POLICY & PROCEDURE **Contingency Plan**		**POLICY #7**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Policy & Procedure 7 v. 9 Contingency Plan	3/1/2014	**5/10/2024**

Purpose

To maintain formal practices for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages, or causes a lack of access to, systems that contain Electronic Protected Health Information (ePHI), addressing the five implementation specifications under 45 C.F.R. §164.308(a)(7)(i).

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

This policy serves as the basis of the Watershed Contingency and Disaster Recovery Plan (CDRP) for handling responses to system emergencies involving ePHI, ensuring continuity of operations during an emergency, and recovering from a disaster, to include:

a. **Data backup plan (Required)**. Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

b. **Disaster recovery plan (Required)**. Establish (and implement as needed) procedures to restore any loss of data.

c. **Emergency mode operation plan (Required)**. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

d. **Testing and revision procedures (Addressable)**. Implement procedures for periodic testing and revision of contingency plans.

  e. **Applications and data criticality analysis (Addressable)**. Assess the relative criticality of specific applications and data in support of other contingency plan components.

Procedures

1. The Security Officer, or designee, is responsible for coordinating the various plans to ensure a cohesive master CDRP includes the required and addressable elements.
    a. In the event that any system or application containing ePHI pertaining to Watershed is hosted externally, Watershed will obtain assurances, where practical, from the vendor regarding its contingency and disaster recovery procedures and retain copies as part of an overall CDRP.
    b. Refer to the *Security Policy #22, Data Governance and Data Classification*, for additional information on the data classifications.
    c. Where applicable, Watershed's Security Officer or designee will manage the response, resumption recovery, and restoration phases.
2. Data Backup Plan.
    a. The Security Officer or designee will maintain an inventory of:
        i. Company owned, configured, or administered information systems or applications that require data backup;
        ii. Type of data contained in each system or application;
        iii. Use of encryption and encryption key management, if applicable;
        iv. The backup methods for each information system or application (e.g., continuous, full, incremental, differential or continuous backup);
        v. The frequency of performing backups; and
        vi. The Workforce member(s) designated and responsible for performing, cataloging, inspecting, storing, testing, restoring, and securing the backups for each system or application.
    b. The responsible Workforce member(s) will back up the data sets/systems on schedule or configure the backups to be conducted automatically using approved backup software.
    c. For AWS or similar backup processes, the responsible Workforce member(s) will ensure the backup software and/or scripts run on a daily basis, and data is backed up to another storage location within the hosted service.
    d. The Security Officer or designee will:
        i. Ensure procedures are in place to create and maintain exact copies of ePHI;
        ii. Coordinate these procedures with the Data Backup and Storage procedures in *Security Policy #13, Device and Media Controls*;

iii. Track the archive requirements for each backed up data set, ensuring records are maintained for the appropriate retention period; and

iv. Test and revise as needed the procedures and related documentation for Data Backup.

3. Data Backup Restoration Procedure
   a. All Watershed systems with ePHI are contained within the AWS cloud environment.
   b. Infrastructure restoration
      i. Infrastructure instances are replicated across multiple AWS regions.
      ii. To restore from backup, the designated Workforce member will use the snapshot image of our AWS instances and push the latest code from our code repository through automated deployment.
   c. Code restoration
      i. AWS instances containing code are automatically backed up every 2 hours, held for 7 days; weekly, held for a month; and monthly, held for a year.
      ii. To manually restore from backup, the designated Workforce member will log onto AWS, search for the AWS database instance housing code and follow AWS prompts to backup.
   d. Data restoration
      i. AWS instances containing data are automatically replicated across multiple AWS regions and backed up every 2 hours, held for 7 days; weekly, held for a month; monthly, held for a year.
      ii. AWS instances transmitting data are automatically backed up every seven days.
      iii. To manually restore from backup, the designated Workforce member will log onto AWS, search for the AWS SQL instance housing or transmitting data and follow AWS prompts to backup.
   e. Data Retention
      i. Data shall be retained for the duration mandated by relevant contractual, legal, regulatory and business requirements.

4. Disaster Recovery Plan.

   a. The Security Officer or designee will ensure periodic testing of the ability to restore data and will revise the procedures and related documentation for Disaster Recovery as necessary, in accordance with the established Testing and Revision Procedures.

