POLICY & PROCEDURE **Audit Controls**		**POLICY #15**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 15 v.9 Audit Controls	3/1/2014	**5/10/2024**

Purpose

To implement formal hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information (ePHI). Watershed Health, Inc. (Watershed) will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate technical security measures in accordance with 45 C.F.R. §164.312(b).

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

To ensure appropriate access and use of systems, and the data contained therein, utilizing hardware, software, and/or procedural mechanisms to record and examine system activity.

Procedures

1. Watershed's Security Officer or designee will determine the components of Watershed's information system environment that will record audit trails and be used in the internal audit process. Such components may include network perimeter devices (e.g., firewalls, network intrusion protection systems, routers, switches, Virtual Private Network appliances) as well as various types of servers and workstations.
    a. At a minimum, enable event auditing on all computers and/or software applications that process, transmit, and/or store ePHI.

2. As an integral part of the audit control process, the Security Officer, or Designee, will conduct an in-house information system activity review of records of system activity in accordance with *Security Policy #1, Security Management Process*, including reporting and investigating a security incident, as outlined in *Security Policy #6, Security Incidents*.
3. A designated Workforce member will ensure automated audit trail capabilities are enabled for applicable network devices, as appropriate.
4. The Security Officer or designee will ensure availability of servers and databases to store information for a reasonable period.
5. The Security Officer or designee will coordinate with various System Owners to ensure the capability to track and store changes, additions, and deletions of ePHI, as appropriate.
6. A designated Workforce member will ensure the capability of appropriate network security devices and/or software applications (e.g., intrusion protections system) to monitor, track, and prevent unauthorized access as appropriate.
7. A designated Workforce member will identify and implement the measures that will be used to protect the confidentiality, availability and integrity of audit trails and internal audit reports.

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(b)(b) – Standard: Audit controls.

Internal:

1. Security Policy #1, Security Management Process
2. Security Policy #6, Security Incidents

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

Audit Controls			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.312(c)		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(b) & (c)		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	NIST SP 800-53 Rev. 4 AC-4, SC-7
164.312(b) & (c)		PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.312(b)		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	NIST SP 800-53 Rev. 4 SI-7
164.312(b)		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(b)		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	NIST SP 800-53 Rev. 4 AU Family
164.312(b)		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(b)		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(b)		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI- 4
164.312(b)		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
164.312(b)		DE.CM-1: The network is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
164.312(b)		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(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
164.306(e)		DE.DP-3: Detection processes are tested	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM- 14, SI-3, SI-4

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.312(b)		RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4

