Incident Response and Plan		**POLICY #6.1**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program POLICY 6.1 v. 9 Incident Response and Plan	3/1/2014	**5/10/2024**

Purpose

The Incident Response and Plan (Plan) is the primary source for processes for handling Security Matters involving various data classifications of electronic and hard copy information. This Plan was developed pursuant to applicable state and federal privacy and security breach laws, HIPAA Regulations, and Watershed Privacy, Breach, and Security Policies and Procedures, additionally taking into account information privacy, security and confidentiality agreements with Customers and third-party hosting services.

Applicability

This Plan applies to all Watershed workforce members, information systems, data, and networks and any person or device that gains access to these systems or data.

Definitions

For definitions of capitalized terms or phrases, please refer to *Privacy, Security and Data Breach Notification Glossary* and Appendix B.

Incident Response Team (IRT)

1. The IRT is a cross-functional team that is responsible for leading Watershed's response to security and privacy-related matters. All individuals involved in investigating a security matter should maintain confidentiality unless the Cybersecurity Oversight Committee authorizes information disclosure in advance.
    a. The IRT will primarily address significant security matters impacting systems, operations, and Customer data as well as any high-visibility security matters, regardless of the affected number of individuals or Customers.
    b. Members of the IRT must be prepared to assist in the various stages of the investigation (Appendix A, Internal Support).
    c. IRT participants include the following, as available and as depending on the circumstances: The Privacy Officer and Security Officer; a designated member from Technology, Human Resources, Marketing/Communications, Sales, and Finance; Legal Counsel; Senior Management (CEO, COO, President, CTO); designated Internal Support; and any other person deemed appropriate.

d. Each member of the IRT will bring subject matter expertise to aid Watershed with mitigating the situation and complying with any regulatory and/or contractual requirements.

e. Additional representation, depending on the severity, may also include outside counsel, third-party hosting services (e.g., AWS), insurance carriers, public relations, mailing vendor, forensics services, call center vendors, or identity theft/credit monitoring services.

f. IRT members are responsible for:

   i. Making sure that all Workforce members understand how to identify and report a suspected or actual security matter. The Privacy Officer and Security Officer, in consultation with the IRT, are the only ones with authority to designate the type of security matter.

   ii. Notifying Customers, in accordance with contractual obligations, or other relevant third parties, as required;

   iii. Determining if external support should be consulted to augment the Investigation (Appendix A, External Support).

   iv. Overseeing and participating in investigation activities.

   v. Determining if policies, processes, technologies, security measures, controls, or third-party hosting agreements need to be updated to avoid a similar security matter in the future, and whether additional safeguards are required in the environment where the situation occurred.

   vi. Determining whether the Board of Directors should be notified, and reporting to the Board, as appropriate.

Procedures

1. **Preparation.** Preparation includes those activities that enable the IRT to respond to a security matter. Preparation also implies that the affected departments have instituted the controls necessary to recover and continue operations after a security matter is discovered. Analyses from prior security matters should form the basis for continuous improvement of this stage.

   The objective of preparation is to maintain and improve incident response capabilities and minimize the likelihood of security matters through effective management of third-party hosting services, systems, networks, applications and processes that ensure the confidentiality, integrity, and availability of Watershed and Customer data**.**

2. **Detection**. Detection is the discovery of the security matter with security tools or notification by an inside or outside party about a suspected security matter. The objective of detection is to confirm, classify, categorize, scope, and prioritize suspected security matters.

   a. All suspected high severity security matters must be reported directly to the Security Officer or IRT immediately by email (preferred), instant messaging, text, or phone.

   b. Watershed will identify and react to security matters across common attack vectors and utilize these common vectors to define more specific incident procedures. Common attack vectors are manners of attack which include external/removable media, attrition (DDoS, brute force, etc.), website or web-based application exploits, phishing, spear phishing, impersonation, improper usage, and loss or theft of equipment or data, policy and process violations.

c. Signs of a security matter must be followed-up on to monitor and if possible, implement changes to prevent further damage.

