

HIPAA Security Rule



POLICY & PROCEDURE Security Matters and System Incidents		POLICY #6
SUPERCEDES POLICY:	EFFECTIVE:	LAST REVIEWED:
Privacy and Security Compliance Program Policy & Procedure 6 v.9 Security Incidents	3/1/2014	5/10/2024

Purpose

To formalize procedures for reporting and responding to security incidents, whether accidental or intentional.

Consult with Legal Counsel for any applicable state privacy or breach laws or contractual obligations 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 to be aware of this policy and adhere to the given direction and guidance.

Definitions

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

Policy

It is the policy of Watershed that security matters involving Electronic Protected Health Information (ePHI) and system incidents are identified and addressed promptly, that appropriate measures are taken to mitigate any further accidental or intentional security matters or system incidents to reduce the possibility of harm or re-occurrence and that appropriate sanctions are imposed, as applicable.

Procedures

1. Security Matters. A security matter is defined as a security incident that affects the actual or potential jeopardization of the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. All security matter reporting and response activities will be conducted strictly on a need-to-know basis.
 - a. Responsibilities of Workforce Members

HIPAA Security Rule



- i. Workforce members suspecting a security matter will immediately notify their Supervisor/Manager and Security Officer including holidays and weekends.
 - ii. Workforce members will complete and submit the Watershed Security Matter Reporting Form (found on the staff website) immediately to their Supervisor/Manager and the Security Officer (or designee).
 - iii. Workforce members shall be trained regarding appropriate response and reporting procedures of security matters.
 - b. Responsibilities of Security Officer or designee.
 - i. Security Officer or designee will review the submitted Security Matter Reporting Form and investigate each suspected or confirmed security matter.
 - ii. Initiate a triage process, in consultation with the Privacy Officer as applicable, to conduct an initial screening to determine the severity of the suspected or confirmed security matter and determine the requirements for further investigation.
 - iii. Conduct or oversee a detailed investigation to ascertain the circumstances of the suspected or confirmed security matter.
 - iv. Activate the *Incident Response Plan* and Incident Response Team (IRT), as applicable. Refer to the *Incident Response Plan in Security Policy 6.1* for additional details.
 - v. Test the effectiveness of the Incident Response Plan periodically.
- 2. System Incidents. A system incident is defined as an event that causes disruption to or a reduction in quality of a system which requires an emergency response.
 - a. Upon detection of a security incident, the Workforce member who detected the disruption will immediately notify the CEO.
 - b. Either the CEO or the Workforce member who detected the disruption will send a slack to the 911 slack channel with an invitation to join a 911 Zoom call.
 - c. A System Incident Manager is designated who appoints a Scribe, Problem Manager, and coordinates responders to restore service as quickly as possible.
 - d. The Tech Lead runs the tech team to diagnose and fix the disruption.
 - e. The Communications Manager, working closely with the Customer Support Lead and Social Media Lead, communicates the progression of service restoration.
 - f. The Scribe records key information, maintains an incident timeline, assists with the debrief report.
 - g. Diagnosis, communication, and escalation continue until resolution.
 - h. Upon resolution, when the affected service resumes functioning in its usual way, the Problem Manager performs a debrief, describes findings, makes recommendations and next steps, and completes the debrief report.

HIPAA Security Rule



3. Malware - Methods to notify the appropriate parties and respond to malware.
 - a. Exception reports are generated automatically by an auditing control system if defined thresholds are reached, enabling real-time monitoring of system resources and attempted system integrity incidences.
 - b. Automatic reports are generated weekly showing trends and historical statistics for the system administrators.
 - c. Each server is maintained at the latest stable patch level pertaining to the operating system and has anti-malware software installed and running at the latest definition level receiving updates set for automatically times.
 - d. Anti-malware scans have monitoring turned on with logs showing number, types and disposition of any attempted or successful infections.
 - e. In the case of a potential threat identified at the network server level, support teams will work with Information Security to determine the best option for resolution.
 - f. If Watershed maintains any workstations, the Support Teams are responsible for notifying Information Security when they detect malware.
 - g. All incidents of a suspicious nature are escalated to the Security OfficeThe following procedures are used to notify the appropriate parties and respond to Health Insurance Portability and Accountability Act (HIPAA) security matters:
 - h. Exception reports are generated automatically by an auditing control system if defined thresholds are reached. This enables real-time monitoring of attempted system integrity incidences.
 - i. Automatic reports are generated weekly showing trends and historical statistics for the system administrators.
 - j. All matters of a suspicious nature are escalated to the Security Officer.
4. Methods to notify the appropriate parties and respond to system incidents:
 - a. Exception reports are generated automatically by the auditing control system if defined thresholds are reached. This enables real-time monitoring of system resources and usage.
 - b. Automatic reports are generated weekly showing trends and historical statistics for the system administrators.
 - c. All incidents related to a system outage or the unavailability for any reason of access to electronic information are escalated to the Security Officer.

HIPAA Security Rule



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

Watershed's 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)(6)(i) – Standard: Security incident procedures.
2. 45 C.F.R. §164.308(a)(6)(ii) – Implementation specification: Response and Reporting.

Internal:

1. Incident Response Plan
2. Reporting & Assessment Form


External:

1. [Current Administrative Simplification Regulations](#)
2. Refer to *NIST CSF Subcategory & Control Mapping* at the end of this document

HIPAA Security Rule



Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	<div>DocuSigned by:  9418DCC7CF3D47D...</div>
(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

HIPAA Security Rule



NIST CSF Subcategory & Control Mapping

Security Incident Procedures: Response and Reporting		
HIPAA	Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(6)(ii)	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)(6)	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)(6)(ii)	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)(6)(ii)	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
164.308(a)(6)	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
164.308(a)(6)(i)	DE.AE-2: Detected events are analyzed to understand attack targets and methods	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
164.308(a)(6)(ii)	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
164.308(a)(6)(ii)	DE.AE-4: Impact of events is determined	NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
164.308(a)(6)(i)	DE.AE-5: Incident alert thresholds are established	NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
164.308(a)(6)(ii)	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
164.308(a)(6)(i)	RC.CO-1: Public relations are managed	None listed
164.308(a)(6)(i)	RC.CO-2: Reputation after an event is repaired	None listed

HIPAA Security Rule



HIPAA		Cybersecurity Framework Subcategory	NIST Control Mapping
164.308(a)(6)(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)(6)(ii)		RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4
164.308(a)(6)(ii)		RS.AN-2: The impact of the incident is understood	NIST SP 800-53 Rev. 4 CP-2, IR-4
164.308(a)(6)		RS.AN-3: Forensics are performed	NIST SP 800-53 Rev. 4 AU-7, IR-4
164.308(a)(6)(ii)		RS.AN-4: Incidents are categorized consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR- 8
164.308(a)(6)(i)		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)(6)(ii)		RS.CO-2: Events are reported consistent with established criteria	NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
164.308(a)(6)(ii)		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
164.308(a)(6)		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)(6)		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	NIST SP 800-53 Rev. 4 PM-15, SI-5
164.308(a)(6)(ii)		RS.MI-1: Incidents are contained	NIST SP 800-53 Rev. 4 IR-4
164.308(a)(6)(ii)		RS.MI-2: Incidents are mitigated	NIST SP 800-53 Rev. 4 IR-4
164.308(a)(6)(ii)		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
164.308(a)(6)(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