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

Purpose

To ensure that security violations of Electronic Protected Health Information (ePHI) are prevented, detected, contained, and corrected and provide details of Watershed Health, Inc. (Watershed) responsibilities and procedures related to the Security Management Process.

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

The Watershed Information Security Management Program (ISMP) is based on the NIST CSF framework. As such, Watershed shall (i) consider all the control objectives of the accepted industry framework (including mapping security tools to 405(d) requirements); (ii) document any excluded control objectives of the NIST CSF framework and reasons for exclusion, if applicable; and (iii) update its ISMP annually and/or when there are significant changes in the environment.

Watershed implements an integrated control system characterized using different control types (e.g. layered, preventative, detective, corrective, and compensating) that mitigates identifies risks.

Additionally, Watershed will properly document and implement any Security Management Process actions, activities, and assessments as necessary to comply with Watershed Data Governance Policies and Procedures and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, to include:

a. **Risk Analysis (Required).** Watershed will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of ePHI held by Watershed that (i) addresses all the major objectives of the HITRUST CSF; (ii) are consistent and identify information security risks to Watershed; (iii) are performed at planned intervals and when major changes occur in the environment; and (iv) are reviewed annually.

b. **Risk Management (Required)**. Watershed will implement security risk management measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

c. **Sanctions Policy (Required)**. Watershed will apply appropriate sanctions against Workforce members who fail to comply with Watershed's security policies and procedures or who engage in system misuse, abuse or fraudulent activity.

d. **Information System Activity Review (Required)**. Watershed will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to maintain ongoing understanding of activity in information systems that create, maintain, process, or transmit ePHI.

Procedures

1. **General Rules**

a. Security Officer or designee will direct and manage the Security Management program and operations.

b. Security Officer or designee will maintain an asset inventory of systems and devices, including all hardware and software, as well as the owners of the devices, that are used to create, receive, maintain, collect, store, process, or transmit ePHI and as classified in *Security Policy #22, Data Governance and Data Classification*.

c. Any additions or changes in the inventory should comply with *Security Policy #3, Workforce Security*.

d. Security Officer or designee will annually direct or perform a criticality analysis (Refer to *Security Policy # 7, Contingency Plan*) and determine the value and relative desired assurance levels for each asset identified; consider the levels needed to ensure Confidentiality, Integrity, and Availability; and ensure that ePHI components are identified and included.

e. Cybersecurity Oversight Committee will analyze business functions from time to time and verify ownership and control of information system elements as necessary.

2. **Risk Analysis** - Security Officer or designee will direct or conduct an accurate and thorough assessment of the potential threats and vulnerabilities to the Confidentiality, Integrity, and Availability of systems with ePHI.

    a. A risk analysis shall be annually conducted either by the Security Officer or a qualified external consultant as time and resources permit. The Risk Analysis methodology will meet the guidance recommended by the Office for Civil Rights and documented in the National Institute of Standards and Technology's (NIST) Special Publication 800-30, Revision 1 – Guide for Conducting Risk Assessments.

        i. The risk analysis shall demonstrate, at a minimum, a defined scope that identifies all systems and assets that create, transmit, maintain, or receive ePHI, including the criticality of each asset.

            (1) Watershed will identify all information systems that house ePHI including all assets (e.g., hardware, software, applications, information/data sets, routers, switches) that are used to create, transmit, maintain, or transmit ePHI. The information systems must be identified regardless of whether they are hosted on or off premises with a service provider or a cloud-hosted application.

        ii. Identify the vulnerabilities that these assets may have or be associated with in their day-to-day operations. Watershed will consider technical, administrative/process, and physical vulnerabilities, including vulnerabilities that could impact the Confidentiality, Integrity and Availability of ePHI.

        iii. Identify the threats that could exploit the vulnerabilities identified. Watershed will consider human (intentional and unintentional) and environmental (e.g., weather, air quality) threats, including all known threats that could impact the Confidentiality, Integrity and Availability of ePHI.

        iv. Estimate the likelihood that a threat would successfully exploit each of the identified vulnerabilities and the impact to Watershed business operations if the exploit was successful, given the current safeguards or countermeasures employed to guard against such exploits.

        v. Compute the level of risk presented by each threat and vulnerability. This is accomplished by determining the impact to Watershed (e.g. system outage, loss of worker productivity, sensitive data breach, etc.) if the threat can successfully exploit the vulnerability and multiplying this by the likelihood that the threat can successfully exploit this vulnerability, given the presence and effectiveness of the various administrative, physical, and technical IT security controls currently in place. Both impact and likelihood will be expressed using a 5-point scale, where “1” represents a 'rare' impact and ‘insignificant’ for likelihood, and 5 represents a 'disastrous' impact and an ‘almost certain’ for likelihood.

