
## You Know You Need To Be HIPAA Compliant, But Where Do Start?

The regulation of healthcare continues to evolve and become more complex. Keeping your practice compliant with requirements can be extremely confusing and frustrating. Your resources are already stretched to the limit because you're busy doing what you do best - taking care of patients.

Many medical practices have gotten by with their current plans because there has been minimal enforcement. Those days are gone! The Department of Health and Human Services has hired Consultants to audit the HIPAA privacy and security compliance. Security breaches are being found and the punitive damages for HIPAA noncompliance continues to grow.

It's imperative to have an understanding of where you need to be spending your time and what controls need to be implemented to protect your patient's and customer's information.

NNYOnline specialists can assist healthcare organizations in successfully navigating the HIPAA maze. Our Meaningful Use Security Risk Assessment program provides advisory services for clients to achieve compliance with Part 15 of your Electronic Health Record Meaningful Use Core Objectives. Our skilled experts can guide your team as it prepares to implement the institutional changes needed to improve HIPAA Security Rule practices, ensure a sustainable program is in place and prepare for a potential audit.

## Avoid Fines, Loss of Income and a Damaged Reputation!

**Call 315.782.6944 for a free consulation today!**

## NNY Online's Complete List of Services:

- Managed Off-site Backup
- Managed Firewall Services
- Managed Web Hosting
- Managed Email Services
- Managed Content Filtering
- Hosted Virtual Servers and Workstations
- Hosted Physical Servers and Workstations
- Server and Workstation Monitoring
- Server and Workstation Patch and Update Services
- Vulnerability Scans
- Continuous Data Protection
- Managed Antivirus Services
- HIPAA Compliance Services
- PCI Compliance Services
- Network and Security Assessment Services

## Northern Computers

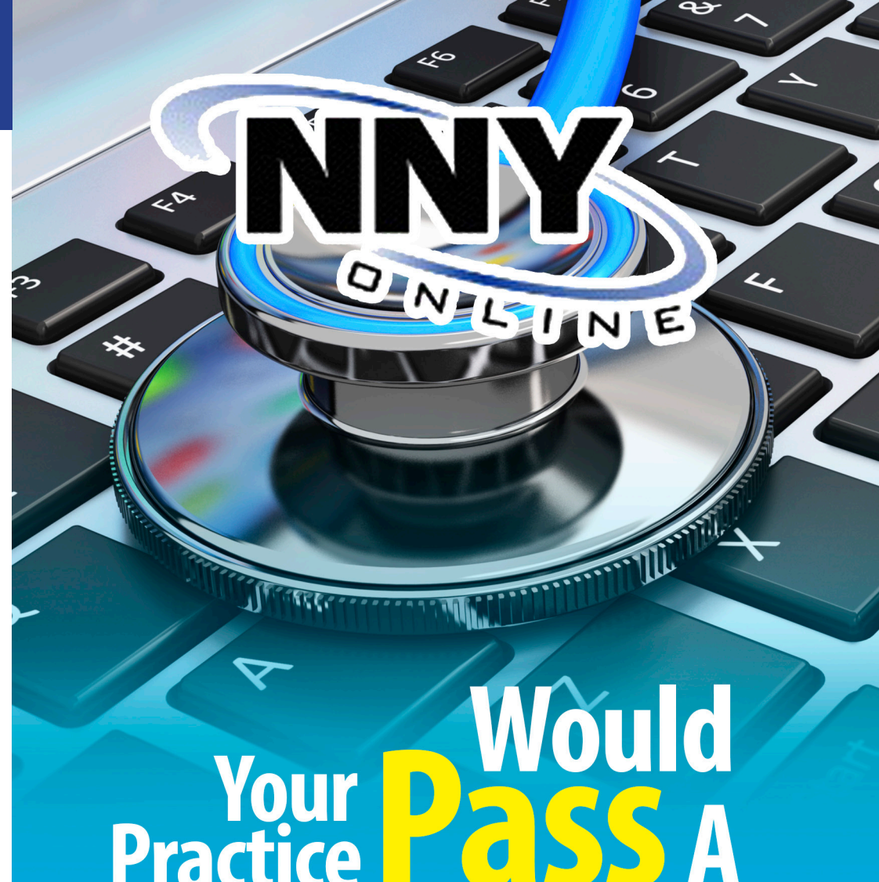
***Computers Sales & Service • Phone Systems • Networks***

Northern Computers support gives you the freedom to focus on what you do best; running and growing your business. Our professional staff provides managed IT and Telephony services to both business and residential customers.

