Technical evaluations will include , vulnerability and penetration testing, security awareness testing, web application testing (as appropriate), and other analysis and verification.

      i. Watershed will perform, or engage a third-party to perform, as appropriate, technical and non-technical evaluations. The initial basis for security requirements will be the HIPAA Security Rule; considerations for any environmental or operational changes will also be included in each evaluation.

ii. In the event the evaluations will be performed by a third-party vendor, Watershed will ensure the vendor meets the professional and ethical requirements commensurate with those of Watershed.

b. The evaluation will include:

i. External Network Vulnerability Assessment and Penetration Testing utilizing scenarios approved by management and Cybersecurity Oversight Committee.

ii. Internal Network Vulnerability and Penetration Testing utilizing scenarios approved by management.

iii. Web Application Testing (as appropriate) utilizing scenarios approved by management.

iv. Other types of tests as appropriate to Watershed's systems and capabilities as determined by the Security Officer, or designee, in consultation with management and other experts.

c. Conducting the evaluations.

i. Preparation

(1) Identify the persons who will be performing the evaluation. Evaluators will be selected based on the security principle of separation of duties to avoid a conflict of interest that could compromise the process. Further, the principle of Least Privilege (constraining individual access to resources to the minimum necessary to perform his/her duties) will be applied in the definition of individual functions. Evaluators will have the appropriate technical skills (with respect to the operating systems and applications) to perform the evaluation correctly.

(2) Identify the Workforce member/role who will be overseeing the evaluation process.

ii. Conduct evaluations

(1) Perform applicable analysis activities as determined during preparation to check the correctness and adequacy of the controls within the network architecture, operating system environments, and applications. Examples of such activities include information flow analyses, access control mechanism adequacy checks, system configuration analyses, and data segregation and labeling examinations.

(2) Perform testing activities as determined during preparation. Such activities should be performed to ensure all technical requirements are adequately fulfilled. Tests to determine the correctness of functionality of security controls, as well as the assurance levels afforded to them may be included. Automated vulnerability scanners, as well as various penetration test scenarios and methods may be employed depending on the scope of the assessment.

d. Procedures for testing and verification.

i. Procedures for security functional testing:

(1) For each component to be tested, identify the security functionality that is expected from the component. Such functionality may include logging capabilities, access control/filtering mechanisms, encryption, integrity checks, and/or other features.

(2) For each function identified, formulate a test case to measure the effectiveness of the component with respect to performing that function.

(3) Conduct the test cases identified, documenting the results.

(4) Make recommendations for and/or implement changes to the system based on deficiencies found.

ii. Procedures for penetration testing:

(1) Qualified penetration testers will not intentionally change, alter, corrupt data, or disrupt any Watershed's system. Any tests that have a reasonable probability of causing a system disruption should be conducted during periods of low usage. The actual exploitation of security vulnerability should not be pursued further than is necessary to confirm that a vulnerability exists.

(2) Identify the targets to be tested.

(3) Perform scanning and probing activities to determine the network topology, the services running on the components, and the operating systems used.

(4) Using the information gathered, attempt to exploit vulnerabilities discovered using any available scripts, tools, or methods. Where applicable, utilize compromised machines to launch further attacks, leveraging any trust relationships that exist.

(5) Document all methodologies, test cases, and results. Make recommendations for and/or implement changes to the system based on deficiencies found.

iii. Follow-up:

(1) Include the evaluation findings as an input into the risk management process.

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)(8) – Standard: Evaluation.

Internal:

1. Security Policy #1, Security Management Process
2. Security Policy #22, Data Governance and Data Classification

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

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
5/15/23	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

Security Evaluation			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.308(a)(8)		ID.AM-3: Organizational communication and data flows are mapped	NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
164.308(a)(8)		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)(8)		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)(8)		ID.BE-5: Resilience requirements to support delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
164.308(a)(8)		ID.RA-1: Asset vulnerabilities are identified and documented	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA- 3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
164.308(a)(8)		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
164.308(a)(8)		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
164.308(a)(8)		PR.IP-3: Configuration change control processes are in place	NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
164.308(a)(8)		PR.IP-7: Protection processes are continuously improved	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR- 8, PL-2, PM-6
164.308(a)(8)		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, IR-8, SI-4
164.308(a)(8)		DE.CM-1: The network is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
164.308(a)(8)		DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 RA-5
164.308(a)(8)		DE.DP-2: Detection activities comply with all applicable requirements	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
164.308(a)(8)		DE.DP-5: Detection processes are continuously improved	NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14
164.308(a)(8)		RC.IM-1: Recovery plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(8)		RC.IM-2: Recovery strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(8)		RS.IM-1: Response plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(8)		RS.IM-2: Response strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