vi. Identify the level of risk (the risk threshold) associated with the likelihood and impact scenarios acceptable to Watershed. The risk threshold is leveraged to prioritize appropriate risk treatment or response.

vii. Survey the controls and costs of safeguards (technical and administrative). Incorporate safeguards that produce an expected annual cost savings based on the annual loss expectancy or are otherwise necessary to meet the requirements of the HIPAA Security Rule or other mandates. Consider the reasonableness and appropriateness of security controls selected, considering factors specific to the organization (e.g., size, environment, operating changes, and configuration).

b. Watershed will develop a risk action plan that includes:

i. Steps to be taken to reduce the risks above threshold to an acceptable residual level below the threshold;

ii. Risk Owners who are responsible for addressing the risk treatment; and

iii. Governance evaluation and sign-off on risk treatment recommendations.

c. Watershed's Security Officer or designee will ensure all assets, security controls, risk ratings, and vulnerability reports are documented and communicated to senior management for prioritization of resources to resolve any risks that are above the acceptable threshold.

3. **Risk Management** - Watershed will (i) implement security measures sufficient to reduce threats and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. §164.306(a); and (ii) integrate the risk management process with the change management process (Security Policy 25, Configuration and Change Management)

a. Ensure personnel are adequately trained with respect to information security policies and procedures, including relevant threats, vulnerabilities and countermeasures.

b. Leverage the results of information system activity reviews and evaluation programs to identify and address areas of deficiency.

c. Conduct technical evaluations (e.g. vulnerability testing, penetration testing), as applicable.

d. Consider other relevant inputs (e.g., incident trends) and outputs (e.g., contingency plan modifications and security control updates).

e. Security patches identified by the vendor are set up to automatically deploy to all critical instances related to ePHI.

f. Once safeguards or countermeasures have been incorporated based on the outcome of the risk analysis process, identify any residual risk remaining. For the residual risk, analyze the applicable threats, vulnerabilities and controls to determine the potential for a security incident.

g. Based on the probability of occurrence and the value of the applicable asset(s), determine if the residual risk is acceptable. If it is not, continue assessing control options, including processes, technologies, and approaches to reduce the risk to an acceptable level.

h. Base security controls and residual risk tolerance on factors specific to Watershed (e.g., data sensitivity, organizational size, IT environment, operating changes, and configuration). Formulate a scale for determining "reasonable and appropriate" for Watershed. Ensure Confidentiality, Integrity and Availability are considered.

4. **Sanctions.** Watershed will apply appropriate sanctions against members of its Workforce who fail to comply with Watershed's policies and procedures or engage in system misuse, abuse, or fraudulent activity.

5. **No Sanctions Based on Whistleblowing or Complaints**. Refer to *Privacy Policy #6, Reporting Violations, Mitigation, and Sanctions*.

6. **Information System Activity Review** - Watershed will implement procedures to review monthly records of information system activity, such as audit logs, access reports, and security incident tracking reports.

   a. Preparation for activity reviews

      i. The Security Officer or designee is responsible for oversight of the conduct of regular reviews of Watershed's information system activities.

      ii. Necessary safeguards to protect the Confidentiality, Availability and Integrity of audit trails and information system activity review reports will be implemented. Such safeguards may be provided by the information system components (e.g., password-protected access to audit logs, file integrity checkers), as well as by organization-defined processes (e.g., regularly backed up audit logs, which, if applicable, are stored in fire-resistant, offsite, locked containers).

      iii. Audit logs that demonstrate a Security Event to be investigated will be retained as part of the investigation documentation and will be retained a minimum of six years from the date the investigation is completed. Audit logs that do not result in Security Events will be securely disposed of once the review has been documented in the system activity review log and is no longer needed.

      iv. To the degree possible, automated processes will be used to identify anomalies or unusual activity. Checks to be performed to assess the Integrity and/or correctness of the individual information processed, created, transmitted and/or stored or maintained by the information systems must be identified, documented and implemented, including:

         (1) Failed and successful login attempts;

         (2) Changes to files and databases;

(3) Incidents or unusual system occurrences; and

(4) System activity by internal and external users.

b. Conducting activity reviews

i. For each component identified above, when audit log alerts trigger notification of a potential event, the Watershed 911 Zoom Group will be activated.

ii. All significant findings are recorded using Watershed's YouTrack application for tracking issues.

iii. Review findings and recommendations are presented to the appropriate management of Watershed.

iv. Documentation, notes, and findings are maintained in YouTrack.

c. Follow-up actions

i. Adjustments to the administrative, physical, and technical safeguards will be made as necessary based on the review findings.

ii. Findings and recommendations will be incorporated into Watershed's security training program as appropriate.

iii. Review findings will be included 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

<u>Regulatory Authority:</u>

1. 45 C.F.R. §164.308(a)(1) – Standard: Security management process.

