POLICY & PROCEDURE **Documentation**		**POLICY #20**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Exhibit EE, Documentation Retention and Storage	3/1/2014	**5/10/2024**

Purpose

To address the requirement to maintain, update, and make available documentation to comply with the standards, implementation specifications, or other requirements contained in the Health Insurance Portability and Accountability Act (HIPAA) Regulations at 45 C.F.R. §164.316(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 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

Watershed will maintain documentation, in written or electronic form, of policies, procedures, communications, and other administrative documents; and if an action, activity or assessment is required to be documented, maintain a written and/or electronic record of the action, activity, or assessment. This includes:

a. **Time Limit**

b. **Availability**

c. **Updates**

Procedures

1. The Security Officer or Designee will maintain in written form (paper and/or electronic) all documentation of actions, activities, or assessments for regulation compliance for the same period applied to policies and procedures. These may include:

   a. All policies and procedures to demonstrate compliance with the Security Rule;

b. All documentation of decisions to implement an alternative Addressable Specification, including documentation describing how the specification was not deemed reasonable and appropriate, and how the chosen alternative is reasonable and appropriate;

c. Risk Analysis Records;

d. Risk Management decisions to implement measures sufficient to reduce risks and vulnerabilities to reasonable and appropriate levels;

e. Records demonstrating regular review of information system activities;

f. The performance of periodic technical and non-technical evaluations;

g. Documentation of the repairs and modifications to physical facilities affecting security;

h. Records of movements of hardware and electronic media containing Electronic Protected Health Information (ePHI) and the person responsible; and

i. The appointment of the HIPAA Security Officer.

2. Continually monitor for events that would necessitate documentation revision that may include:

   a. Update of applicable regulations, laws, standards, or other mandates;

   b. Change in system configuration;

   c. Change in operational environment (to include threat, vulnerability and risk assessment findings);

   d. Change in organizational structure; and

   e. New or changed requirement resulting from a business associate contract.

3. Update the policies and procedures, or other documentation as required, to maintain current practices.

4. Disseminate all updates to documentation to those persons responsible for implementing the procedures to which the documentation pertains as applicable within 60 days of any changes.

5. Ensure the documentation is available to the workforce members who must implement.

6. Retain documentation created, or obtained, 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.

7. Destroy any documentation that is no longer required in a manner appropriate to the data classification described in *Security Policy #22, Data Governance and Data Classification*.

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. §164.316(b) Standard: Documentation.

Internal:

1. Security Policy #22, Data Governance and Data Classification

External:

1. Current Administrative Simplification Regulations
2. HHS Guidance – Guidance on Risk Analysis Requirements under the HIPAA Security Rule
3. 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
5/10/2024	Nicole Montagnet	9.0	Reviewed

NIST CSF Subcategory & Control Mapping

Documentation			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.316(b)(2)		ID.AM-4: External information systems are catalogued	NIST SP 800-53 Rev. 4 AC-20, SA-9
164.316(b)(2)(iii)		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
164.316(b)(2)(iii)		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
164.306(e)		PR.IP-7: Protection processes are continuously improved	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR- 8, PL-2, PM-6
164.316(b)(2)(iii)		PR.IP-7: Protection processes are continuously improved	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR- 8, PL-2, PM-6
164.316(b)(2)(iii)		RC.IM-1: Recovery plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.316(b)(2)(iii))		RS.IM-1: Response plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

