

# HIPAA Security Rule



<b>POLICY &amp; PROCEDURE</b> <b>Email Security</b>		<b>POLICY #23</b>
<b>SUPERCEDES POLICY:</b>	<b>EFFECTIVE:</b>	<b>LAST REVIEWED:</b>
Privacy and Security Compliance Program Security Policy & Procedure 23 v.9 Email Security	3/1/2014	5/10/2024

## Purpose

To ensure that Watershed Health, Inc. (Watershed) email systems are used only for authorized purposes and that certain rules are followed for the use of email in general, and specifically, for transmission of electronic Protected Health Information (ePHI). Watershed will implement this email policy and ensure that the requirements are followed and enforced.

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

Watershed provided email systems must be used for official business only. Personal email will not be used for official company business.

Watershed owns any communication sent via Watershed email accounts or that is stored on company assets (e.g., Webmail). Management and other authorized staff have the right to access any content in the email systems and therefore workforce members must not have any expectation of privacy related to emails.

## Procedures

1. Watershed provided email accounts shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, appearance, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin. Workforce members who receive any emails with such content from any Watershed employee must report the matter to their Supervisor/Manager immediately.

# HIPAA Security Rule

- 
2. Workforce member responsibilities.
    - a. Workforce members must not click on any links or open attachments in any emails whose senders they do not recognize.
      - i. Receipt of an email of this type must be reported by utilizing existing technical tools, such as PhishNotify.
        - (1) The Security Officer, Privacy Officer or designee will relate, as needed, additional instructions to Workforce members who report a suspicious email.
      - ii. **Important:** This requirement must specifically be included in the Watershed's Security Awareness Training program so that all Workforce members are aware of the dangers of potential phishing attempts or malware.
    - b. Workforce members must not install any unauthorized plug-ins on their email clients.
    - c. Watershed's confidential or extremely sensitive information must not be sent via email unless there is a specific official business need and authorized by management. Any transaction of such sensitive information via email must require use of approved password or encryption methods or technologies (refer to *Security Policy #22, Data Governance and Data Classification* for a description of information that must adhere to these requirements).
      - i. Workforce members should work with their Supervisors/Managers to relocate confidential or extremely sensitive information received via email to a secure location that conforms to the requirements outlined in *Security Policy #22, Data Governance and Data Classification* and fully delete any such information from email.
    - d. Workforce members should not forward or auto-forward Watershed's email to external/third party email systems (e.g., Gmail or other personal email accounts).
  3. Watershed's email systems must have appropriate spam, virus, or malware filters implemented.
  4. Software or patch updates on email systems must be applied in a timely manner.
  5. Reporting.
    - a. Workforce members must report any security incident involving the impermissible disclosure of confidential or extremely sensitive information via email to the Security Officer and the Privacy Officer, or designee, as described in *Security Policy #6, Security Incidents*.
  6. Watershed's Security Officer or designee must include the relevant end-user requirements of this policy within the organization's Security Awareness Training program which must be conducted at appropriate intervals (refer to *Security Policy # 5, Security Awareness and Training*).

# 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

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:

No specific regulatory standard or implementation specification listed in HIPAA.

### Internal:

1. Security Policy #5, Security Awareness and Training
2. Security Policy #6, Security Incidents
3. Security Policy #21, Mobile Device Security
4. Security Policy #22, Data Governance and Data Classification

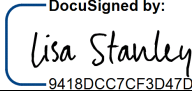
### External:

1. [Current Administrative Simplification Regulations](#)
2. Refer to *NIST Publications Reference Guide* for specific guidance

HIPAA Security Rule



Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	<div>DocuSigned by:  9418DC67CF3D47D...</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
5/17/2023	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