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

Purpose

Watershed is a remote workforce and is no longer relying on a physical work environment. Should Watershed return to a physical work environment, this policy shall serve to limit physical access to its information systems, applications, and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed. Watershed will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. As such, Watershed will continually assess potential risks and vulnerabilities to electronic Protected Health Information (ePHI) and Protected Health Information (PHI) in its possession, and develop, implement, and maintain appropriate physical security measures. This policy and these procedures include details of Watershed's responsibilities in accordance with 45 C.F.R. §164.310(a)(1), the Facility Access Controls Standard.

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 and these procedures describe how Watershed will limit physical access to its ePHI systems and applications or PHI and the facility or facilities in which they may be housed, of which Watershed has control, while ensuring that properly authorized access is allowed.

a. **Contingency operations (Addressable)**. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

b. **Facility security plan (Addressable)**. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

c. **Access control and validation procedures (Addressable)**. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

d. **Maintenance records (Addressable)**. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Procedures

1. The policies and procedures stated herein (i) apply to all ePHI/PHI maintained or transmitted by Watershed from a physical work environment; (ii) are available to all Workforce members via the staff website; and (iii) are reviewed and updated (as needed) at least annually
2. Contingency Operations.
    a. The Security Officer or designee will ensure, in the event of a loss of ePHI/PHI due to a disaster or emergency, Watershed's designated personnel can enter its facilities to take the necessary actions defined in the Contingency and Disaster Recovery Plan (CDRP).
    b. The Security Officer or designee will:
        i. Determine those Workforce members who need facility access in the event of a disaster or emergency;
        ii. Document roles and responsibilities;
        iii. Document the processes to be followed to ensure continuation of business processes to protect the security of ePHI/PHI and the restoration of lost data;
        iv. Determine a backup authentication scheme to regulate facility access in the event of a disaster or emergency;
        v. Consider emergency communications means to ensure authorized access is gained in the event an obstacle is encountered; and
        vi. Ensure any modifications to physical security controls, of which Watershed has control, are carried out by authorized Workforce members.
    c. The Security Officer will coordinate these procedures with *Security Policy #7, Contingency Plan*, and Watershed's CDRP.
        i. The Facility Security Plan should be incorporated into the overall CDRP for safeguarding facilities and premises from unauthorized physical access, tampering, or theft, including the equipment contained therein, of which Watershed has control. The Security Officer or designee is responsible for ensuring this plan is in place and provides suitable protection for ePHI/PHI.
    d. Should any system or application containing ePHI pertaining to Watershed be hosted externally, the Security Officer or designee will obtain assurances, where practical, from the vendor

regarding its contingency operations and incorporate this into the overall CDRP. It is important to note that not all vendors will readily provide this information for security purposes to an external organization.

3. Facility Security Plan.

   a. The Security Officer or designee will coordinate with each department operating information systems or applications containing ePHI to document an inventory and facility plan for those departments or areas. At a minimum, documentation must identify:

      i. The information systems or applications to be protected from unauthorized physical access, tampering, and theft;

      ii. The processes and physical controls used to protect the information systems or applications;

      iii. The actions to be taken if unauthorized access, tampering or theft is attempted or suspected;

      iv. Responsibilities of the Workforce for reporting attempted access, tampering, or theft; and

      v. A schedule that specifies how and when physical controls and responses will be tested, for those systems and applications under Watershed's control.

   b. The Security Officer or designee will coordinate with Facility Management Personnel to ensure procedures for safeguarding the interior of premises and buildings include:

      i. All doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices;

      ii. Doors and windows lock by default, and additional security measures are considered for windows at ground level;

      iii. Intrusion detection systems are used, where appropriate;

      iv. Vacant secure areas are locked and periodically inspected; and

      v. Recording equipment is not allowed to be used unless authorized.

   c. The Security Officer or designee will review procedures for safeguarding equipment contained within facilities and on premises to ensure:

      i. Equipment requiring additional levels of protection is isolated from other equipment to the extent possible;

         (a) Network equipment and servers will be placed in a secure location limited by authorized access.

      ii. Workstations are positioned such that monitor screens and keyboards are not directly visible to unauthorized persons;

      iii. Workstations will be located in rooms with doors and windows that are locked when unattended;

iv. Workstations will not be located in areas that are unattended and have unrestricted access by the public.

v. Appropriate actions will be taken to safeguard equipment that is located at ground level and visible through exterior windows.

vi. Appropriate controls are in place to guard against equipment theft; and

vii. Reasonable controls to guard against fire damage (e.g. smoke detectors, fire alarms, and extinguishers); controls to ensure air quality is maintained that is appropriate for the equipment (e.g. air conditioning, heating, dust filters, and air humidifiers/de-humidifiers); and controls to guard against power surges and outages (e.g. multiple power feeds, backup generators, and uninterruptable power supplies) are implemented.

