190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Wireless Network Security Policy

Version	Approval Date	Owner
1.1	December 11, 2019	Chief Information Security Officer

1. Purpose

To ensure the protection of HealthShare Exchange (HSX) enterprise data in wireless networks.

To ensure the protection of HSX network infrastructure that supports wireless access services.

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, third parties, and computing devices connecting to any HSX wireless network.

Telework and security requirements for wireless connections outside of HSX premises (e.g., home networks, hot spots, hotel networks, etc.) are outside the scope of this policy.

3. Policy and Procedure

Wireless Network Controls Policy

- HSX shall manage and control its wireless networks in order to protect HSX enterprise data and other information assets that access, traverse, or reside within the HSX network.
- A current wireless network diagram shall exist and shall be updated whenever there are network changes and no less than every 6 months.
- HSX shall physically secure its network closet to protect from any unauthorized establishment of, or access to, unauthorized wireless connections.
- HSX shall maintain an inventory of authorized wireless access points, including a documented business justification to support unauthorized WAP identification and response.

- The wireless network diagram shall be made immediately and continuously available for HSX official operational, planning, and coordination purposes. The wireless network diagram shall be classified as internal-use-only in accordance with the *Data Classification Policy* and shall be handled in accordance with the *Data Handling, Labeling, and Storage Policy*.
- Vendor defaults for wireless access points shall be changed prior to authorizing the implementation of the access point. At a minimum, this includes changing the manufacturer's default settings for encryption keys, SSIDs, known and trusted wireless devices, and passwords.
- Wireless access points shall be configured with strong encryption (WPA2) at a minimum).
- Wireless access points shall be placed in secure locations unless otherwise approved by the Chief Information Security Officer (CISO).
- File sharing shall be disabled on wireless-enabled devices.
- All wireless network devices shall be identified and authenticated prior to establishing a connection. Only wireless access points expressly authorized by the CISO shall be permitted to establish a connection.
- Firewalls shall be configured to deny by default (deny all, permit by exception) or control any traffic from a wireless environment into the confidential data (e.g., PHI, SSN, PII) environment.
- Wired ports in walls and cubicles are not patched into the corporate data switch without CISO approval.

Wireless Network User Policies

- Wireless networks shall be monitored and audited for policy compliance.
- Wireless network use shall be subject to all applicable HSX policies.
- The guest wireless network shall not connect to the HSX wireless network.
- HSX shall reserve the right to prohibit or deny connections to its wireless networks at any time for any reason.

4. Procedure

None

5. Enforcement

- 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 §164.312(a)(2)(i), HIPAA §164.312(c)(1), HIPAA §164.312(c)(2), HIPAA §164.312(d), HIPAA §164.312(e)(1), HIPAA §164.312(e)(2)(i), HIPAA §164.312(e)(2)(ii)
- HITRUST Reference: 09.m Network Controls
- PCI DSS v3 1.1.1, PCI DSS v3 1.1.2, PCI DSS v3 1.1.3, PCI DSS v3 1.1.4, PCI DSS v3 1.1.5, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 1.2.2, PCI DSS v3 1.2.3, PCI DSS v3 2.1.1, PCI DSS v3 4.1.1, PCI DSS v3 11.1

Policy Owner	Security Officer	**Contact**	brian.wells@healthshareexchange.org
Approved By	HSX Management Team; Board	**Approval Date**	December 11, 2019
Date Policy In Effect	May 13, 2015	**Version #**	1.1
Original Issue Date	May 13, 2015	**Last Review Date**	September 15, 2019 January 19, 2017 May 13, 2015

Related Documents	Data Classification Policy Data Handling, Labeling, and Storage Policy Glossary Incident Management Policy Wireless Network Diagram