POLICY & PROCEDURE **Workforce Security**		**POLICY #3**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy 3 v.9.0 Workforce Security	3/1/2014	**5/10/2024**

Purpose

Watershed Health, Inc. (Watershed) will maintain formal Workforce Security procedures to ensure that all Workforce members have appropriate levels of access to electronic Protected Health Information (ePHI) and to prevent Workforce members who do not require access from obtaining access.

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 implement procedures to ensure that all Workforce members have appropriate access to ePHI and to prevent Workforce members who do not require access from obtaining access to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, to include:

a. **Authorization and/or Supervision (Addressable).** Watershed will ensure appropriate authorization of and/or supervision of Workforce members who work with ePHI or who work in locations where it might be accessed.

b. **Workforce Clearance Procedure (Addressable).** Watershed will ensure that Workforce member access to ePHI is appropriate.

c. **Termination Procedures (Addressable**). Watershed will terminate access to ePHI when the employment of, or other arrangement with a Workforce member ends, or if it has been determined that a Workforce member’s access to ePHI is no longer appropriate or needed in their current role.

Procedures

1. Authorization and/or Supervision.
    a. Authorization
        i. When defining a new or changed position, the Human Resources Department, in consultation with the Security Officer, Privacy Officer, system owner, and other appropriate individuals, will assign access based on job descriptions.
        ii. *Privacy Policy #30, Minimum Necessary Uses, Disclosures, and Requests*; and *Security Policy #22, Data Governance and Data Classification*, set the minimum necessary standard for access to ePHI .
    b. Supervision
        i. Supervisors/Managers having responsibility over areas in which ePHI is accessed will enforce procedures to limit access to Workforce members with valid access rights.
            (1) Supervisors/Managers will consider the principles of least privilege, need-to-know, minimum necessary, and separation of duties in making recommendations that identify the level of security responsibility and amount of supervision required for a role.
            (2) Access authorization and modifications should comply with *Security Policy #4, Information Access Management*.
        ii. Non-Workforce access.
            (1) Should a Subcontractor or Vendor require access to Watershed’s systems or applications, Watershed will ensure that any access requires a separate user account for each individual. The account must be subject to the minimum necessary standards and prevent the use of any cached passwords to access Watershed’s systems or applications.
2. Workforce Clearance Procedure.
    a. Watershed’s Human Resources Department will review the background of all Watershed’s Workforce members before hiring. Verification checks must be made, as appropriate, that are relevant to the level of access required for the job position. Verification checks include criminal background check and social security checks as well as any other contractual obligations as required.
    b. If job candidates are provided via an agency, Watershed’s contract with each agency must clearly state the agency’s responsibilities for reviewing the candidates’ backgrounds.

   c. If the services of a third-party or agency are used, the third-party or agency must certify in writing (e.g., contract provisions) that they comply with the minimum verification check requirements outlined in Section 2.a. above.

   d. Workforce members being considered for a change in access levels providing elevated access to ePHI are subject to any additional background checks, as applicable to any legal or regulatory requirements. All required checks must be performed before elevated access is provided.

3. Termination Procedures.

   a. Supervisors/Managers who become aware of the impending departure of a Workforce member, or aware that access to ePHI is no longer needed for a specific Workforce member, will immediately notify both Human Resources and the Security Officer or Designee.

      i. The Security Officer or designee, upon receipt of the notification, will update the inventory accordingly.

   b. Physical Property.

      i. Upon notification of a Workforce member's termination by the Human Resources Department, the terminated individual's Supervisor/Manager will ensure that all previously issued software, corporate documents, company equipment, and all other organizational materials, such as mobile computing devices, credit cards, keys, access cards, tokens, manuals and information stored on electronic media are collected, and that the Security Officer or designee and the Human Resources Department are notified that the objects have been returned.

         (1) The Human Resources Department and Security Officer or Designee, upon confirmation of the collection from the Supervisor/Manager, will update their respective inventories accordingly.

      ii. Should all the distributed objects not be collected in a timely manner, the Security Officer or designee will take the appropriate steps to ensure the security of components associated with the objects (e.g., freeze or remote wipe of laptops and mobile phones, network/account access termination, rekeying locks, disabling access card/tokens, etc.).

   c. System or Information Access.

      i. The Human Resources Department or Security Officer or designee will communicate with the appropriate system owner regarding any changes or terminations of a Workforce members access to systems and applications.

      ii. Appropriate system owners will notify the Human Resources Department and Security Officer or designee when the change/termination is completed using the Termination Checklist.

