POLICY & PROCEDURE **Business Associate Contracts and Other Arrangements**		**POLICY #9**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 9 v.9 Business Associate Contracts and Other Arrangements	3/1/2014	**5/10/2024**

Purpose

To describe the relationship and respective commitments, responsibilities, and obligations of Watershed Health, Inc. (Watershed) and any Business Associates Subcontractors (Subcontractors) of Watershed and other third parties who use or disclose Electronic Protected Health Information (ePHI) and Protected Health Information (PHI) in accordance with applicable Health Insurance Portability and Accountability Act (HIPAA) Regulations.

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

It is the policy of Watershed to protect ePHI/PHI and to require Subcontractors and other third parties who use or disclose ePHI/PHI on behalf of Watershed to provide satisfactory assurances that they will protect ePHI/PHI. The assurances will be documented through a written Business Associate Agreement (BAA) or other agreement that meets the requirements of state and federal privacy laws and HIPAA Regulations.

Procedures

1. Downstream Business Associate Subcontractors.

    a. Determine if the Person or Entity is a Downstream Subcontractor. Subcontractors do not include persons or entities that would not, in the normal course of their activities, use or disclose ePHI/PHI but who may inadvertently have contact with such information. Watershed's Legal Counsel will ensure that those Subcontractors sign a confidentiality agreement but are

otherwise not covered by this policy (see the *HHS Guidance - Other Situations in Which a Business Associate Contract Is NOT Required*, located at the External References section at the end of this policy).

b. Disclosures to a Subcontractor. Watershed may not disclose ePHI/PHI to a Subcontractor or allow a Subcontractor to create, receive, maintain, or transmit ePHI/PHI on behalf of Watershed until Watershed obtains satisfactory assurance that the Subcontractor will appropriately safeguard the information as required by the security standards and implementation standards in the HIPAA Security Rule applicable to Business Associates. This satisfactory assurance must be documented in writing in the form of a contract, agreement, or other written arrangement, and must also include the obligations of Watershed with regard to the ePHI/PHI to be held by the Subcontractor.

c. Subcontractors must report to Watershed any security incident of which it becomes aware, including breaches of unsecured PHI.

d. Watershed will disclose only the minimum necessary information to a Subcontractor that is reasonably necessary to accomplish the intended purpose of the disclosure.

2. Upstream Business Associate Agreement

a. Upstream Covered Entity may provide a BAA for Watershed to sign. Should the upstream Covered Entity not provide their BAA, Watershed can provide its BAA.

b. Upon termination of an upstream BAA, Watershed will return to the Client/Customer or destroy, as feasible, all PHI provided by the upstream Covered Entity within the time and in the manner specified in the Client/Customer's BAA. The Privacy Officer or designee will make the determination regarding the feasibility of returning or destroying PHI.

c. Prior to returning or destroying such PHI, if requested by the Client/Customer and if feasible to do so, Watershed will recover any PHI in the possession of its downstream Business Associates and will destroy or return to the Client/Customer any PHI so recovered.

i. If it is not feasible for Watershed to return or destroy the PHI or obtain any PHI in the possession of a downstream Business Associate, the Privacy Officer or designee will notify the Client/Customer in writing. The notification must include:

(1) A statement that Watershed has determined that it is infeasible to return or destroy the PHI in its possession; and

(2) The reasons for such determination.

d. Watershed will, if it still possesses PHI after the BAA terminates, continue to extend the protections contained in these policies and procedures and any similar contractual obligations to the Client/Customer's PHI and limit any further uses and/or disclosures of such PHI to the purposes that make the return or destruction of the PHI infeasible. As soon as return or destruction of the PHI becomes feasible (as determined by Legal Counsel), Watershed will promptly return or destroy the PHI that it had retained.

3. For more comprehensive information regarding Business Associates and BAAs, refer to the Watershed *Privacy Policy #11, Business Associate Contracts and Other Arrangements*.

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. §164.308(b) – Business associate contracts and other arrangements.
2. 45 C.F.R. §164.308(a) – Business associate contracts and other arrangements .

Internal:

1. Privacy Policy #11, Business Associate Contracts and Other Arrangements

External:

1. Current Administrative Simplification Regulations
2. HHS Guidance – Other Situations in Which a Business Associate Contract Is NOT Required
3. HHS Sample Business Associate Agreement Provisions (Published January 25, 2013)
4. 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
5/15/23	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

Organizational Requirements: Business Associate Contracts or Other Arrangements			
HIPAA		**Cybersecurity Framework Subcategory**	**NIST Control Mapping**
164.308(b) 164.314(a)(1) & (2)		ID.AM-4: External information systems are catalogued	NIST SP 800-53 Rev. 4 AC-20, SA-9
164.314		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third- party stakeholders	NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
164.314		ID.BE-1: The organization's role in the supply chain is identified and communicated	NIST SP 800-53 Rev. 4 CP-2, SA-12
164.314		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	NIST SP 800-53 Rev. 4 CP-2, SA-12
164.314(a)(1)		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
164.308(b) 164.314		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	NIST SP 800-53 Rev. 4 PM-1, PS-7
164.314		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
164.308(b)		ID.GV-4: Governance and risk management processes address cybersecurity risks	NIST SP 800-53 Rev. 4 PM-9, PM-11
164.314		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
164.314(a)(2)(i)(C)		ID.RA-6: Risk responses are identified and prioritized	NIST SP 800-53 Rev. 4 PM-4, PM-9
164.308(b)(1) & (3)		PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
164.308(b) 164.314(a)(1) & (2)		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	NIST SP 800-53 Rev. 4 PS-7, SA-9
164.308(b)(1)		PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 SC-28
164.308(b)(1)		PR.DS-2: Data-in- transit is protected	NIST SP 800-53 Rev. 4 SC-8

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(b)(2)		PR.DS-2: Data-in- transit is protected	NIST SP 800-53 Rev. 4 SC-8
164.314(a)(2)(i)(C) & (iii)		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
164.314(a)(2)(i)(C) & (iii)		DE.DP-4: Event detection information is communicated to appropriate parties	NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA- 5, SI-4
164.314(a)(2)(i)(C)		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4
164.314(a)(2)(i)(C) & (iii)		RS.CO-2: Events are reported consistent with established criteria	NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
164.314(a)(2)(i)(C)		RS.CO-3: Information is shared consistent with response plans	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR- 4, IR-8, PE-6, RA-5, SI-4

