| **POLICY & PROCEDURE**<br>**Workstation & Acceptable Use** | | **POLICY #11** |
|---|---|---|
| **SUPERCEDES POLICY:** | **EFFECTIVE:** | **LAST REVIEWED:** |
| Privacy and Security Compliance Program<br>Policy & Procedure 11 v.9<br>Workstation & Acceptable Use | 3/1/2014 | **5/10/2024** |

# Purpose

To formalize practices for the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. (ePHI).

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

Workforce members shall use Workstations in a manner which reflects the sensitivity of the information contained therein and minimize the possibility of unauthorized access to such information.

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 or mobile 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. The Security Officer or designee will identify the classes of workstations appropriate for accessing ePHI and will document the types of workstations and their functions.

 

2. The Security Officer or designee will document the classes of workstation and their functions as follows:
    a. Thin clients
    b. Desktops
    c. Laptops
    d. Virtual Servers
3. Workstation Use.
    a. Workforce members should only access systems or applications in the performance of their job functions.
    b. Workforce members shall not access systems or applications through a public or open Wi-Fi network.
    c. System or network activities.
        i. Acceptable system or network activities may include:
            (1) Communicating and exchanging information directly relating to Watershed's purpose and business;
            (2) Posting Watershed policies and procedures;
            (3) Participating in the review and edit of content via wiki pages, blogs, and/or comments;
            (4) Downloading or viewing content from the appropriate Intranet space or page required for the user's job responsibilities;
            (5) Obtaining research material and training related to the user's job responsibilities;
            (6) Trouble-shooting business or technical problems;
            (7) Previewing new business products; or
            (8) Testing new software or applications, including those from a vendor's website.
        ii. Unacceptable system or network activities may include:
            (1) Violating federal or state laws;
            (2) Introduction of malicious software or programs into the network or server (e.g., viruses, worms, Trojan horses);
            (3) Using writable, removable media in organizational systems;
            (4) Revealing account passwords to others or allowing use of an account by others;
            (5) Effecting security breaches or disruptions of network communications;
            (6) Circumventing user authentication or security of any host, network or account;
            (7) Introducing honeypots, honeynets, or similar technology on the Watershed network;

 

(8) Transmitting threatening, obscene, or harassing messages;

(9) Engaging in discussions considered to be disparaging, embarrassing, or otherwise reflecting negatively on Watershed, its Workforce members, or any person or entity;

(10) Making an unauthorized entry to any other machine or account via the network;

(11) Intentionally seeking unauthorized information, or obtaining copies of password files or passwords belonging to others;

(12) Duplicating copyrighted and licensed software unless it is explicitly stated that it may be done;

(13) Distributing unsolicited advertising; or

(14) Developing or executing programs intentionally designed to harass other users or infiltrate, damage, and/or alter a computer or computing system.

d. Intranet and/or Internet activities.

i. Monitoring.

(1) Watershed reserves the right to monitor usage by user and the sites they view.

ii. Acceptable uses of the Intranet and Internet may include:

(1) Communicating and exchanging information directly relating to the Watershed's purpose and business;

(2) Announcing Watershed policies and procedures;

(3) Participating in the review and edit of content via wiki pages, blogs, and/or comments;

(4) Downloading or viewing content from the appropriate Intranet space or page required for the user's job responsibilities;

(5) Obtaining research material and training related to the user's job responsibilities;

(6) Trouble-shooting business or technical problems;

(7) Previewing new business products; and

(8) Testing new software at a vendor's website.

iii. Unacceptable uses of the Intranet and Internet may include:

(1) Violating federal or state laws;

(2) Transmitting threatening or harassing messages;

(3) Engaging in discussions considered to be disparaging, embarrassing, or otherwise reflecting negatively on the Watershed, its employees, or any person or entity;

(4) Transmitting obscene messages;

(5) Making an unauthorized entry to any other machine or account via the network;

 

(6) Intentionally seeking unauthorized information, or obtaining copies of password files or passwords belonging to others;

(7) Duplicating copyrighted and licensed software unless it is explicitly stated that it may be done. The use of unlicensed software is a violation of the Copyright Act of 1976 and can subject the Watershed to penalties of $100,000 per copy of the unlicensed software;

(8) Distributing unsolicited advertising; or

(9) Developing or executing programs intentionally designed to harass other users or infiltrate, damage, and/or alter a computer or computing system.

4. 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(b) – Standard: Workstation use

## Internal:

1. Security Policy #22, Data Governance and Data Classification
2. Security Policy #24, Email Security

## 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

| Workstation Use | | | |
|---|---|---|---|
| **HIPAA** | | **Cybersecurity Framework Subcategory** | **NIST Control Mapping** |
| 164.310(b) | | PR.AC-3: Remote access is managed | NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 |
| 164.310(b) | | 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 |
| 164.310(b) | | PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | NIST SP 800-53 Rev. 4 AC-4, SC-7 |
| 164.310(b) | | 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(b) | | 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(b) | | 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 |

 