5. Emergency Mode Operations.

   a. Pre-emergency planning.

      i. Utilizing the results of the most recent risk analysis (Refer to *Security Policy #1, Security Management Process*), the current data criticality analysis, and other available resources, and in coordination with Watershed's CDRP, the Security Officer or designee will:

         (1) Evaluate the impact of entering emergency mode on the protection of the security of ePHI systems and processes to determine the effect on the security of ePHI;

         (2) Evaluate that all systems and processes used during normal operations to protect ePHI are maintained during an emergency;

(a) This includes ensuring the Integrity and Availability, as well as the Confidentiality of all information data sets;

(3) Where systems and processes are identified that cannot continue to ensure the Confidentiality, Availability and Integrity of ePHI, the Security Officer or designee will evaluate alternatives;

(a) This may include arranging for an alternate location, mirroring data to a remote site, uninterruptible power supplies, and/or having agreements with vendors and suppliers for rapid provisioning of equipment;

(4) Report the findings to Watershed's Chief Operating Officer for approval of additional resources, alternatives or other decision making related to continuity of operations for the business; and

(5) Incorporate the decisions and resource allocations in Watershed's CDRP.

ii. If an alternate site will be used where protection of ePHI cannot be assured at the primary location, the Security Officer, in coordination with the Chief Technology Officer (CTO) will:

(1) Select and maintain the alternate site;

(2) Determine the resources needed to bring the site to full functionality;

(3) Ensure hardware/software compatibility between the primary and backup sites;

(4) Ensure backup power and communications will be sustained; and

(5) Stage equipment and resources, as appropriate, prior to an emergency.

iii. Test and revise the Plan as necessary.

b. Emergency Mode activation.

i. When notified of an emergency through Watershed's processes, the CTO or designee will notify the Security Officer who will initiate actions.

ii. The Security Officer or designee will:

(1) Determine the effect of the emergency on protection of the security of ePHI, based on the extent and seriousness of the emergency;

(2) Define the minimum ePHI necessary to treat patients in the event of an emergency and limit the access to that minimum amount.

(3) Identify and define manual and automated methods to be used by authorized Watershed's Workforce members to access ePHI during an emergency.

(4) Identify and define appropriate logging and auditing that must occur when authorized Watershed's Workforce members access ePHI during an emergency.

(5) Receive direction from the Chief Executive Officer or designee to invoke Watershed's Disaster Recovery Plan; and

(6) Set up operations at an alternative site, if used.

iii. As the emergency mode operations continue, continuously evaluate the protection of the security of ePHI and revise as necessary to ensure protection.

iv. The Security Officer or designee will determine if elevated access privileges are needed for members of the Workforce and will direct and document the provision and level of such access, as appropriate to the event, expected duration, and circumstances.

v. On resumption of normal operations, the Security Officer or designee will ensure elevated privileges are removed.

6. Review, Testing, and Revision of Contingency Plan.

a. The Security Officer, or designee, in coordination with the approval of the CEO and senior management, will review and conduct, at least annually and/or when there are significant changes to the environment, one or more of the following exercises to test Watershed's Contingency Plan to include backup, disaster recovery, and emergency mode operations plans:

i. Paper test. A detailed walk-through of the plan that typically includes tasks such as validating the vendor call and notification lists and reviewing end user procedures;

ii. Tabletop exercises of response to specific scenarios;

iii. Limited scope test. A test of one or more components of the Disaster Recovery Plan:

(1) Typical test tasks include using backup tapes to restore selected information systems at a remote recovery facility or on test machines within Watershed; and testing communications between Watershed and its alternate/recovery facility or facilities;

iv. Technical restoration activities;

v. Supplier facility and or service tests; or

vi. Complete drills of the plan components.

b. The Security Officer or designee will formally document the results of such tests and present to appropriate Watershed management, and

i. Revise the Contingency Plan (1) to address any deficiencies discovered during the testing activities. Focus on improvements to role and responsibility definitions, processes, practices and strategies; and (2) as needed if there are important changes involving personnel, contact information, suppliers, legislation, or business risks, processes or strategies.

7. Applications and Data Criticality Analysis Procedures.

a. Leverage the results of any recent Business Impact Analyses or Risk Assessments to complete the analysis (Refer to *Security Policy # 1, Security Management Process*, Risk Analysis Specification Section).

b. Identify the assets (e.g., hardware, software, applications, information sets) involved in critical business processes that receive, process, store, or transmit ePHI.

   i. Identify the dependencies between these systems.

   ii. Identify and determine the likelihood of risks that threaten Watershed’s information systems and data.

   iii. Identify and document the impact these risks have to Watershed’s services, processes and business objectives if specific critical information systems are unavailable for different periods of time (e.g. hours, days).

   iv. Prioritize Watershed’s information systems according to their criticality to Watershed’s ability to function at normal levels.

   v. Define information sets to categorize criticality rating.

c. Define impact levels for criticality, considering the desired levels of:

   i. Integrity – The determination that ePHI is not changed without authority.

   ii. Availability – The ePHI is available where and when needed to perform the functions of the organization.

   iii. Confidentiality – The ePHI is protected against unauthorized disclosure, theft or compromise.

d. For each business process and/or supporting software application/data set and infrastructure service, define the Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Data Loss Events (DLEs) that may adversely affect that business process.

e. Use the RTOs, RPOs and DLEs to prioritize the order of recovery for the ePHI systems, applications and data.

