POLICY & PROCEDURE **Access Control**		**POLICY #14**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Security Policy & Procedure 14 v.9 Access Control	3/1/2014	**5/10/2024**

Purpose

To implement technical policies and procedures for information systems that maintain electronic Protected Health Information (ePHI) to allow access only to those Workforce members or software programs that have been granted access rights. This policy and procedure includes details of Watershed Health, Inc. (Watershed) responsibilities in accordance with the Access Control Standard at 45 C.F.R. §164.312(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

This policy implements technical standards for information systems that maintain ePHI to allow access only to those Workforce members or software programs that have been granted access rights.

a. **Unique user identification (Required)**. Assign a unique name and/or number for identifying and tracking user identity.

b. **Emergency access procedure (Required)**. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

c. **Automatic logoff (Addressable)**. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

d. **Encryption and decryption (Addressable)**. Implement a mechanism to encrypt and decrypt ePHI.

Procedures

1. General Procedures.
    a. Access for Workforce members will only be given to those that have been granted access rights as specified by *Security Policy #4, Information Access Management*.
    b. Only authorized Workforce members will access ePHI, including the hardware and/or software on which the ePHI is stored, according to *Security Policy #3, Workforce Security.*
    c. Watershed's System or Application Owners must ensure that new or modified software development and implementation incorporates sufficient controls to limit access to ePHI to only those Workforce members that have been granted access rights.
        i. Configure access controls on all systems processing ePHI to regulate access based on Supervisor/Manager approved authorizations (in accordance with *Security Policy #4, Information Access Management*).
        ii. Configure the system to only allow privileges to access control settings.
        iii. Verify that access permissions are set correctly and functioning properly when any modifications are made to the Authorized User lists.
        iv. Compare access permission settings with authorizations for correctness and attempt authorized and non-authorized actions on behalf of a given user or process to ensure proper function.
2. Procedures for Unique User Identification.
    a. Watershed's information systems must grant Users access via unique identifiers that identify Workforce members or other Users and allows activities performed on information systems to be traced back to a particular individual through tracking of unique identifiers. Unique identifiers must not give any indication of the privilege level.
    b. Group user identifiers must not be used to gain access to Watershed's information systems that contain ePHI. When unique user identifiers are insufficient or inappropriate, group identifiers may be used only to gain access to Watershed's information systems that do not contain ePHI.
    c. Assign each User having access to ePHI a unique username and/or number.
    d. Use a standard convention for assigning unique user identifiers.
        i. For Users having access to multiple systems within the organization, employ the same unique user identifiers wherever possible.
    e. Maintain a protected record of name and/or number assignments.
    f. Configure computers to track User activity, recording the events as dictated by Watershed's security policy.

3. Emergency Access Procedures.
    a. The Security Officer or designee is responsible for coordinating technical emergency access procedures with the Contingency and Disaster Recovery Plan (CDRP) to address how Watershed will ensure technical mechanisms are defined to access ePHI while operating in an emergency mode.
        i. Watershed's formal emergency access procedure enabling authorized Workforce members to obtain required ePHI during an emergency is documented in *Security Policy #7.*
        ii. Should the emergency access procedures require facility access, such access will be in line with *Security Policy #10, Facility Access Control* as applicable.
4. Automatic Logoff Procedures
    a. Information systems (including operating systems and application information systems) that contain or can access sensitive data must be automatically locked or the electronic session must be automatically terminated after a maximum of 60 minutes of inactivity.
    b. Automatic session termination capabilities provided by commercial operating systems typically lock a terminal or Workstation/laptop (requiring re-authentication) rather than completely ending a user's session. Each terminal or Workstation/laptop should be configured to automatically terminate an electronic session after 20 minutes of inactivity.
    c. To restart a session following a period of inactivity, users must re-enter the password (and/or other authentication mechanisms as required) when prompted.
5. Encryption and Decryption Procedures.
    a. Where necessary, appropriate encryption must be used to protect the confidentiality of ePHI contained on Watershed's information systems or applications. At a minimum, Watershed's risk analysis must consider the following factors when determining whether specific ePHI must be encrypted:
        i. The risks to the ePHI;
        ii. The expected impact to Watershed functionality and workflow if the ePHI is encrypted; and
        iii. Alternative methods available to protect the confidentiality, integrity, and availability of the ePHI.
    b. All encryption technologies used to protect the confidentiality of ePHI contained on Watershed's information systems or applications, as applicable, must meet the guidelines set forth by the Cybersecurity Oversight Committee. Watershed must protect all cryptographic keys against modification and destruction; secret and private keys must be protected against unauthorized disclosure.
    c. Watershed must have a formal process (i.e., AWS KMS) for managing the cryptographic keys used to encrypt ePHI on Watershed's information systems. This process includes procedures for:

i. Generating keys for different cryptographic systems;

ii. Distributing keys to intended users and then activating them;

iii. Enabling authorized users to access stored keys;

iv. Changing and updating keys;

v. Revoking keys;

vi. Archiving keys; and

vii. Appropriate logging and auditing of cryptographic key management.

d. When possible, Watershed's cryptographic keys must have defined activation and deactivation dates.

6. Workforce members will be trained on the procedures to ensure their Workstation is electronically secure from unauthorized access.

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(a)(1) – Standard: Access control.
2. 45 C.F.R. §164.312(a)(2) – Implementation specifications.
3. 45 C.F.R. §164.312(a)(2)(i) – Unique user identification (Required).
4. 45 C.F.R. §164.312(a)(2)(ii) – Emergency access procedure (Required).
5. 45 C.F.R. §164.312(a)(2)(iii) – Automatic logoff (Addressable).
6. 45 C.F.R. §164.312(a)(2)(iv) – Encryption and decryption (Addressable).

Internal:

1. Security Policy #3, Workforce Security

2. Security Policy #4, Information Access Management
3. Security Policy #7, Contingency Plan
4. Security Policy #10, Facility Access Controls

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 9418DCC7CE3D47D...
(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

Access Controls: Unique User Identification, Emergency Access Procedures, Automatic Logoff, & Encryption and Decryption			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.312(a)(2)(ii)		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
164.312(a)(2)(ii)		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
164.312		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)
164.312(a)(1)		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
164.312(a)(1)		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(a)(2)		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(a)(1) & (2)		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
164.312(a)(1)		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7
164.312(a)(1) & (2)(iii) & (iv)		PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.312(a)(2)(ii)		PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
164.312(a)		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(a)(2)(ii)		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	NIST SP 800-53 Rev. 4 CP-2, IR-8

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.312(a) & (a)(2)(ii) & (iv)		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(a)(1) & (2)(iv)		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
164.312(a)(1) & (2)		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
164.312(a)(1)		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(a)(2)(i)		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
164.312(a)(1) & (2)(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
164.312(a)(2)(ii)		RS.CO-1: Personnel know their roles and order of operations when a response is needed	NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
164.312(a)(2)(ii)		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.312(a)(2)(ii)		RS.RP-1: Response plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR- 8

