Northwell Health

POLICY TITLE: Anti-Virus Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.06	**CATEGORY: Information Services**
System Approval Date: 2/25/16 **Site Implementation Date:** 4/22/16	**Effective Date:** 8/10/2010 **Last Reviewed/Revised: 1/2016**
Prepared by: Office of the CIO– IS Policy & Procedure Committee	**Superseded Policy(s)/#:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this policy is to establish requirements for deploying, using and supporting anti-virus software on the Northwell Health network.

POLICY

All computing devices, or devices with embedded computers (for example, laptops, workstations, servers, medical devices, HVAC, etc.) that are connected to the Northwell Health network must be protected against viruses and malware. This shall be accomplished through the use of anti-virus/malware software, where possible.

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

Bring Your Own Device (BYOD): A computer that is not owned by Northwell Health but is brought onto Northwell Health premises to access Northwell Health information. A BYOD may be a portable computer (for example, a laptop or notebook), smartphone, tablet, or other wearable smart technologies (Wear Your Own Device).

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. General

- Anti-virus software is not always commercially feasible, technically supported or even available on all operating systems or devices. Consequently, where anti-virus software cannot be used, appropriate compensating controls to limit the effects of malware will be employed, such as the use of firewalls, security patching, vulnerability scans and system monitoring.
- All computing devices with anti-virus software must have the software installed, have current virus signature files applied, and be actively running.
- BYOD devices connected to the Northwell Health network but not owned by Northwell Health (such as personal or vendor-owned) must also use anti-virus software and be configured to meet the standards in this policy.
- Anti-virus software must be configured such that:

- Only approved anti-virus software may be used;
- The auto-protect feature (real-time protection) is enabled;
- Signature files are automatically and frequently updated; and
- Logging and alerting is enabled.

- Anti-virus software does not offer absolute protection against the latest threats. Extreme caution must be exercised when visiting websites, opening embedded links in emails, downloading files, and connecting storage devices to machines connected to the Northwell Health network.

B. End-User Requirements

- End-users are not permitted to uninstall, reconfigure, disable or modify the anti-virus software in any way.
- Users are prohibited from engaging in any activities with the intention of downloading, creating, or distributing malicious programs.
- All newly attached storage devices, except network drives, should be scanned.
- Northwell Health devices that are kept offsite (e.g. at home) and infrequently used must be connected to the Northwell Health network periodically to obtain the latest anti-virus signatures.
- Users are required to comply with policy 900.01 *Internet, Cloud, Instant Messaging and Other Web Services Usage Policy*.
- Users should notify the IS Help Desk when a file is quarantined in error or when more information is required about appropriate anti-virus software.

C. Anti-Virus Support

- Information Services is responsible for:
  - Developing and maintaining the Northwell Health anti-virus security strategy, policy and procedures.
  - Reviewing anti-virus trending and activity reports to better assist in determining the optimal strategy and configuration.
  - Approving all changes to the servers and anti-virus configuration (such as rebooting, software updates, hardware changes, policy and reconfiguration).
  - Installation, configuration, monitoring and managing the anti-virus software and quarantining features on Northwell Health owned devices.
  - Virus remediation, the temporary removal of infected devices from the network, cleaning and subsequent releasing of “cleaned” files.
  - Generating ad-hoc and daily or weekly reports (for example, activity, trending).
- Regularly scheduled virus signature updates and operating system (OS) patches do not require IT Security approval and should be performed as frequently as recommended by the vendor.

Refer to 100.009 *Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy* for the policy and procedure requirements regarding the protection against viruses and malware within the segmented, secure network where Payment Card transactions (as defined in the policy) are processed. Should there be a discrepancy between 100.009 and this policy, 100.009 takes precedence.

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

- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- 900.00 Computer Use Policy
- 900.01 Internet, Cloud, Instant Messaging and Other Web Services Usage Policy
- 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164

CLINICAL REFERENCES

N/A

ATTACHMENTS

N/A

FORMS

N/A

APPROVAL:	
System P&P Committee	8/10/10; 8/29/13 (Prov); 9/26/13 (Final); 2/1/16 *(e-vote)*
System PICG/Clinical Operations Committee	9/23/10; 10/17/13; 2/25/16 *(e-vote)*

Versioning History:
9/10
10/13

1/16