d. Common sources of identifying a security matter are:

   i. Reporting by workforce member

   ii. Intrusion Detection System / Intrusion Prevention System

   iii. Security information and event management system

   iv. Endpoint protection

   v. Third party monitoring services

   vi. Operating system logs, service logs, and/or application logs

   vii. Network device logs or network flow data

3. **Triage.** Triage is the phase where the Privacy Officer and/or Security Officer, or designee, as appropriate, will conduct an initial screening to determine the severity of the security matter or complaint to:

a. Communicate as soon as practicable to activate the IRT, if applicable, regarding a security matter:

   i. Determine timing for notifying Senior Management and Customers (pursuant to contractual obligations), if applicable;

b. Set priorities for next steps:

   i. Defining the types of indicators that may be a security matter to be investigated;

   ii. Who among the team will determine the criticality and immediate response actions for a security matter;

   iii. The team member who will record and report the investigation activities;

   iv. Key steps to be taken when a security matter begins, and if/when it escalates;

   v. Determine whether the security matter is grave enough to warrant some type of disaster recovery process;

   vi. Determine whether Customer data is impacted and coordinate appropriate response(s);

   vii. Determine whether a Workforce member is responsible for the security matter, and if so, implement measures to minimize compromise or damage; and

   viii. Assess the risk of continuing operations, consulting with system owners and/or managers as appropriate.

4. **Incident Analysis**. The objective of Incident Analysis is to identify indicators of compromise, determine root cause, and take appropriate actions. The effectiveness of the analysis relies upon the knowledge and capabilities of the IRT. Many of these steps will take place concurrently.

    a. The Security Officer/Privacy Officer must **perform an analysis** immediately to validate security matters or indicators of compromise. The team will collect all relevant data for analysis and determine the scope, source, and how the situation occurred:

        i. The nature of the suspected security matter, including:

            (1) Suspected security matter type (e.g., administrator- or user-level compromise, denial of service, malicious logic such as virus and worms, unauthorized access attempt, social engineering);

            (2) Suspected method of compromise (i.e., tools or approaches used); and

            (3) Vulnerabilities exploited;

        ii. The extent of the security matter and any immediate steps to contain it;

        iii. The effect on Confidentiality, Integrity or Availability of the electronic information; and

        iv. If inappropriate disclosure of electronic information is suspected:

            (1) The data classification;

            (2) The number of records involved;

            (3) The types of data involved;

            (4) The person or entities to whom disclosed; and

            (5) Any mitigating steps to contain the disclosure (e.g. contact with the recipient to arrange return or destruction of the data).

        v. If it is determined that a security matter did not occur, the Security Officer/Privacy Officer or designee will document this determination.

    b. The Security Officer will, with the approval of the IRT, and if appropriate, engage the services of outside specialists to aid in investigation and mitigation.

    c. **The IRT is solely responsible for notifying the Board of Directors** of any confirmed security matter, if they have not yet been made aware and keep them appraised of the ongoing investigation and mitigation efforts. The notification must:

        i. Describe the nature of the security matter including where possible, the data classification categories and an approximate number of individuals concerned.

        ii. Communicate the details for point of contact point for the IRT team lead.

        iii. Describe the likely consequences of the security matter.

iv. Describe the measures taken, or proposed to be taken, to address the security matter, including, where appropriate, measures to mitigate its possible adverse effects.

d. If applicable, **notify other internal or external (i.e., Customers) stakeholders**. If the terms of a Business Associate Agreement have been violated, the COO or Privacy Officer, in consultation with outside counsel if deemed necessary by management, will comply with the requirements set forth in *Privacy Policy #11, Business Associate Contracts and Other Arrangements* and the Business Associate Agreement, to notify the Customer.

e. The Privacy Officer, and outside counsel if deemed necessary by management, in consultation with the Security Officer and the IRT will determine if notification is required in accordance with Watershed's Breach Notification Policies and Procedures:

i. Determine the "probability of compromise" with respect to Watershed's breach risk assessment policy as set forth in *Breach Policy #2, Breach Risk Assessment*.

ii. Determine whether notifications are required under the HIPAA Breach Notification Rule and *Breach Policy #2, Breach Risk Assessment*, using the ***Watershed Reporting & Assessment Form***.

(1) If notification is required, the Privacy Officer or designee will contact the Customer's Privacy Office, Security Office, or other contact designated in the Customer contract within the time outlined in the Business Associate Agreement (or other written agreement with the Customer) regarding the details of the security matter; and if required by the Customer Contract, Watershed will draft and provide a report to Customer.

iii. Determine if notification to affected Individuals is required.

(1) Immediately begin to identify any affected Individuals, as required, and the information that was used or disclosed; and

(2) The Privacy Officer or designee will, at the direction of the Customer, as applicable, respond directly to the affected Individual in accordance with *Breach Policy #3, Breach Notification Requirements* and any other applicable federal or state laws or contractual obligation.