8. Responsibilities.

   a. The Security Officer or designee is responsible for ensuring a Data Backup Plan is in place for all ePHI held by Watershed. The plan will be coordinated with *Security Policy #13, Device and Media Controls,* Data Backup and Storage procedures to ensure complete coverage.

   b. The Security Officer or designee is responsible for coordinating a Disaster Recovery Plan for ePHI with other Disaster Recovery and Business Continuity Plans developed by Watershed.

   c. The Security Officer or designee is responsible for coordinating an Emergency Mode Operations Plan and procedures to enable continuation/continuity of critical business processes for the security of ePHI while Watershed is operating in emergency mode.

   d. The Security Officer or designee is responsible for implementing procedures to periodically test and revise contingency plans.

   e. The Security Officer or designee is responsible for ensuring a formal, up-to-date Business Impact Analysis is performed and available in support of other contingency plan components.

9. The Security Officer or designee, in coordination with Human Resources Department, will ensure that all Workforce members who administer processes pursuant to the policy and procedure are properly trained.

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 (a) (7)(i) – Standard: Contingency Plan.
2. 45 C.F.R. §164.308 (a) (7)(ii) – Implementation specifications.

Internal:

1. Security Policy #1, Security Management Process
2. Security Policy #13, Device and Media Controls
3. 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
5/10/2024	Nicole Montagnet	10.0	Reviewed and updated by Privacy & Security Officer

NIST CSF Subcategory & Control Mapping

Contingency Plan:
Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision Procedures, & Applications and Data Criticality Analysis

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(7)(ii)(E)	🟦	ID.AM-2: Software platforms and applications within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8
164.308(a)(7)(ii)(E)	🟦	ID.AM-5: Resources	NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
164.308(a)(7)(ii)(C) & (E)	🟦	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
164.308(a)(7)(ii)(C) & (E)	🟦	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
164.308(a)(7)(ii)	🟦	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	NIST SP 800-53 Rev. 4 PM-11, SA-14
164.308(a)(7)(i) & (ii)(E)	🟦	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(a)(7)	🟦	ID.BE-5: Resilience requirements to support delivery of critical services are established	NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
164.308(a)(7)(ii)(E)	🟦	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
164.308(a)(7)(ii)(E)	🟦	ID.RA-4: Potential business impacts and likelihoods are identified	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
164.308(a)(7)(ii)(D) & (E)	🟦	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
164.308(a)(7)(i) & (ii)(C) & (E)	🟦	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
164.308(a)(7)(i) & (ii)(A)	🟪	PR.AC-2: Physical access to assets is managed and protected	NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
164.308(a)(7)	🟪	PR.DS-4: Adequate capacity to ensure availability is maintained	NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(7)	🟪	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
164.308(a)(7)(ii)(D)	🟪	PR.IP-10: Response and recovery plans are tested	NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
164.308(a)(7)(ii)	🟪	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
164.308(a)(7)(i) & (ii)(C)	🟪	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
164.308(a)(7)(ii)(D)	🟪	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
164.308(a)(7)	🟪	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	NIST SP 800-53 Rev. 4 CP-2, IR-8
164.306(e)	🟨	DE.DP-3: Detection processes are tested	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM- 14, SI-3, SI-4
164.308(a)(7)(ii)	🟩	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
164.308(a)(7)(ii)(D)	🟩	RC.IM-1: Recovery plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(7)(ii)(D)	🟩	RC.IM-2: Recovery strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(7)	🟥	RC.RP-1: Recovery plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
164.308(a)(7)(ii)	🟥	RS.AN-2: The impact of the incident is understood	NIST SP 800-53 Rev. 4 CP-2, IR-4
164.308(a)(7)(ii)	🟥	RS.CO-1: Personnel know their roles and order of operations when a response is needed	NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
164.308(a)(7)	🟥	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(7)(ii)(D)	🟥	RS.IM-1: Response plans incorporate lessons learned	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
164.308(a)(7)(ii)(D)	🟥	RS.IM-2: Response strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(7)(i) & (ii)	🟥	RS.RP-1: Response plan is executed during or after an event	NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR- 8