Simple pricing tailored to the amount of support you actually need and quick technical methods make it easy to have all the advantages of a full-time IT department working for your business.

Northern Computers provides a "One-Stop Shop" for all of your hardware, software, telephony and network needs and is dedicated to making your business operate as efficiently as possible.

**Serving Northern & Central New York**




# Would Your Practice Pass A HIPPA Meaningful Use Security Risk Assessment?

**NNYOnline**
130 Park Place
Watertown, New York 13601
(315) 782-6944 | nnyonline.com


## What is Meaningful Use?

As a part of the provisions of The American Recovery and Reinvestment Act of 2009 (ARRA), the federal government has allocated funds to encourage increased usage of EHR technology by medical professionals. This provision, or the HITECH Act, will provide incentive payments administered by the Centers for Medicare and Medicaid to eligible medical pratices that adopt and successfully implement "meaningful use" of certified EHR systems.

As of 2015, eligible providers participating in Medicare and Medicaid will must meet HITECH EHR requirements. ***Professionals who cannot demonstrate the required meaningful use of a certified EHR system will incur financial penalties in the form of reduced Medicare and Medicaid reimbursements.***

NNYOnline will partner with you to understand your organization, compliance requirements, security needs, and technology infrastructure. Our comprehensive security risk assessment is designed to help you comply with Part 15 of your Electronic Health Record Meaningful Use Core Objectives. Our reviews are designed to give you a comprehensive analysis of your administrative, physical and technical safeguards.

In addition, we reach out to you throughout the year to help you deal with the latest healthcare regulatory and technology challenges. Through our year round service strategy and customized recommendations, we help you better manage and protect electronic and paper patient information to avoid regulatory violations and help mitigate changing security threats.

**Call NNYOnline to schedule your HIPAA Meaningful Use Security Risk Analysis at (315) 782-6944 Today!**

## The Process to Achieve Meaningful Use

### *Step 1: Conduct a Discovery and Risk Consultation*

NNYOnline will meet with your Security Compliance Officer to determine the current physical and administrative security measures in place. It is imperative that you implement safeguards to keep information confidential and secure within internal operating systems and external communication. These safeguards include facility access controls, workstation security and use , security awareness and training, security incident procedures, and information access management based on employees roles and responsibilities.

### *Step 2: Conduct a Comprehensive Evaluation of the Practice Technology Environment to Determine the Current Status of Your Network and IT Security*

NNYOnline will conduct a full scan of your entire network to determine if your meet technical standards such as implementing access and authorization controls, network integrity, secure transmission controls, and personal authentication requirements.

### *Step 3: Using the Results of the Discovery and Technology Environment Evaluation, Analyze and Evaluate Security Risks and Potential Vulnerabilities*

After performing your comprehensive evaluation, NNYOnline will analyze the results and begin to determine your need and outline the practice's current security risks.

### *Step 4: Create an Analysis Report with Priorities for Resolution*

After the comprehensive analysis is complete, NNYOnline with create a GAP Report detailing the results of the analysis which will show the practice's security vulnerabilities, and the priorities for resolution.

### *Step 5: Present Findings*

NNYOnline will present the results of a detailed GAP Report to the security compliance officer and advise on how to remediate security vulnerabilities.

### *Step 6: Remediate Vulnerabilities*

NNYOnline will work with your practice to assist in remediating security threats.

### *Step 7: Periodic Reviews*

The initial Security Risk Assessment will satisfy Part 15 of the Meaningful Use Risk Assessment requirement, however, it is highly suggested that NNYOnline perform periodic security risk assessments to ensure your practice's continued compliance and demonstrate documented security risk resolutions.


## Top 5 Myths of Security Risk Analysis

| MYTH | FACT |
|---|---|
| The security risk analysis is optional for small providers. | **FALSE!** All providers who are "covered entities" under HIPAA are ***REQUIRED*** to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments ***MUST*** conduct a risk analysis. |
| Simply installing a certified EHR fulfills the security risk analysis MU requirement. | **FALSE!** Even with a certified EHR, you ***MUST*** perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR. |
| My EHR vendor took care of everything I need to do about privacy and security. | **FALSE!** Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely ***YOUR RESPONSIBILITY*** to have a complete risk analysis conducted. |
| My security risk analysis only needs to look at my EHR. | **FALSE!** Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. |
| I only need to do a risk analysis once. | **FALSE!** To comply with HIPAA, you ***MUST*** continue to review, correct/modify, and update security protections. |

*Credit: Taken in part from the Guide to Privacy and Security ofHealth Information. Department of Health & Human Services.*