POLICY & PROCEDURE **Transmission Security**		**POLICY #18**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Exhibit DD, Transmission Security	3/1/2014	**5/10/2024**

Purpose

To guard against unauthorized access to electronic Protected Health Information (ePHI) that is being transmitted over an electronic communications network. As such, Watershed Health, Inc. (Watershed) will continually assess potential threats and vulnerabilities to ePHI in its possession, and develop, implement, and maintain appropriate technical security mechanisms to guard against unauthorized access to data that is transmitted over a communications network, and incorporate the specifications required in 45 C.F.R. §164.312(e)(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

This policy and procedures will implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network:

a. **Integrity controls (Addressable)**. Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

b. **Encryption (Addressable)**. Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Procedures

1. Integrity Controls.

a. Watershed shall implement and maintain integrity controls to ensure the validity of ePHI transmitted over a communications network, to protect the ePHI from unauthorized modification. The data classifications of electronic information will be necessary when determining the extent of technical controls required for certain data types (refer to *Security Policy #22, Data Governance and Data Classification*).

b. At a minimum, Watershed's risk analysis will consider the following factors when determining if integrity controls must be used when sending specific data over an electronic communications network:

   i. The threats to the data;

   ii. The data classification;

   iii. The expected impact to Watershed functionality and workflow if the data are and are not sent with integrity controls; and

   iv. The ability of the recipient of the data to check the integrity of the data that was sent.

c. All integrity controls used to protect the confidentiality, integrity and availability of Watershed's data transmitted over wireless or wired networks shall be reviewed by Watershed's Security Officer or designee.

d. Determine the information communicated across networks for which data integrity will be checked; ensure that all traffic containing ePHI is included.

e. Determine the integrity resources that will be used to perform the integrity inspections.

   i. The Security Officer, or designee, shall confirm that FIPS-approved encryption (*e.g.* minimum of AES WPA2) has been configured and enabled for authentication and transmission.

2. Encryption controls. When risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity and availability of Watershed's data transmitted over electronic communications networks. The risk analysis must also be used to determine the type and quality of the encryption algorithm and the length of cryptographic keys.

   a. At a minimum, Watershed's risk analysis will consider the following factors when determining if encryption must be used when sending specific data over an electronic communications network:

      i. The risk to the data if not encrypted;

      ii. The data classification;

      iii. The expected impact to Watershed functionality and workflow if data is or is not encrypted;

      iv. Alternative methods available to protect the confidentiality, integrity and availability of data; and

      v. The ability of the recipient to decrypt the data received.

b. Watershed shall employ encryption to protect ePHI communications transmissions over open and public networks to ensure that such transmissions cannot be easily intercepted and interpreted by parties other than the intended recipient. Determine the encryption mechanisms that will be used in transmitting or receiving ePHI messages over an open communications network (e.g., the Internet). Ensure that such mechanisms are equivalent to or compatible with the encryption features employed by the entities with which Watershed communicates.

   i. Encryption control procedures will be employed when the risk analysis indicates it is necessary and in accordance with *Security Policy #22, Data Governance and Data Classification*. Appropriate encryption must be used to protect the confidentiality of Watershed's data transmitted over electronic communications networks.

   ii. Watershed must protect all cryptographic keys against modification and destruction; secret and private keys must be protected against unauthorized disclosure.

   iii. Ensure that each ePHI message is encrypted (using one of the predetermined mechanisms) while in transit over an open or public network.

   iv. Ensure that the password(s) and/or token(s) associated with the encryption measure(s) are protected from unauthorized disclosure.

   v. Utilize the cryptographic features to decrypt incoming encrypted messages.

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(e)(1) – Standard: Transmission security.
2. 45 C.F.R. §164.312(e)(2) – Implementation specifications.
3. 45 C.F.R. §164.312(e)(2)(i) – Integrity controls (Addressable).
4. 45 C.F.R. §164.312(e)(2)(ii) – Encryption (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	9.0	Reviewed

NIST CSF Subcategory & Control Mapping

Transmission Security: Integrity Controls & Encryption			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.312(e)(1) & (2)(ii)		PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
164.312(e)(1) & (2)		PR.DS-2: Data-in- transit is protected	NIST SP 800-53 Rev. 4 SC-8
164.312(e)(2)(i)		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(e)(2)(i)		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

