POLICY & PROCEDURE **Data Integrity**		**POLICY #16**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 16 v.9 Data Integrity	3/1/2014	**5/10/2024**

Purpose

To corroborate that ePHI has not been altered or destroyed in an unauthorized manner as required by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. As such, 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(c)(1).

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 will implement appropriate technical controlsto confirm that ePHI contained on Watershed's information systems or applications has not been altered or destroyed in an unauthorized way.

Procedures

1. The regularly scheduled Information Risk Analyses will assess threats and vulnerabilitieswhich may put information assets at risk. The risk likelihood and impact will be assessed using a combination of existing security controls and sensitivity of the information being protected. Refer to *Security Policy #22, Data Governance and Data Classification*.

2. Watershed will consider the following processes when assessing appropriate technical controls:

   a. Protecting ePHI from improper alteration or destruction;

   b. Detecting improper alteration or destruction; and

   c. Actions to be taken when improper alteration or destruction is detected.

3. Watershed’s System Owners will take reasonable and appropriate steps to implement appropriate technical controls, where applicable, to ensure the integrity of the information is maintained including:
   a. Which ePHI will be validated; and
   b. Which technical controls would be reasonable and appropriate.
4. Watershed’s Security Officer or designee will approve the technical controls, in concert with the appropriate governance body, to be considered for implementation to protect ePHI from unauthorized alteration or destruction. The Security Officer or designee will ensure data integrity is validated and will take reasonable and appropriate steps to ensure that the technical controls are reviewed, and integrity incident reports are generated from the technical controls.
   a. Such controls may include:
      i. Checksums;
      ii. Digital Signatures;
      iii. Hash values;
      iv. Message authentication codes; or
      v. Encryption.
5. Watershed’s Department Supervisors/Managers will take reasonable and appropriate steps to train Workforce members regarding the technical control(s) implemented and the necessity for maintaining the integrity of ePHI.

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(c)(1) – Standard: Integrity.
2. 45 C.F.R. §164.312(c)(2) – Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).

Internal:

1. 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
5/10/24	Nicole Montagnet	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Integrity

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.312(c)(1) & (2)	🟪	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	NIST SP 800-53 Rev. 4 SI-7