1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Mobile Computing Device Security Policy

Version	Approval Date	Owner
1.1	December 13, 2019	Chief Information Security Officer

1. Purpose

To establish provisions for using, configuring, acquiring, accessing, maintaining, protecting, and securing mobile computing devices (e.g., smartphones, tablets, laptops, portable media, etc.). Devices are to be protected at all times, including travel to high risk locations, by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, secure configuration, and physical protections. HSX personnel are authorized to check and take reasonable action for malware and physical tampering of all mobile computing devices at any time.

2. Scope

This policy applies to mobile computing devices that connect to HealthShare Exchange. (HSX) network(s) and/or access HSX's confidential data.

All employees, interns, contractors, members, participants, users, and third parties utilizing mobile computing devices connecting to the HSX network, and/or accessing HSX confidential data, assume the responsibility for the security and privacy of information contained within.

3. Policy

Mobile Computing Device Policy:

- HSX shall manage and control use of mobile computing devices, and appropriate security measures shall be adopted to protect against the risks of using mobile computing devices. Mobile device management (MDM) shall be conducted by HSX through approved mobile device management applications.
- Transmitting HSX confidential data via text messaging technology shall only be allowed by the methods approved by the Chief Information Security Officer (CISO).

- Mobile computing devices that are personally owned by employees and contractors are the responsibility of the owner to ensure that if HSX information is being accessed on the device, that the device is compliant with HSX policy.
- The owner of any personally-owned mobile computing devices connected to HSX information assets (e.g. network, email system, website, etc.) is fully responsible for the behavior of all users of the mobile computing device, and for all data and network traffic accessed or transmitted to and from the mobile computing device, regardless of whether the owner is aware of the data and network traffic.
- Personally-owned mobile devices shall not be whitelisted for access to any HSX information assets other than [Redacted] and messaging applications (e.g., [Redacted]).
- Usage of mobile computing devices must comply with all international, federal and state laws, and HSX policies. Unauthorized disclosure of HSX confidential data may violate federal and/or state laws, accreditation standards, and/or ethical standards, and may cause injury. Unauthorized disclosure may result in disciplinary and/or legal actions being taken, including but not limited to termination of privileges and / or employment in accordance with the *Sanctions Policy* and the *Termination Policy*.
- Users shall have no expectation of privacy associated with any of the HSX enterprise data they store in or send through mobile computing devices.
- Users are responsible for ensuring mobile computing device applications and multimedia capabilities are not used to breach privacy and confidentiality according to the *Acceptable Use Policy.*
- To minimize security risks associated with mobile computing devices, all such equipment must be encrypted, password protected, and physically secured, minimizing the threat of loss or theft of the device itself and any confidential data contained therein.
- All devices that will store, transmit, and process confidential information must use mobile device management that enforces built-in detection and prevention controls.
- Approved mobile device management applications will be used for laptop management, and MDM will be used for smartphones that access an HSX approved application (see HSX Business Applications document).
- Operating System updates and security patches for mobile computing devices shall be kept up to date.
- All business mobile computing devices must be disposed of in accordance with the *Secure Disposal Policy* once they reach end of life.

Mobile computing devices shall be protected at all times including:

- **Physical Protection**: Users shall not leave mobile computing devices unattended in public areas (e.g., vehicles, hotel rooms, conference rooms, airports) even for a short period of time. Mobile computing devices shall be carried as hand luggage when

traveling and never checked as baggage or stored anywhere prohibiting immediate access or visual contact with the device.

- In the event that a mobile computing device is lost or stolen, the incident must be reported according to the *Incident Management Policy*.
- **Access Controls**: All mobile computing devices shall require authentication (e.g., password, pin number, biometric, etc.) and shall automatically time out after 5 minutes of inactivity. Any and all mobile computing devices shall be in compliance with HSX's Password Management Policy.
- **Encryption**: All mobile computing devices that receive, transmit, or store confidential data shall be encrypted according to the *Encryption Policy*.
- **Anti-Malware**: All mobile computing devices shall be compliant with the *Endpoint Protection Policy*.
- **Security Configuration**: If supported by the mobile computing device, remote wipe functionality shall be enabled in case of loss. Wireless access (e.g., W-Fi, Bluetooth) must be configured to request confirmation before establishing a connection.
- Users of mobile computing devices connected to HSX email must notify the CISO when the device is no longer in use. The CISO shall follow standard procedures to remotely delete HSX content from the device.
- HSX prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).

Network Connections:

- HSX shall monitor for unauthorized connections of mobile computing devices to the HSX Wi-Fi network on a quarterly basis.
- Mobile computing devices that remotely access the HSX network shall comply with the *Remote Access Policy*.
- Personally-owned mobile computing devices may connect to the HSX network and access HSX confidential data in accordance with this policy and associated procedures.
- If the CISO has reason to believe that a mobile computing device connected to the HSX network is using HSX information asset resources inappropriately, or is acting in violation of federal and state laws or regulations, network traffic to and from that mobile computing device shall be monitored. If justified, the mobile computing device shall be disconnected from the HSX network, and appropriate actions will be taken in accordance with the *Sanctions Policy* and federal and state law and regulations.
- The current approved application stores is limited to the Apple App Store. For any other application store needs, permission must be granted by a member of the IT Technical Operations team under direction of the CISO, and only a member of the IT Technical Operations team will be able to install the necessary authorized

application. Non-approved applications or approved applications not obtained through the application store is prohibited.

Security Awareness:

- Employees, interns and contractors using mobile computing devices shall be trained on the risks, the controls implemented, and their responsibilities.
- Users must agree to take responsibility for the security of their mobile computing device and the HSX data it contains.
- Users are not permitted to bypass, or attempt to bypass, security protections on mobile computing devices connected to the HSX network or HSX communication systems. This includes modifying vendor-provided operating system settings (i.e., "Jailbreaking" a device).
- Users shall be responsible for ensuring that HSX confidential data is only transmitted using approved/secure communication functions including HSX email.
- Business mobile computing devices issued for business purposes remain the property of HSX. When the business mobile computing device is allocated, the user assumes responsibility for physical security of the device and any HSX data contained within. Prior to leaving the employ of HSX, the user shall return the device.
- All mobile devices permitted for use through HSX's Bring Your Own Device (BYOD) program or a HSX-assigned mobile device shall allow for remote wipe by the HSX Privacy or Security Officer or shall have all company-provided data wiped by the HSX Privacy or Security Officer.

Mobile Code Protection:

- Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to policy.
- Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).
- A formal policy shall be in place for mobile code protection and to ensure protective measures including anti-malware software are in place and regularly updated.

4. Procedure

The following procedures apply to HSX internal operations only:

- Mobile Device Protection Procedures
- Wireless Network Security Procedures

5. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- The CISO shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

6. Definitions

For a complete list of definitions, refer to the *Glossary*.

7. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.308(a)(5)(ii)(B), HIPAA § 164.310 (b)
- HITRUST Reference: 01.x Mobile Computing and Communications, 09.k Controls Against Mobile Code
- PCI Reference: PCI DSS v3 1.4

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Management	**Approval Date**	December 13, 2019
Date Policy In Effect	December 13, 2019	**Version #**	1.1
Original Issue Date	March 9, 2017	**Last Review Date**	September 17, 2020 December 13, 2019 November 18, 2019

Related Documents	Acceptable Use Policy Encryption Policy Endpoint Protection Policy Glossary Incident Management Policy Password Management Policy Remote Access Policy Sanctions Policy Secure Disposal Policy Termination Policy