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

Purpose

To implement a security awareness and training program for all members Watershed Workforce, including those who use and disclose Electronic Protected Health Information (ePHI) in the performance of their job functions.

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's Security Officer or designee will ensure that security awareness and training is provided to Workforce members, as well as agents, and contractors, if necessary, for awareness of security concerns and initiatives, including:

a. **Security reminders (Addressable**). Periodic security updates.

b. **Protection from malicious software (Addressable)**. Procedures for guarding against, detecting, and reporting malicious software.

c. **Log-in monitoring (Addressable)**. Procedures for monitoring log-in attempts and reporting discrepancies.

d. **Password management (Addressable)**. Procedures for creating, changing, and safeguarding passwords.

e. **Teleworking**. Procedures and updates for establishing and maintaining a compliant telework environment.

Procedures

1. Security Awareness Training.
   a. Security Awareness Training will be based on Watershed's policies and procedures and will be completed annually by each Workforce member. Supervisors/Managers are responsible for providing any additional training specific to the Workforce member's job responsibilities and daily tasks not covered in the Security Awareness Training. The Security Officer or designee will provide guidance on additional training, as necessary.
   b. Security Awareness Training will include applicable information regarding the following:
      i. Overall discussion of threats and vulnerabilities specific to ePHI;
      ii. Information access control;
      iii. Access authorization levels;
      iv. Incident reporting;
      v. Viruses and other forms of malicious software;
      vi. User log-in monitoring;
      vii. Password requirements and maintenance;
      viii. Social engineering awareness and recognition;
      ix. Organizational privacy and security policies and procedures, and the sanctions; and
      x. Civil and criminal penalties prescribed for wrongful actions.
   c. Incident reporting education will include applicable information regarding the following:
      i. Symptoms of an incident;
      ii. Persons to notify immediately in the event of a suspected incident;
      iii. Emphasis on not disclosing the incident to persons without a need-to-know; and
      iv. Any applicable steps to contain the incident.
2. Periodic security reminders, in addition to Security Awareness Training, will be distributed by the Security Officer or designee to all Workforce members, or when any of the following events occur:
   a. Revisions to Watershed's information security policies or procedures;
   b. New information security controls implemented at Watershed;

c. Significant changes made to Watershed's information security controls;
d. Changes to Watershed's information security, legal, or business responsibilities;
e. New threats or risks that arise against Watershed's information systems or data;
f. Changes to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule; or
g. As directed by Watershed's Chief Executive Officer (CEO) or other senior member of management.

3. Watershed will install and update on a regular basis the appropriate software and hardware to protect its ePHI information systems from malicious software. Education to protect from malicious software (viruses, Trojan horses, ransomware and similar disruptive processes) will include:
    a. Potential harm that can be caused by malicious software;
    b. Signs that malicious software may have infected a system, such as:
        i. Unexplained file changes (e.g., content, size, or location);
        ii. New (unrecognized) files;
        iii. Irregular consumption of system resources (e.g., disk drive space or CPU cycles);
        iv. Significantly slower system performance; and
        v. Messages received that may indicate a ransomware attack.
    c. Basic prevention strategies, including:
        i. Not opening files or attachments that are unrecognized;
        ii. Not visiting websites that are unauthorized;
        iii. Not uploading software except as approved by the Security Officer; and
        iv. Not introducing USB drives or other external media, except as approved by the Security Officer.
    d. What to do if malicious software or processes are suspected:
        i. Methods and steps for reporting suspected malicious software; and
        ii. Approved steps to contain the infection.
    e. Watershed will implement software to monitor for malicious software.
4. Watershed will monitor log-in activity in the ePHI information systems to identify discrepancies in the login process on such systems and unauthorized access or use of ePHI.
5. Workforce members will receive Password Management education to include:

a. Rules to be following in creating and changing passwords, including password adequacy (e.g., length, complexity) and frequency considerations;

b. Importance of keeping passwords confidential, to include not disclosing passwords to others, storage and protection requirements, and not using passwords in any automated log-on process;

c. Ensuring that Watershed's Network/Software Administrators utilize strong password capability; and

d. Password expiry must never be set to "never expire."

e. Refer to *Security Policy #17, Person or Entity Authentication*, for additional information.

6. Workforce members will receive Social engineering education to include:

   a. Emphasis on adhering first to all published policies and procedures, despite claims by persons that they should do otherwise;

   b. Emphasis on reporting suspected phishing attempts;

   c. Emphasis on the practice of verifying an official's identity, position, and/or authority prior to taking direction from that person with respect to security measures; and

   d. A sampling of common "social engineering" measures and countermeasures to prevent attacks such as:

      i. Phishing;

      ii. Spear phishing; or

      iii. Vishing.

7. Workforce members will receive teleworking education to include:
   a. Location of workstation in rooms with doors and windows that are locked when unattended; and
   b. Prohibition of workstation in areas that are unattended and/or have unrestricted access by the public.

8. Responsibilities.

   a. Watershed's Security Officer or designee is responsible for the development or sourcing of Security Awareness Training.

   b. The Security Officer or designee will be responsible for delivery and maintenance of records of all training events and attendance or completion (based on the method of delivery).

      i. A copy of the completed training for all Workforce members shall be retained in an approved location.

ii. The Security Officer or designee will update the Workforce as needed with HIPAA reminders, Security Reviews, the HIPAA Compliance Officers' Contact Information, and any other applicable and informative Security Training materials.

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)(5)(i) – Standard: Security awareness and training.
2. 45 C.F.R. §164.308(a)(5)(ii)(A) – Security Reminders.
3. 45 C.F.R. §164.308(a)(5)(ii)(B) – Protection from Malicious Software.
4. 45 C.F.R. §164.308(a)(5)(ii)(C) – Log-in Monitoring.
5. 45 C.F.R. §164.308(a)(5)(ii)(D) – Password Management.

Internal:

1. Security Policy # 1, Security Management Process
2. Security Policy #6, Security Incidents
3. Security Policy #17, Person or Entity Authentication

External:

1. Current Administrative Simplification Regulations
2. 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
5/10/24	Nicole Montagnet	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Security Awareness and Training:
Security Reminders, Protection from Malicious Software, Log-in Monitoring, & Password Management

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(5)(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)(5)		PR.AT-1: All users are informed and trained	NIST SP 800-53 Rev. 4 AT-2, PM-13
164.308(a)(5)		PR.AT-2: Privileged users understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(5)		PR.AT-4: Senior executives understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(5) 164.530(b)(1)		PR.AT-5: Physical and information security personnel understand roles & responsibilities	NIST SP 800-53 Rev. 4 AT-3, PM-13
164.308(a)(5)(ii)(C)		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)(5)(ii)		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)(5)(ii)		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)(5)(ii)(C)		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)(5)(ii)(B)		DE.CM-4: Malicious code is detected	NIST SP 800-53 Rev. 4 SI-3
164.308(a)(5)(ii)(B)		DE.CM-5: Unauthorized mobile code is detected	NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
164.308(a)(5)(ii)		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)(5)(ii)		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)(5)(ii)		RS.CO-2: Events are reported consistent with established criteria	NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(5)(ii)		RS.CO-3: Information is shared consistent with response plans	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR- 4, IR-8, PE-6, RA-5, SI-4

