POLICY & PROCEDURE **Workstation Security**		**POLICY #12**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 12 v.9 Workstation Security	3/1/2014	**5/10/2024**

Purpose

To formalize practices for physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users. Watershed Health, Inc. (Watershed) will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate physical security measures in accordance with 45 C.F.R. §164.310(c).

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 Workforce members must (i) prevent unauthorized physical access to Workstations that are used to access or store sensitive data; and (ii)take reasonable measures to prevent unauthorized viewing of sensitive data on display screens. The level of physical protection provided for Watershed's Workstations containing sensitive data must be commensurate with that of identified risks. For teleworking sites, this Policy is intended to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to Watershed's internal systems.

a. For clarification, *Workstation* is defined under the Health Insurance Portability and Accountability Act (HIPAA) to be an electronic computing device, for example, a **laptop or desk computer**, or any other device that performs similar functions, and electronic media stored in its immediate environment (collectively referred to as End User devices).

b. The sensitivity of data is classified in accordance with the *Security Policy #22, Data Governance and Data Classification*, to separate out the controls required to protect each classification level.

Procedures

1. Physical safeguards will be implemented for all Workstations that access ePHI, restricting access to authorized users only.
   a. The requirements outlined in *Security Policy #21, Mobile Device Security*, includes desktop computers and is categorized as a mobile device.
   b. Mobile devices used to access ePHI applications are to be stored securely when not in use.
   c. Do not leave mobile devices visible in cars or hotel rooms, or unattended in airports or similar public locations.
2. Workstation Physical Security.
   a. Workforce members must prevent unauthorized physical access to Workstations that are used to access or store ePHI as classified in *Security Policy #22, Data Governance and Data Classification* by:
      i. Screen locking workstations prior to leaving the area;
      ii. Logging off prior to leaving the Workstation for extended periods or when others may share the Workstation;
      iii. Closing files and applications when not in use;
      iv. Complying with all applicable password policies and procedures, including storing any written passwords only in secure locations (e.g., locking file cabinets, safe).
   b. Watershed prohibits the use of (i) writable, removable media; and (ii) personally owned, removable media. Removable media includes USB Drives (flash or thumb drives), memory sticks, external hard drives, SSD drives, CDs, DVDs.
   c. Workforce members must take reasonable measures to prevent unauthorized viewing of display screens by:
      i. Locating information systems in secured areas not accessible to unauthorized persons; and
      ii. Positioning or shielding Workstations such that the monitor screens and keyboards are not visible to unauthorized persons.
   d. Workforce members will not download software or applications that have **not** been previously approved for use by Watershed:
      i. If a Workforce member requires additional software or applications to perform their job function that are not part of Watershed's approved suite of tools, the Workforce member will contact the Security Officer or designee;

ii. The Workforce member and their Supervisor will provide the Security Officer or designee with written justification as it relates to the necessity of using the software or application to perform job functions; and

iii. The Security Officer or designee will conduct a review of the software or application and grant any approvals prior to installation. The Security Officer or designee is the final authority for granting or denying the use of non-Company sanctioned software or applications.

e. Additional requirements relating to other mobile devices and formats can be found in *Security Policy #21, Mobile Device Security*.

3. Workforce member(s) will be issued specifically configured mobile devices for travel to locations that Watershed deems to be of significant risk in accordance with internal policies and procedures. Upon return from these locations, the Security Officer, or designee, shall check these devices for malware and physical tampering.

4. Watershed's Workforce members must immediately report to their Supervisor/Manager and the Security Officer or Designee, any loss or theft of a mobile device that is used to access Watershed's systems, applications, or information.

5. All Workforce members will be trained on proper Workstation use and security.

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(c) – Standard: Workstation security.

Internal:

1. Security Policy #3, Workforce Security
2. Security Policy #21, Mobile Device Security

3. 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

Workstation Security			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.310(d)		ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8
164.310(d)		ID.AM-3: Organizational communication and data flows are mapped	NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
164.310(b), 164.310(c)		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)		PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.310(c)		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
164.310(c)		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(c)		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

