POLICY & PROCEDURE **Mobile Device Security & Management**		**POLICY #21**
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Security Policy and Procedure 21 v.9 Mobile Device & Security Management	3/1/2014	**5/10/2024**

Purpose

To safeguard electronic information, to include Electronic Protected Health Information (ePHI), on all mobile devices that create, receive, maintain, collect, store, process, or transmit such data, and implement reasonable physical and technical security safeguards for all mobile devices.

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

Mobile devices are defined as those devices that are designed to be mobile and which have electronic computing or processing capabilities. Examples of such devices include (but not limited to) laptop computers, Smartphones, and tablet devices such as iPads. The definition does not include removable storage media such as USB drives or jump drives. A separate policy (*Security Policy #13, Device and Media Controls*) addresses the physical security requirements for removable storage media.

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

Policy

Watershed will properly document and implement security protocols as it relates to the mobile device environments to comply with Data Governance Policies and Procedures and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Only approved mobile devices must be used to connect to Watershed's internal network (if available) or systems. At teleworking sites, this Policy is intended to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to Watershed's internal systems.

Procedures

1. Inventory. The Security Officer, or Designee, will maintain an inventory of IT assets that are authorized for storage of ePHI, in accordance with *Security Policy #3, Workforce Security*; and *Security Policy #4, Information Access Management*.
    a. Watershed maintains an inventory of IT assets including details of owners, serial number, asset tracking number, encryption status, type of asset, and operating system. The standard laptop configuration will be maintained, updated, and applied to individual equipment to provide up-to-date protection features to secure local information.
    b. The Security Officer or designee will perform annual reviews of the inventory of IT assets and will update this inventory during installations, equipment removals, and system changes.
    c. Watershed's Workforce members should not download or store ePHI on any mobile device without a specific business need and as authorized by appropriate management.
    d. All use of mobile devices must adhere to Security and any related employment or Human Resources policies.
2. Encryption. The Security Officer or designee will ensure that company-owned mobile devices containing ePHI have encryption activated on these devices (refer to *Security Policy #14, Access Controls*).
    a. Full disk encryption software is employed, such as Microsoft's BitLocker, Apple's FileVault, and/or Linux's dm-crypt.
    b. Remote access to/from ePHI on devices must be done in a secure manner so that unauthorized access to the information is not allowed during transmission.
3. Device-based Firewalls. The Security Officer or designee must ensure that company-owned devices (e.g., laptops, desktops) have appropriate software firewall activated (e.g., Windows Defender) and configured to block unauthorized programs or inbound or outbound communications.
4. Physical Security. Workforce members must always take reasonable measures to ensure physical security of all mobile devices to avoid loss or theft. This is especially true when the devices are used in public places and during travel. Workforce members will ensure that they adhere to *Privacy Policy #3, Safeguards*; and *Security Policy #12, Workstation Security* as it relates to physical security and transporting of devices.
    a. Watershed prohibits the use of (i) writable, removable media; and (ii) personally owned, removable media. Removable media includes USB Drives (flash or thumb drives), memory sticks, external hard drives, SSD drives, CDs, DVDs.
    b. In the event that Watershed transports physical media housing covered and/or confidential information, Watershed shall protect the media from unauthorized disclosure or modification by the appropriate application of at least one of the following:
        i. Use of locked containers;
        ii. Delivery by hand;

iii. Tamper-evident packaging (which reveals any attempt to gain access); or
iv. Splitting of the consignment into more than one delivery and dispatch by different routes.

5. Authentication. The Security Officer or designee will ensure that all company-owned mobile devices are configured with a form of device level authentication, such as a password, biometric identifier (e.g. fingerprint or facial recognition), or personal identification number (PIN) when the device is powered on.
6. Screen-lock. The Security Officer or designee will ensure that company-owned mobile devices are configured to lock after 20 minutes of inactivity. The Workforce member must be required to reenter the device authentication credentials in order to resume use of the device (refer to *Security Policy #14, Access Controls*).
7. Security Patches. The Security Officer or designee will ensure that the application of security patches on company-owned mobile devices is a high priority task among the list of Watershed's vulnerability management activities.
    a. Certain key "helper" applications that are frequently installed on most mobile devices should be set to automatically update as older versions of these programs may have security weaknesses that can be exploited by System Crackers. These include:
        i. Java Runtime Engine;
        ii. Adobe Acrobat; and
        iii. Internet browsers other than Internet Explorer or Edge, such as Firefox and Chrome.
8. Personally-Owned Smartphones and Tablets.
    a. Approval and User Agreement.
        i. If using a personal device, Workforce members must sign a BYOD user agreement..
    b. Security Patches and Updates.
        i. Workforce members are responsible for ensuring that any software updates or patch updates are applied in a timely manner to the device operating system issued by the vendor to address known and potential security weaknesses.
        ii. Workforce members are encouraged to configure their devices to do this automatically, if they are not configured to do so by default.
9. Reporting.
    a. If a company-owned or personally-owned mobile device that accesses or stores ePHI is lost, stolen, or damaged:
        i. The Workforce member must report any loss or theft of a mobile device immediately to his/her Supervisor/Manager and the Security Officer or designee.

ii. The *Watershed's Reporting & Assessment Form*, available on the Staff Website, will be completed to document the loss or theft.

10. Termination. If a Workforce member terminates employment with Watershed, or is terminated, all Watershed data and access to applications must be removed on or before their last day of employment; such removal shall be confirmed and documented by Watershed.
11. Security Awareness. The Security Officer or designee will ensure that security safeguards related to use of mobile devices are included in Watershed's Security Awareness program (refer to *Security Policy #5, Security Awareness and Training*).

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 #3, Workforce Security
2. Security Policy #4, Information Access Management
3. Security Policy #5, Security Awareness and Training
4. Security Policy #6, Security Incidents
5. Security Policy #8, Workstation Security
6. Security Policy #13, Device and Media Controls
7. Security Policy #14, Access Controls
8. Security Policy #22, Data Governance and Data Classification
9. Security Policy #23, Wireless Security

10. Security Policy #24, Email Security
11. Privacy Policy #3, Safeguards
12. Privacy Policy #7, Investigating Impermissible Uses and Disclosures

External:

1. Current Administrative Simplification Regulations
2. HHS Guidance – Guidance on Risk Analysis Requirements under the HIPAA Security Rule
3. Refer to *NIST Publications Reference Guide* for specific guidance

Document Control

APPROVED BY:		
Lisa Stanley	5/24/2024	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
5/17/2023	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

