POLICY & PROCEDURE **Person or Entity Authentication**		**POLICY #17**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 17 v.9 Person or Entity Authentication	3/1/2014	**5/10/2024**

Purpose

To verify that an individual or entity seeking access to electronic Protected Health Information (ePHI) is the one claimed in accordance with 45 C.F.R. §164.312(d).

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 Health, Inc. (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

It is the policy of Watershed to utilize the following entity authentication mechanisms to corroborate the identity of an individual or entity:

a. Biometric Identification

b. Passwords

Procedures

1. General Authentication Procedures.

   a. Implement a security control or combination of controls outlined in Section 2 below, as feasible and appropriate, to authenticate individuals and/or entities.

   b. The authentication control(s) must support the level of assurance needed as outlined in *Security Policy #22, Data Governance and Data Classification*.

   c. Employ multi-factor authentication, where feasible.

2. Implementation-specific procedures will be dependent on the data classification and the technical capabilities of the devices used to access ePHI. Workforce members should use the highest level of authentication permitted by the device, system, or application. The primary methods of authentication deployed are:

   a. **Biometric Identification** procedures for identifying a person from a measurement of a physical feature or repeatable action.

   b. **Password** procedures:

      i. System Administrators will configure the systems or applications to enforce the password policies.

      ii. Default passwords shall be changed immediately on all devices, systems, and applications.

      iii. All Workforce members must select quality passwords and take measures to keep their password confidential, avoid keeping a record of passwords, protect their passwords ensuring they are securely stored in an approved method of storage, and not disclosing them to others for any reason.

         (1) In the event the password is suspected to be **compromised**, Workforce members are required to change their password and must immediately report such occurrence to their Supervisor/Manager and the Security Officer or designee. The Workforce member will use the automated password reset functionality of the system or application to reset the password.

         (2) In the event the password is **forgotten**, the Workforce member will use the automated password reset functionality of the system or application to reset the password.

         (3) If the Workforce member is unable to use the automated password reset functionality, they should contact the appropriate Help Desk or System Administrator.

         (4) The Workforce member should not reuse the same password and will not use the same password for business and non-buiness purposes.

      iv. Files containing passwords should be limited to a least-privilege and need-to-know basis (usually to only the System Administrator) and should be encrypted in accordance with *Security Policy #22, Data Governance and Data Classification*.

      v. Password Management. Within any specific computing environment, application or processing platform, the ability of general Users to access the files containing passwords should be limited. Access of password files by Users will be monitored for unauthorized activity where possible. When possible, the password file is encrypted to make the passwords unreadable to anyone who possesses the file.

         (1) At a minimum, the following items are implemented within the Watershed applications and processing platforms:

            (a) All users require a unique user ID and are not allowed to share user accounts and respective passwords.

(b) Passwords are a minimum of 8 characters in length.

(c) Passwords automatically expire every 90 days.

(d) Passwords contain both upper- and lower-case characters (e.g., a-z, A-Z) and at least one numeric or special character.

(e) When new institution or users are brought on-line, passwords are uniquely set prior to logging in the system.

(f) Null passwords are not allowed.

(g) The user's past 6 passwords are remembered and not available for use within a given application.

(h) User accounts are disabled after 5 invalid login attempts and reset themselves after 5 minutes or when manually reset.

(i) Application timeouts is invoked after 15 minutes of inactivity and is password protected.

(j) All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) are changed on an annual basis or as needed when individuals with administration privileges leave Watershed or no longer require access.

vi. Passwords are set to expire every 90 days on the information system(s) Watershed is responsible for administering (e.g., Watershed software application).

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. §164.312(d) – Standard: Person or entity authentication.

Internal:

1. Security Policy #22, Data Governance and Data Classification

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
5/15/2023	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

Person or Entity Authentication

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.312(e)	🟦	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
164.312(d)	🟪	PR.AC-1: Identities and credentials are managed for authorized devices and users	NIST SP 800-53 Rev. 4 AC-2, IA Family
164.312(e)	🟪	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7
164.312(d)	🟪	PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.312(e)	🟪	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
164.312(d) & (e)	🟪	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
164.312(e)	🟪	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
164.312(d) & (e)	🟨	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