POLICY & PROCEDURE Vendor Risk Management		POLICY #26
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
n/a	5/19/22	5/10/2024

Purpose

To establish policy governing security requirements for third-party IT vendors or service organizations (hereinafter referred to as "vendors") who support, create, receive, maintain, or transmit electronic information or systems. This includes but is not limited to Electronic Protected Health Information (ePHI) and Protected Health Information (PHI) in accordance with applicable Health Insurance Portability and Accountability Act (HIPAA) Regulations.

Applicability

Watershed Workforce members are responsible for awareness of this policy and adherence to the given direction and guidance.

Definitions

"Vendor" includes any entity or person not under the direct business control of an organization with whom it engages in a business relationship, including any vendor, supplier, support provider, fulfilment provider, agent, consultant, advisor, contractor, business, marketing or strategic partner, joint venture, associate and correspondent.

"Vendor or third party risk management" is the process of fully identifying all of the significant vendors or Business Associates that aid in the delivery of a product or service to the organization or their customers in which access to or use of Protected Health Information (PHI) or sensitive information (SI) is a component and implementing processes to prevent the loss of confidentiality, integrity, or availability of PHI/SI throughout the vendor lifecycle (procurement, contracting, onboarding, service delivery, renewal, and offboarding) in order to mitigate vulnerabilities and adverse events.

Policy

It is the policy of Watershed to develop the Vendor Risk Management (VRM) Program to identify and categorize vendors who create, receive, maintain, or transmit or support Watershed's electronic information and systems:

a. The Watershed Cybersecurity Oversight Committee is responsible for vendor risk assessment and management of vendor approval.
b. The Security Officer or approved designee shall

i. review the potential risks to Watershed's information assets when business processes involve third parties, to identify appropriate controls implemented and to mitigate risks before granting access;
ii. conduct due diligence on potential third parties before selecting and entering contracts or relationships; and
iii. require Vendors and other third parties who use or disclose electronic information on behalf of Watershed to provide satisfactory assurance that they will protect electronic information.

Procedures

1. Watershed will maintain an up-to-date inventory of vendors.
    a. A *Vendor Intake Form* may be used to evaluate the vendor and determine a risk category.
2. Watershed will conduct an initial risk assessment as part of its vendor due diligence utilizing any or all of the following information:
        i. Vendor Intake Form;
        ii. SOC or other reports containing an analysis of the vendor's information security program;
        iii. Background checks (e.g., OIG exclusion);
        iv. Description of vendor services, specifically those to be provided to Watershed;
        v. Copies of any data flows, architectural renderings, or compliance mappings as made available by the Vendor that describe its security controls;
        vi. Policies, procedures, or compliance statements related to the vendor's privacy, breach, and security programs (e.g., HIPAA, GDPR, CCPA) as made available by the vendor;
        vii. Contractual or legal issues (e.g., Office for Civil Rights investigations).
    b. Watershed will assign a risk rating based on the findings of the initial risk assessment and any or all of the following:
        i. Access to Watershed's data;
        ii. Nature of the type of data set involved (client confidential, private data, financial transactions, identifiers, passwords, etc.);
        iii. Volume of data;
        iv. Vendor size;
        v. Number of downstream subcontractors;
        vi. Supporting compliance documentation (e.g. Soc, HITRUST, etc.);
        vii. Overall impression of security, privacy, and breach compliance efforts based on documentation;

viii. Breach history;

ix. Business Associate Agreement with Vendor;

x. Data and information security expectations (related to nature of data);

xi. Financial standing of the vendor;

xii. Data storage location (country or region) (on-shore or off-shore) or where the vendor is headquartered:

(1) Some jurisdictions have looser regulations, a noted tendency for corruption in the market, opaque business practices or a lack of enforcement of good corporate governance.

3. Watershed will make a final determination of risk tolerability, and once risk acceptance has been completed, the remaining onboarding steps can be completed.
4. Vendor Access Control Requirements.
   a. Watershed will only allow third parties to create, receive, maintain, or transmit electronic information on its behalf after Watershed obtains written satisfactory assurance that the third party will appropriately maintain and enforce the privacy and security of Watershed's data, including, where relevant, protecting electronic information via the Business Associate Agreement.
   b. Third party access will be based on the principles of need-to-know and least privilege. Third party access will be granted only for the duration required.
   c. Remote access connections between Watershed and third parties must be encrypted and will be monitored on an ongoing basis.
5. Vendor Agreements.
   a. Agreements, including but not limited to Business Associate Agreements (where applicable), Service Level Agreements (SLAs), and other contractual requirements, with third parties involving accessing, processing, communicating, or managing Watershed's information or assets or adding products or services, will cover relevant security requirements and include appropriate security and privacy controls.
   b. As required and applicable, agreements will include provisions for breach notification and termination upon breach and define the disposition of electronic information on termination of the agreement.
   c. Watershed will disclose only the minimum necessary information to a third party that is reasonably necessary to accomplish the intended purpose of the disclosure.
6. Vendor Monitoring and Review.
   a. Watershed will monitor vendors for adherence to provisions described in the agreements.

b. Watershed will review vendors to determine changes in risk rating using any or all of the following:

   i. Asking vendors to complete an annual attestation (e.g. Annual Vendor Compliance and Cyber Risk Management 10-Point Attestation Questionnaire) to determine ongoing levels of compliance, including changes to existing security controls and policies and procedures.

   ii. Identifying any updated services, reports, and documentation as provided by vendor and updating the *Vendor Risk Management Worksheet* and vendor risk rating as appropriate.

   iii. If Watershed discovers a significant change affecting the risk rating of the vendor, Watershed will determine whether the risk is tolerable. If deemed intolerable, the relationship with the vendor may be terminated.

7. Watershed will ensure that processes are initiated for termination and offboarding of a vendor and their workforce members utilizing any or all of the following:

   a. Reviewing the termination provisions outlined in the underlying service agreement and/or Business Associate Agreement for any unique requirements or notification timelines;

   b. Confirming the return of Watershed equipment or other physical assets that may be in the vendor's possession;

   c. Obtaining written assurances from the vendor that data has been returned to Watershed or destroyed, or the reasons why the return or destruction is not feasible;

   d. Disabling physical access to facilities;

   e. Disabling electronic access to any systems or applications; and

   f. Documenting any modifications or inability for vendor to comply with the standard offboarding process.

Enforcement

Violations of this policy 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. Vendor Intake Form
2. Annual Vendor Attestation
3. Vendor Risk Management Worksheet

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)

Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	DocuSigned by: Lisa Stanley 9418DGC7CF3D47D...
(Printed Name)	**(Date)**	**(Signature)**

REVISION HISTORY			
Date	**Author**	**Version**	**Comments**
5/5/2022	Scott Snodgrass	1.0	Implemented
5/20/2022	Lisa Stanley	1.0	Reviewed
5/20/2022	Nicole Montagnet	1.0	Reviewed by Security and Privacy Officers
5/10/2024	Nicole Montagnet	1.0	Reviewed