5. **Containment, Eradication, and Recovery**. The objective of Containment, Eradication, and Recovery is to minimize loss, theft of information, or service disruption. Response to the security matter must be prioritized to first prevent a Breach of Confidential Information of Customers, PII and PHI, second to prevent personal data that is breached from becoming rendered intelligible, thirdly to minimize the number of data subjects and data records that are breached, and finally to minimize the adverse effects to the data subjects.

a. **Containment.** Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated. The objective of the containment phase is to limit the extent to which the security matter can cause harm.

i. Once the nature, scope, and origin of the security matter have been determined, the Security Officer/Privacy Officer, or designee, in consultation with the IRT as applicable, will be responsible for making all necessary decisions to contain the security matter. For example, for miscommunicated information, retrieve or confirm destruction of the information using the sample provided in Appendix C.

ii. Evidence gathering will be performed in such a way as to preserve the chain of custody and will comply with all applicable laws and regulations.

iii. Following the implementation of the containment strategy and allowing for sufficient time to measure its effectiveness, the IRT must be prepared to communicate as required to the affected Customers, individuals (if required by contract and applicable to PHI), and other required parties.

b. **Eradication**. Eradication efforts involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

i. Eliminate components of the security matter, such as, deleting malware and disabling compromised accounts.

ii. Identify, mitigate, and remediate the vulnerabilities that were exploited.

iii. It is extremely important to identify all affected hosts that were impacted by the security matter to ensure complete eradication and remediation has taken place.

c. **Recovery**. Recovery is the analysis of the security matter for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training:

i. Recovery efforts for security matters will involve the restoration of affected systems to normal operation, and any notifications to and oversight of any recovery activities of applicable third-party hosting service providers. This is dependent upon the type of security matter experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host based security.

ii. Restore affected systems using the last uncompromised backup.

iii. Recommend and/or make changes necessary to address vulnerabilities exploited with respect to the security matter.

6. **Remediation**. Remediation is the post-security matter repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are contractual or regulatory requirements for reporting the security matter (and to which outside parties) will be made at this stage. Apart from any formal

reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the security matter.

It is important to implement higher levels of monitoring and logging on both the systems affected by the security matter, Watershed infrastructure, and third-party hosted environments, as they are likely to be the target of subsequent attacks.

a. The Security Officer/Privacy Officer, or designee, in consultation with the IRT as applicable, will identify and oversee the development and implementation of any required remediation or corrective action plans to reduce the possibility of a reoccurrence.

b. The Security Officer/Privacy Officer or designee will monitor and/or audit to ensure the mitigation and remediation plans are in place, are working, and effective:

    i. A remediation plan may include changes to facility access, data access, data security, policies and procedures, training material, and/or suspension or termination of a Workforce member;

    ii. Obtain verification of destruction or return of the PHI, where applicable.

c. Watershed's Human Resources will be notified of any potential or expected sanctions that may need to be applied, as described in *Privacy Policy #4, Reporting Violations, Mitigation, and Sanctions*, and *Security Policy #1, Security Management Process*, Sanctions Section.

d. Identify any needed changes to Watershed's policies and procedures and develop a plan to update them.

    i. Communicate to the Watershed Workforce any changes in policies and procedures using any of the following methods:

        (1) Sending email communications; or

        (2) Conducting training sessions (live or recorded).

    ii. Change passwords used on affected systems and/or networks as necessary.

7. **Documentation**. All activities and findings will be recorded in a format that ensures an accurate record and will be maintained in accordance with Watershed's document retention policies. Documentation may include: a description and nature of the security matter, the data classification categories involved, and/or an approximate number of individual or Customer records exposed or impacted. If ePHI is involved relating to individuals, documentation as required will be made in the Accounting of Disclosures log.

8. **Post-Incident Activity and Review**. Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security matter. The objective of post-incident activity and review is to better handle future security matters through utilization of reports, "lessons learned," and after-action activities, or mitigation of exploited weaknesses to prevent similar security matters from occurring in the future. Post-incident activities will be incorporated into future training opportunities for all parties involved in the security matter.

a. A post-incident report will be developed that describes the measures taken or proposed to address the security matter, including measures to mitigate any adverse effects.

   i. The IRT will document lessons learned, corrective actions, and areas for improvement, such as:

      (1) Timeline and circumstances of the security matter and response;

      (2) Processes and procedures and any identified gaps;

      (3) Information sharing with internal and external parties, including law enforcement if appropriate;

      (4) Precursors or indicators that should be monitored to help detect future security matters;

      (5) Additional tools and/or resources required to detect and respond effectively to future security matters; and/or

      (6) Changes in contracts with third party hosting suppliers and/or Customers.

   ii. The Post Incident Activity and Review should document each security matter and develop metrics that can be used over time to measure:

      (1) Time and cost of each security matter;

      (2) Justify additional funding for incident response;

      (3) The overall success of the IRT;

      (4) Identify systemic weaknesses and threats; and/or

      (5) Identify changes in incident trends.