4. Access Control and Validation Procedures.

   a. The Security Officer or designee, in coordination with Facilities Management and Human Resources, will ensure procedures for validating Workforce access to facilities by:

      i. Ensuring formal procedures are in place to control and validate a person's physical access to the facility or facilities based on their role or function, including visitor control and control of access to software programs for testing and revision;

      ii. Configuring facility access controls to allow Workforce members access based on the latest authorizations; and

      iii. Establishing a means to update the facility access control settings to reflect Workforce member status changes upon notification.

   b. The Security Officer or designee will ensure procedures for visitor control have been established and are followed by the Workforce, including:

      i. Having visitors sign in at the reception desk upon entering the facility;

      ii. Ensuring each visitor completes an entry in the appropriate visitor log;

         (1) Information to be collected must include name, person(s) to visit, date and time of arrival/departure;

      iii. Assigning a visitor's badge, if appropriate, for ease in visual identification; and

      iv. Identifying external maintenance personnel and ensuring their appropriate access controls and validation to work areas, while minimizing the potential for ePHI access.

   c. The Security Officer or designee will validate procedures for controlling access to software programs for testing and revision by ensuring:

      i. Workforce members testing and/or revising software programs are identified, authenticated, and authorized to perform these functions;

      ii. A neutral Workforce member observes or monitors the tester/reviser; and

iii. Access controls are enforced such that the tester/reviser does not access ePHI/PHI in an unauthorized manner.

d. If available, the Security Officer or designee will obtain assurances, where practical, from the vendor regarding its access controls and validation procedures that may be a part of an externally hosted environment and incorporate this into the overall CDRP. It is important to note that not all vendors will readily provide this information for security purposes to an external organization.

e. Prior to authorizing the implementation of wireless access points, the Security Officer or designee shall change
   i. Vendor default encryption keys;
   ii. Default SNMP community strings on wireless devices;
   iii. Default passwords/passphrases on access points, and
   iv. Other security-related wireless vendor defaults, if possible.

5. Maintenance Records.

   a. The Security Officer or designee will ensure an accurate record is maintained identifying the physical components of the facility that are relevant to security (e.g., hardware, walls, doors and locks).

   b. Security Officer or designee must approve any security-relevant physical modifications prior to their implementation.

   c. Records of all repairs or modifications must be maintained by the Facility Manager or, in the event of a leased facility, through agreement with the landlord, the Security Officer may designate another Workforce member to receive and maintain the records.

   d. Keys, and access codes will be maintained securely and proper chain-of-custody ensured.

   e. If available, the Security Officer or designee will obtain assurances, where practical, from the vendor regarding its maintenance procedures and records that may be a part of an externally hosted environment and incorporate this into the overall CDRP. It is important to note that not all vendors will readily provide this information for security purposes to an external organization.

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. §164.310(a)(1) – Standard: Facility access controls.
2. 45 C.F.R. §164.310(a)(2)(i) – Contingency operations (Addressable).
3. 45 C.F.R. §164.310(a)(2)(ii) – Facility security plan (Addressable).
4. 45 C.F.R. §164.310(a)(2)(iii) – Access control and validation procedures (Addressable).

Internal:

1. Security Policy #7, Contingency Plan

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
5/10/24	Nicole Montagnet	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Physical Safeguards: Facility Access Controls, Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, & Maintenance Records			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.310(a)(2)(ii)		ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8
164.310(a)(2)(i)		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
164.310(a)(2)(i)		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
164.310(a)(2)(i)		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	NIST SP 800-53 Rev. 4 PM-11, SA-14
164.310(a)(2)(i)		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
164.310(a)(2)(i)		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
164.310		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)
164.310(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
164.310(a)(1) & (2)(iii)		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
164.310(a)(2)(i)		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
164.310(a)(1) & (2)		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
164.310(a)(2)(iii)		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

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.310(a)(1)		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7
164.310(a)(2)		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
164.310(a)(2)(i)		PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
164.310(a)(2)(i)		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
164.310		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
164.310(a)(2)(i)		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
164.310(a)(2)(iv)		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
164.310(a)(2)(iv)		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	NIST SP 800-53 Rev. 4 AU Family
164.310(a)(2)(iii)		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
164.310(a)(2)		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE- 20
164.310(a)(1) & (2)		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
164.310(a)(2)(iii)		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
164.310(a)(2)(i)		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.310(a)(2)(i)		RC.RP-1: Recovery plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
164.310(a)(2)(i)		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
164.310(a)(2)(i)		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.310(a)(2)(i)		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