(1) The Security Officer or Designee, upon receipt of a change/termination confirmation from the appropriate system owner, will update the inventory accordingly.

iii. In no event shall terminating login credentials extend beyond 5:00 p.m. local time of the day of the Workforce member's departure, unless an exception has been granted by the Security Officer or designee, which exception may extend such termination until midnight of the day of termination.

iv. When possible, the Supervisor/Manager will obtain written attestation from the individual that they have removed or destroyed all Watershed ePHI from all personal devices.

4. Responsibilities

   a. Watershed's Security Officer, or designee, in coordination with Human Resources and the hiring Supervisor/Manager, must identify the security responsibilities and level of supervision required for each role within Watershed in order to assign an appropriate level of access for each role. The Security Officer or designee will designate specific individuals to perform the functions associated with establishing or removing system access as described in the procedures.

   b. The Security Officer, or designee, may perform periodic reviews of the security measures that Workforce members have implemented on their devices to verify that the requirements laid out in this policy and procedures, and *Security Policy #21, Mobile Device Security*, have been instituted in a timely manner.

   c. The Security Officer or designee in coordination with Human Resources, will ensure that all Workforce members who have access to ePHI are properly trained and sign the employee confidentiality agreement and assignment of rights.

   d. The asset inventory of systems and devices maintained by the Security Officer or designee shall include, as applicable, the elements listed on *Appendix 1: Elements of Asset and System Inventory.*

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)(3)(i) – Standard: Workforce Security.
2. 45 C.F.R. §164.308(a)(3)(ii)(A) – Implementation Specification: Authorization and/or Supervision (Addressable).
3. 45 C.F.R. §164.308(a)(3)(ii)(B) – Implementation Specification: Workforce Clearance Procedure (Addressable).
4. 45 C.F.R. §164.308(a)(3)(ii)(C) – Implementation Specification: Termination Procedures (Addressable).

Internal:

1. Security Policy #4, Information Access Management
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

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: Elements of Asset and System Inventory

The asset inventories include, as applicable:

1. type or classification of the asset;
2. format of the asset;
3. location of the asset;
4. backup information of the asset;
5. license information of the asset;
6. a business value of the asset; and
7. data on whether the device is a portable and/or personal device.

The asset inventory record

8. is used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department.

The asset inventory records:

9. the network addresses;
10. the machine name(s);
11. the purpose of each system;
12. an asset owner responsible for each device; and
13. the department associated with each device.

The inventory

14. does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned.

Records of property assigned to employees

15. is reviewed and updated annually.

The asset inventory includes the:

1. unique identifier and/or serial number of the IT asset;
2. information system of which the component is a part;
3. type of information system component (e.g., server, desktop, application);
4. manufacturer/model information of the IT asset;
5. operating system type and version/service pack level of the IT asset;
6. presence of virtual machines;
7. application software version/license information;
8. physical location (e.g., building/room number) of the IT asset;
9. logical location (e.g., IP address, position with the IS architecture) of the IT asset;
10. Media access control (MAC) address of the IT asset;
11. data ownership and custodian by position and role;
12. operational status of the IT asset;
13. primary and secondary administrators of the IT asset; and
14. primary user of the IT asset.

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

Workforce Security: Authorization and/or Supervision, Workforce Clearance Procedure, & Termination Procedures

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(3)(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)(3)	🟦	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)(3)	🟦	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)(3)	🟦	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)(3)(ii)	🟪	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)(3)	🟪	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)(3)(i)	🟪	PR.AT-2: Privileged users understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(3)(i)	🟪	PR.AT-4: Senior executives understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(3)(i)	🟪	PR.AT-5: Physical and information security personnel understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(3)	🟪	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)(3)	🟪	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)(3)(ii)(A)	🟪	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(3)(ii)(A)	🟪	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)(3)	🟪	PR.PT-2: Removable media is protected and its use restricted according to policy	NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
164.308(a)(3)	🟪	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)(3)(ii)(A)	🟨	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)(3)(ii)	🟨	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