Enforcement

Violations of this Plan will result in sanctions in accordance with Watershed sanctions Plan. This may include suspension or loss of the violator's user 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

Watershed's Privacy Officer is responsible for ensuring this version of the Plan, together with any forms and other documentation created or obtained in accordance with the Plan, 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)(6)(i) – Standard: Security incident procedures.

2. 45 C.F.R. §164.308(a)(6)(ii) – Implementation specification: Response and Reporting.
3. 45 C.F.R. §164.530(f) – Standard: Mitigation.

Internal:

1. Reporting & Assessment Form
2. Security Policy #1, Security Management Process
3. Privacy Policy #4, Reporting Violations, Mitigation, and Sanctions
4. Privacy Policy #8, Accounting of Disclosures
5. Privacy Policy #11, Business Associate Contracts and Other Arrangements
6. Breach Policy #2, Breach Risk Assessment
7. Breach Policy #3, Breach Notification Requirements
8. Security Policy #22, Data Governance and Data Classification

External:

1. Current Administrative Simplification Regulations
2. Refer to *NIST CSF Subcategory & Control Mapping* located in *Security Policy #6, Security Incidents*

Appendices

Appendix A: Incident Response Team

Internal Support

Department/Title	Name	Contact
Privacy Officer	Nicole Montagnet	Nicole.montagnet@watershedhealth.com
Security Officer	Mike Neal	Mike.neal@clearwatersecurity.com
Human Resources representative	Scott Snodgrass	Scott.snodgrass@watershedhealth.com
Senior Management	Chip Grant, CEO Lisa Stanley, COO	Chip.grant@watershedhealth.com Lisa.stanley@watershedhealth.com
Finance representative	Robbie Fuertes	Robbie.fuertes@watershedhealth.com
Marketing/ Communications representative		
Sales representative		
Technology representative	Florin Micle, CTO	Florin.micle@watershedhealth.com
Legal Counsel	Steve Wood (outside counsel) Nicole Montagnet (in-house)	sfwood@bakerdonelson.com Nicole.montagnet@watershedhealth.com

External Support (As Applicable)

Vendor Name	POC	Phone	Email
Forensics			
Marketing & Media Relations			
Identity Theft/Credit Monitoring			
Insurance Carrier			
Eustis Marsh McLennan Agency	Moses Swent	985-856-8028	Moses.swent@marshmma.com
Outside Counsel			
Baker Donelson	Steve Wood	615-260-3650	sfwood@bakerdonelson.com
Third-Party Service Providers			
AWS Microsoft Online Svcs			
Law Enforcement (Local or Federal)			
FBI – New Orleans	Douglas Williams	504-861-3000	
US-CERT			
United States Computer Emergency Readiness Team (US-CERT)		(888) 282-0870	Reporting URL: https://www.us-cert.gov/report?

Appendix B: Additional Definitions

Common Categories of Cyber Incidents

Incident Type	Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a university network, system, application, data, or another resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Malware that has been successfully quarantined by antivirus (AV) software need not be reported.
Improper or Inappropriate Usage	When a person violates acceptable computing policies.
Suspected PHI Breach	If a security matter involves protected health information (PHI) must be reported even if merely suspected.
Suspected loss of Sensitive Information	A security matter that involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, where the cause or extent is not known.

Source: NASA Information Security Incident Management

Impact Definitions

	Potential Impact		
Security Objective	**Low**	**Medium**	**High**
Confidentiality: Assurance against unauthorized restrictions on information access and disclosure, including means protection of personal privacy and proprietary information.	The unauthorized disclosure of information is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity: Assurance against improper modification or destruction of information that ensures non-repudiation and authenticity.	The unauthorized modification or destruction of information is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Availability: The timely and reliable access to and use of information	The disruption of access to or use of information or an information system is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an the information system is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Source: FIPS Publication 199

Appendix C: Sample Attestation

I [INSERT NAME] attest that the information I received in error from Watershed was not further used or disclosed to anyone, has been returned/destroyed/deleted, and that I have not retained any copies. This includes the destruction by shredding, deletion of any electronic copies downloaded to a computer/device, or the deletion of email copies from inboxes and deleted items/trash folders.

Print Name: ______________________________ Date: ____________

Signature: ______________________________

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
5/4/2023	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