**Northwell Health**

| **POLICY TITLE:**<br>Remote Access Policy | **ADMINISTRATIVE POLICY AND PROCEDURE MANUAL** |
|---|---|
| **POLICY #:** 900.08 | **CATEGORY:** Information Services |
| **System Approval Date:** 2/25/16<br><br>**Site Implementation Date:** 4/22/16 | **Effective Date:** 9/14/10<br><br>**Last Reviewed/Revised: 1/2016** |
| **Prepared by:** Office of the CIO—IS Policy & Procedure Committee | **Superseded Policy(s)/#:**<br>N/A |

## GENERAL STATEMENT of PURPOSE

The purpose of this policy is to identify and describe the use of secure, remote network connections originating from users outside of the Northwell Health network into the Northwell Health network.

## POLICY

It is the policy of Northwell Health to grant approved users, secure remote access to certain Northwell Health computers and applications, for job-related functions only. Access to confidential data including protected health information, personal identifiable information, or sensitive or highly sensitive information requires appropriate authentication mechanisms. Use of any remote access technology that is not explicitly approved by IT Security is prohibited.

All other requests for remote access not described below will be reviewed by the IT Security department and require approval by the Chief Information Security Officer (CISO) or his/her designee.

## 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

**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

**Remote Access**: *Remote Access* provides access to Northwell Health's network or Information Systems assets from a connection point originating outside of Northwell Health's network and firewalls.

**Remote Access Portal (RAP)**: *Remote Access Portal* refers to Northwell Health's web-based point of entry for remote access.

**Token**: A *token* is a hardware or software device that generates a one-time random password. This is considered two-factor authentication.

**Virtual Desktop Infrastructure/Interface (VDI)**: *Virtual Desktop Infrastructure/Interface* is a technique enabling access to a virtualized desktop, which is hosted internally over the Internet. VDI uses risk-based authentication in addition to a password.

**Virtual Private Network (VPN)**: A *Virtual Private Network* is a secure encrypted connection between two points. A VPN connection may be temporary for the duration of the session (between a user and a specific remote network) or constructed as a permanent connection between two networks (site-to-site).

**PROCEDURE/GUIDELINES**

Employee, vendor, consultant, and non-employee requests for remote access must be submitted to the IS Helpdesk and approved by the pertinent department manager or supervisor.

Vendors, consultants, and non-employees are required to do one of the following:

- Sign a *Business Associate's Agreement* (BAA);
- Sign a non-disclosure agreement; or
- Consent to confidentiality language in a signed agreement.

All remote users are required to follow and adhere to Northwell Health policies and procedures to protect unauthorized access to data and systems. These procedures will be enforced by Northwell Health through automated processes, whenever possible, such as terminating a VPN session after a period of inactivity.

Remote access to Northwell Health's network requires additional controls such as strong authentication with two factor or risk-based authentication, and encryption depending on the method of access.

Logging, monitoring, and reporting tools will be used by Northwell Health to manage remote access usage.

A. Remote Access Methodology

Northwell Health provides different methods of remote access as follows:

- ESS Connection offers a browser-based VPN connection which provides an employee access to the HR suite of self service offerings. Some of these services include but are not limited to: benefits, personal, payroll and time reporting information as well as access to their Northwell Health Email account. Users are required to provide their network credentials and their unique PIN (also called "ESS Key").
- Tokenless RAP offers a browser-based VPN connection to access select applications such as Microsoft Web Outlook, the employee Intranet, and the Electronic Medical Information Library (EMIL).
- Token RAP is also a browser-based VPN connection to a select group of sensitive applications such as those related to patient care or financial data.
- NetConnect VPN provides an extension of Northwell Health's network and access to the applications, assets, and resources that would normally be available from the client's workplace desktop. Use of a token is required to access NetConnect VPN.
- *VDI Connection* allows users to see and use their desktop computer as if they were sitting in the office.

B. Tokens

- All individuals requiring tokens must sign a confidentiality agreement or agree to other

contractual approved language.

- Tokens may be requested from the IS Help Desk with the individual's manager's approval.
- Tokens are assigned to individual users for authentication; the sharing of tokens is prohibited.
- Tokens are the property of Northwell Health and must be returned upon termination or when remote access is revoked.

C. User Requirements

- It is the user's responsibility to follow and adhere to the training materials and guidelines which can be provided by the IS Help Desk or accessed directly through the Remote Access Portal.
- Never leave a remote access session unattended. Lock your computer (by pressing Ctrl-Alt-Delete) or disconnect from the Northwell Health network by logging off of your session. Refer to the 900.00 *Computer Use Policy* for additional information.
- Never let another person use your computer or device while connected to the Northwell Health network.
- Computers are configured with anti-virus software and the latest virus definitions in compliance with Policy 900.06 *Anti-Virus Policy*. If you suspect that your device may be infected with a virus or malware, **DO NOT CONNECT TO THE NORTHWELL HEALTH NETWORK**. In this situation, seek assistance from the IS Help Desk.

**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 Hotmail 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
- 900.06 Anti-Virus Policy

- 900.12 Data Classification and Handling Policy
- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) Pub. L. No. 111-5 (February 17, 2009)

**CLINICAL REFERENCES**
N/A

**ATTACHMENTS**
N/A

**FORMS**
N/A

| **APPROVAL:** | |
|---|---|
| System Administrative P&P Committee | 9/14/10; 10/12/10; 11/21/13; 2/1/16 *(e-vote)* |
| System PICG/Clinical Operations Committee | 9/23/10; 10/28/10; 12/12/13; 2/25/16 *(e-vote)* |

Versioning History:
9/10
10/10
12/13
1/16