POLICY & PROCEDURE **Device and Media Controls**		**POLICY #13**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 13 v.9 Device and Media 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 monitor the receipt, removal, and movement of hardware and electronic media that contain electronic Protected Health Information (ePHI) to and from remote Workforce members and the facility or facilities in which they are housed when unassigned.

This policy and these procedures include details of Watershed Health, Inc. (Watershed) responsibilities in accordance with the Standard at 45 C.F.R. §164.310(d)(1), Device and Media Controls.

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 procedures governs the receipt and removal of hardware and electronic media that contain ePHI.

a. **Disposal (Required)**. Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

b. **Media re-use (Required)**. Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

c. **Accountability (Addressable)**. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

d. **Data backup and storage (Addressable)**. Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Procedures

1. Accountability.
   a. The Security Officer or designee will ensure all movements of information systems and media containing ePHI into and out of Watershed's facilities are identified, accounted for, tracked, and logged in accordance with *Security Policy #21, Mobile Device Security & Management*.
   b. Procedures for accepting hardware into the environment for ePHI:
      i. A secure record will be maintained by the Security Officer or designee that documents, for each Workforce member, all hardware approved for use.
      ii. A designated Workforce member will label all hardware according to access, clearance levels, and/or data set type as needed.
      iii. A designated Workforce member person will ensure the inventory list is reviewed and updated annually and in accordance with *Security Policy #21, Mobile Device Security & Management*.
      iv. A designated Workforce member will scan the components (e.g., software, storage devices) for viruses and other malicious software using automated tools prior to delivering the component(s) to the appropriate person(s) in Watershed.
      v. A designated Workforce member will deliver the components to the appropriate person(s) (ensuring appropriate authorizations are in place first), who should acknowledge in writing (email is acceptable) that they have received such components in acceptable condition.
      vi. A designated Workforce member will regularly check to see that all hardware receipt is done in accordance with these policies and procedures and immediately take corrective action if necessary.
      vii. The asset inventory will document that all hardware is returned to Watershed upon employee termination or change in position requiring hardware return.
   c. Asset Inventory List
      i. The Asset Inventory List shall include the following information:
         (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;
         (7) Data on whether the device is a portable and/or personal device;
         (8) The network address (as applicable);

(9) The machine name(s);
(10) The purpose of each system;
(11) The asset owner responsible for each device; and
(12) The department associated with each advice.

ii. The Asset Inventory List shall record the following:
(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, application desktop);
(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 (if applicable);
(9) Logical location (*e.g.,* IP address, position with the IS architecture) of the IT asset;
(10) Media access control (MAC) 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.

2. Procedures for backing up and storing ePHI.
   a. Backups of ePHI are occurring at the application level.
3. Procedures for disposing of hardware on which ePHI is stored.
   a. Watershed's Security Officer or designee is responsible for ensuring proper disposal of all ePHI and the hardware or software on which it is stored when the hardware is classified as "Out of Service."
   b. A designated Workforce member will ensure the inventory should be appropriately updated upon the disposal of components containing ePHI.
   c. A designated Workforce member will oversee the physical destruction of components on which sensitive data may be stored and document by Destruction Lot # on the Asset Inventory List when destruction is complete
4. Procedures for the re-use of media and devices that contain ePHI including hardware and/or software on which such data is stored.
   a. The Security Officer or designee is responsible for establishing procedures to govern media re-use, ensuring ePHI is removed prior to re-use.
   b. The Security Officer or designee will ensure the inventory is appropriately updated upon the re-allocation of components containing ePHI.

c. Prior to re-use, a designated Workforce member will securely overwrite components on which sensitive data is stored. The Security Officer or designee will verify and document that sanitization steps have been completed.

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(d)(1) – Standard: Device and media controls.
2. 45 C.F.R. §164.310(d)(2) – Implementation specifications.
3. 45 C.F.R. §164.310(d)(2)(i) – Disposal (Required).
4. 45 C.F.R. §164.310(d)(2)(ii) – Media re-use (Required).
5. 45 C.F.R. §164.310(d)(2)(iii) – Accountability (Addressable).
6. 45 C.F.R. §164.310(d)(2)(iv) – Data backup and storage (Addressable).

Internal:

1. Security Policy #3, Workforce Security
2. Security Policy #4, Information Access Management
3. Security Policy #7, Contingency Plan
4. Security Policy #11, Workstation & Acceptable Use
5. Security Policy #21, Mobile Device Security
6. 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 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
5/15/23	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

Device and Media Controls: Disposal, Media Re-Use, Accountability, and Data Backup and Storage			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.310(d)(1) & (2)(iii)		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(d)(1) & (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(d)(2)(iv)		PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
164.310(d)(2)(iv)		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(d)(2)		PR.IP-6: Data is destroyed according to policy	NIST SP 800-53 Rev. 4 MP-6
164.310(d)(1) & (2)		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
164.310(d)(2)(iii)		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(d)(1) & (1)		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
164.310(d)(2)(iii)		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
164.310(d)(1) & (2)(iii)		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

