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

End User Computing Device Security Policy

Version	Approval Date	Owner
1.2	September 28, 2017	Information Technology

1. Purpose

To establish provisions for using, configuring, acquiring, accessing, maintaining, protecting, and securing end-user computing devices (e.g., smartphones, tablets, laptops, portable media, etc.).

2. Scope

This policy applies to end-user 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 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

End User Computing Device Policy

- HSX shall manage and control use of end-user computing devices, and appropriate security measures shall be adopted to protect against the risks of using end-user computing devices.
- Transmitting HSX confidential data via text messaging technology shall only be allowed by the methods approved by the Chief Information Security Officer (CISO).
- End-user computing devices that are personally owned by employees and contractors are the responsibility of the owner.
- The owner of any personally-owned end-user 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 end-user computing device, and for all data and

network traffic accessed or transmitted to and from the end-user computing device, regardless of whether the owner is aware of the data and network traffic.

- Usage of end-user 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 end-user computing devices.
- Users are responsible for ensuring end-user 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 end-user 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.
- Operating System updates and security patches for end-user computing devices shall be kept up to date.
- All business end-user computing devices must be disposed of in accordance with the *Secure Disposal Policy* once they reach end of life.
- Allowed/permitted software shall be reviewed upon a case-by-case basis by the Senior Director of Information Technology.

End User Computing Devices Shall be Protected at All Times Including

- **Physical Protection**: Users shall not leave end-user computing devices unattended in public areas (e.g., vehicles, hotel rooms, conference rooms, airports) even for a short period of time. End-user 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 end-user computing device is lost or stolen, the incident must be reporting according to the *Incident Management Policy*.
- **Access Controls**: All end-user computing devices shall require authentication (e.g., password, pin number, passcode, biometric, etc.) and shall automatically time out after 15 minutes of inactivity.
- **Encryption**: All end-user computing devices that receive, transmit, or store confidential data shall have encryption enabled according to the *Encryption Policy*.
- **Anti-Malware**: All end-user computing devices shall be compliant with the *Endpoint Protection Policy*.

- **Security Configuration:** If supported by the end-user 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 end-user 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.
- Location Services: shall be enabled if supported by the end-user computing device.

Network Connections

- HSX shall monitor for unauthorized connections of end-user computing devices to the HSX network.
- End-user computing devices that remotely access the HSX network shall comply with the *Remote Access Policy*.
- Personally-owned end-user 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 an end-user 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 end-user computing device shall be monitored. If justified, the end-user 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.

Security Awareness

- Employees, interns and contractors using end-user 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 end-user computing device and the HSX data it contains.
- Users are not permitted to bypass, or attempt to bypass, security protections on end-user 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 end-user computing devices issued for business purposes remain the property of HSX. When the business end-user computing device is allocated, the user assumes responsibility for physical security of the device and any HSX data contained within.

End User Code Protection

- End-user code shall be authorized before its installation and use, and the configuration shall ensure that the authorized end-user code operates according to policy.
- Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of end-user code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).
    - This includes the required installation of a device management application, providing an additional layer of security by preventing program executions of unauthorized software programs in addition to other functionalities. The device management application operates in a deny-all, allow by exception policy to prevent the execution of unauthorized software on the information system and does so on all servers, workstations and laptops.
- A formal policy shall be in place for end-user code protection and to ensure protective measures including anti-malware software are in place and regularly updated.

4. Procedure

- Software Blacklisting

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 President

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 End-user Computing and Communications, 09.k Controls Against End-user Code
- PCI Reference: PCI DSS v3 1.4

Policy Owner	Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	Board HSX Management Team	**Approval Date**	September 28, 2017
Date Policy In Effect	May 13, 2015	**Version #**	1.2
Original Issue Date	May 13, 2015	**Last Review Date**	September 16, 2020 September 28, 2017
Related Documents	Acceptable Use Policy Encryption Policy Endpoint Protection Policy Glossary Incident Management Policy Remote Access Policy Sanctions Policy Secure Disposal Policy Termination Policy		