Northwell Health

POLICY TITLE: Wireless Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.15	**CATEGORY:** Information Services
System Approval Date: 2/25/16 **Site Implementation Date:** 4/22/16	**Effective Date:** 8/10/10 **Last Reviewed/Revised: 1/2016**
Prepared by: Office of the CIO– IS Policy & Procedure Committee	**Superseded Policy(s)/#:** N/A

GENERAL STATEMENT of PURPOSE

Wireless access to the Northwell Health Enterprise Network must be secure to mitigate the risks that could cause a breach of data confidentiality, loss of data integrity, availability or privacy. This policy provides requirements to be followed when using Northwell Health approved devices (such as laptops, iPads, and smartphones) to connect to the internet and Northwell Health's network.

POLICY

Wireless access connections must meet Northwell Health's requirements, and only approved devices and/or methods may be used.

SCOPE

This policy applies to all members of the Northwell Health workforce including, but not limited to: employees, medical staff, volunteers, students, physician office staff, and other persons performing work for or at Northwell Health; faculty and students of the Hofstra Northwell Health School of Medicine conducting Research on behalf of the School of Medicine on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell Health School of Graduate Nursing & Physician Assistant Studies.

DEFINITIONS

Enterprise wireless network: The private network used for business purposes by Northwell Health. This includes all business and health care related applications and devices. This network uses strong encryption to protect the data.

Wireless device: A smartphone, laptop, or other computing device that connects to a wireless (Wi-Fi) network.

Guest wireless network: A public network available to any user within the confines of Northwell Health.

Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information collected or stored by a facility. Individually identifiable health information includes demographic information and any information that relates to the past, present, or future physical or mental condition of an individual. The *Health Insurance Portability and Accountability Act* (HIPAA) details eighteen items that render PHI identifiable.

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, Zip code, and their equivalent geocodes, except for the initial three digits of a Zip code in certain situations
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Medical device identifiers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

PROCEDURE/GUIDELINES

A. Connecting Over Health System Wireless Networks

1. In most facilities, Northwell Health provides wireless access over two separate wireless networks: the internal Enterprise wireless network and a Guest wireless network.
2. Only Northwell Health-provided wireless devices, or personal wireless devices (e.g. smartphones or tablets) configured by Northwell Health, are permitted to connect to the internal Enterprise wireless network. All other wireless devices must use the Guest network.
3. Users on the Guest wireless network who need access to Northwell Health resources must use a secure VPN connection to Northwell Health's internal network.
4. All wireless devices used within Northwell Health must comply with the transmission protocols, security measures, and encryption standards approved by the IS department.

5. Unauthorized wireless devices and/or access points are strictly forbidden and are subject to immediate disconnection from Northwell Health's private wireless network.
6. Users must contact the IS Help Desk to request authorization before connecting their wireless device to Northwell Health's private wireless network

B. Wireless Devices Guest Wireless Network

Northwell Health provides a separate wireless network for visitors and guests.

- Users connecting to Northwell Health's guest wireless network are responsible for understanding and following the requirements outlined on the guest wireless splash page (i.e. the first page the user sees before connecting to the wireless network) and may be held responsible for any misuse or violation.
- Use of the guest network to access Northwell Health applications and documents containing Sensitive or Highly Sensitive information must use an authorized strong encryption method such as Northwell Health's Remote Access Portal. (Refer to the 900.08 Remote Access Policy.)

C. Connecting Over Public or Unsecured Networks

1. Caution must be taken when connecting to an unsecured or public network, as they often are not configured to provide maximum security. When connecting to Northwell Health via such wireless networks, the:
   - Device must be updated to the most recent patch level;
   - Device must have anti-virus software installed and updated;
   - Device must establish a secure VPN connection; and
   - User must take precautions to prevent the screen from being observed by unauthorized persons.
2. Users are prohibited and will be prevented from establishing simultaneous VPN connections to any other networks while connected to Northwell Health.

D. Connecting Over Private or Home Networks

1. The same precautions as those for Public or Unsecured networks (above) must be followed when accessing Northwell Health's network from a private or home network.
2. Home wireless networks that will be used to provide a connection to Northwell Health should:
   - Have the default administrative settings such as passwords and network names (SSID) periodically changed;
   - Use strong encryption (such as WPA2); and
   - Not broadcast the network ID (SSID).

   Consult your router's user guide for more information on changing these and other settings.

E. Transmitting Sensitive or Highly Sensitive Information

All transmission of Sensitive or Highly Sensitive information (PHI, PII or employee private data) may only be accomplished using the Enterprise wireless network or a wireless network using a secure VPN connection with encryption.

ENFORCEMENT

Users should report any violations of this policy immediately to his or her manager. If appropriate, the violation should be escalated and reported to the IS Help Desk or the Office of Corporate Compliance Help Line. Anyone found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or engagement, as applicable, in consultation with Human Resources.

CONTACT INFORMATION

What	**Where**
Northwell Health Help Desk	(516) (718) (631) 470-7272
Northwell Health Help Desk Email	servicedesk@Northwell.edu
IT Security Hotline Email	ITSecurity@Northwell.edu
Office of Corporate Compliance Help Line	(800) 894-3226
Office of Corporate Compliance Website	www.Northwell.ethicspoint.com

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- 900.00 Computer Use Policy
- 900.08 Remote Access Policy

CLINICAL REFERENCES

N/A

ATTACHMENTS

N/A

FORMS

N/A

APPROVAL:	
System Administrative P&P Committee	8/10/10; 11/21/13; 2/1/16 *(e-vote)*
System PICG/Clinical Operations Committee	9/23/10; 12/12/13; 2/25/16 *(e-vote)*

Versioning History:

9/10

12/13

1/16