2. 45 C.F.R. §164.308(a)(1)(ii)(A) – Risk analysis (Required).

3. 45 C.F.R. §164.308(a)(1)(ii)(B) – Risk management (Required).
4. 45 C.F.R. §164.308(a)(1)(ii)(C) – Sanction policy (Required).
5. 45 C.F.R. §164.308(a)(1)(ii)(D) – Information security activity review (Required).

Internal:

1. Security Policy #3, Workforce Security
2. Security Policy #6, Security Incidents
3. Security Policy # 7, Contingency Plan
4. Security Policy #22, Data Governance and Data Classification
5. Risk Analysis
6. Risk Action Plan

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
5/4/2023	Nicole Montagnet	9.0	Reviewed and updated by Privacy & Security Officer
5/10/2024	Nicole Montagnet	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Security Management Process:
Risk Analysis, Risk Management, Sanctions, & Information System Activity Review

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(1)(ii)(A)		ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8
164.308(a)(1)(ii)(A)		ID.AM-2: Software platforms and applications within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8
164.308(a)(1)(ii)(A)		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)(1)(ii)(A)		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)(1)(ii)(A)		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)(1)(ii)(B)		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)(1)(i)		ID.GV-1: Organizational information security policy is established	NIST SP 800-53 Rev. 4 PM-1, PS-7
164.308(a)(1)(i)		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		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)
164.308(a)(1)		ID.GV-4: Governance and risk management processes address cybersecurity risks	NIST SP 800-53 Rev. 4 PM-9, PM-11
164.308(a)(1)(ii)(A)		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

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
No direct analog to HIPAA Security Rule	🟦	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
164.308(a)(1)(ii)(A)	🟦	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)(1)(ii)(D)	🟦	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)(1)(i)	🟦	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)(1)(ii)	🟦	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
164.308(a)(1)(ii)(B)	🟦	ID.RA-6: Risk responses are identified and prioritized	NIST SP 800-53 Rev. 4 PM-4, PM-9
164.308(a)(1)(ii)(B)	🟦	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	NIST SP 800-53 Rev. 4 PM-9
164.308(a)(1)(ii)(B)	🟦	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	NIST SP 800-53 Rev. 4 PM-9
164.308(a)(1)(ii)(B)	🟦	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
164.308(a)(1)(ii)(B)	🟪	PR.AC-2: Physical access to assets is managed and protected	NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
164.308(a)(1)(ii)(D)	🟪	PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.308(a)(1)(ii)(A)	🟪	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
164.308(a)(1)(ii)	🟪	PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
164.308(a)(1)(ii)(D)	🟪	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)(1)(ii)(D)	🟪	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	NIST SP 800-53 Rev. 4 SI-7

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(1)(ii)(C)	🟪	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	NIST SP 800-53 Rev. 4 PS Family
164.308(a)(1)	🟪	PR.IP-12: A vulnerability management plan is developed and implemented	NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
164.308(a)(1)(i)	🟪	PR.IP-2: A System Development Life Cycle to manage systems is implemented	NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA- 10, SA-11, SA-12, SA-15, SA-17, PL-8
164.308(a)(1)(ii)(D)	🟪	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	NIST SP 800-53 Rev. 4 MA-4
164.308(a)(1)(ii)(D)	🟪	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	NIST SP 800-53 Rev. 4 AU Family
164.308(a)(1)(ii)(D)	🟪	PR.PT-4: Communications and control networks are protected	NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
164.308(a)(1)(ii)(D)	🟨	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI- 4
164.308(a)(1)(ii)(D)	🟨	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)(1)(ii)(D)	🟨	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)(1)(ii)(D)	🟨	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
164.308(a)(1)(ii)(D)	🟨	DE.CM-4: Malicious code is detected	NIST SP 800-53 Rev. 4 SI-3
164.308(a)(1)(ii)(D)	🟨	DE.CM-5: Unauthorized mobile code is detected	NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
164.308(a)(1)(ii)(D)	🟨	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA- 9, SI-4
164.308(a)(1)(ii)(D)	🟨	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
164.308(a)(1)(i)	🟨	DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 RA-5

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(1)(i)	🟨	DE.DP-2: Detection activities comply with all applicable requirements	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
164.306(e)	🟨	DE.DP-3: Detection processes are tested	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM- 14, SI-3, SI-4
164.308(a)(1)	🟥	RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4
164.308(a)(1)(ii)(A)	🟥	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
164.308(a)(1)(ii)(B)	🟥	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5