

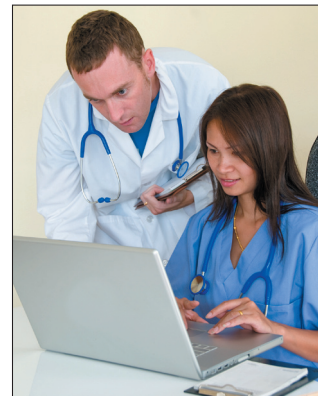
# Health IT Security

**NYSTEC**

Your Independent Technology Advisor

The Health Information Technology for Economic and Clinical Health Act (HITECH) provides billions of dollars in incentives for the adoption and use of Health Information Technology (HIT) by eligible Medicare and Medicaid health care entities. To receive Medicare and Medicaid incentive payments, eligible health care professionals and hospitals must demonstrate “meaningful use” of certified software for Electronic Health Records (EHRs). Additionally, the HITECH Act expands on HIPAA Security and Privacy requirements and implements significant penalties for non-compliance including mandatory public disclosure of data breaches and a tiered system of fines that can reach \$1.5 M per year.

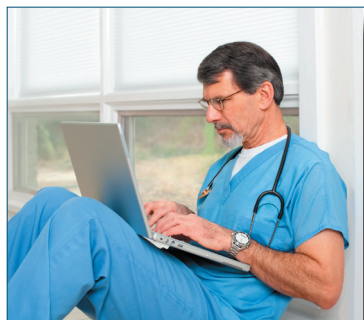
NYSTEC, a not-for-profit independent technology advisor, is intimately familiar with New York State and federal technology standards for information security — including new HITECH-driven HIPAA privacy and security provisions — that participants must meet to benefit from this program. As EHRs are captured and shared more broadly across networks, compliance with security and privacy is critical to ensuring clinicians’ and patients’ trust in the electronic exchange of these records. The HITECH program encourages adoption of HIT across three stages of “Meaningful Use:”



1. **Information Capture** - During this first stage, participants will obtain EHR software that will capture and store health information in electronic format and use the information to track key clinical conditions, communicate for care-coordination purposes, implement decision support tools, and report clinical quality measures and public health information. Compliance with security and privacy standards will be a large part of this capture stage.
2. **Improve Patient Care** - To improve health care, various participants will exchange the health information that they’ve captured. During this stage, Health Information Exchange (HIE) will happen more broadly between inpatient and out-patient hospital networks. At this stage security and privacy compliance becomes more critical as information is shared and risks of patient data breaches must be mitigated.
3. **Integrated Network** - A “network of networks” among health care professionals and hospitals will be finalized to advance decision support, patient self-management tools, comprehensive patient-care data, and to promote effective quality care and safe outcomes. At this stage, large volumes of EHRs are being utilized and exchanged and consequences for compliance failures could be costly.

*Health care CIOs and technology managers can take various actions to jump-start HITECH and HIPAA security compliance. Here are some important early initiatives that NYSTEC can assist you with implementing:*

1) **Ensure that security is built-in, and not an afterthought.** Security must be an integral element of your HIT and HIE planning, and NYSTEC can help you from the start. NYSTEC’s approach to HITECH Security Compliance is threefold:



- ◆ Assess organizational security readiness and compliance with pertinent laws and best practices
- ◆ Develop mitigation plans for compliance
- ◆ Educate and assist your organization with compliance actions

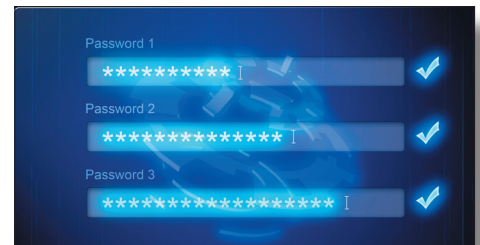
2) **Perform a risk assessment.** A risk-assessment methodology is integral to HIT planning, compliance with stronger HIPAA privacy and security requirements, information capture, and information exchange. This methodology involves identifying your organization’s assets and categorizing potential losses; identifying threats, vulnerabilities, existing controls, and the value of different pieces of information to the organization and your patients; and identifying the risk, as well as controls and actions

necessary to mitigate the risk.

3) **Take early steps to mitigate risks in your information security environment.** Information and network security is vital to the Information Exchange and Outcome Improvement stages, when the “network of networks” will facilitate the exchange of information to improve health outcomes.

4) **Act now.** The latest HITECH privacy and security provisions took effect on February 17, 2010. Enhancements to HIPAA security and privacy such as FIPS approved encryption, message signing and extensive audit requirements will be challenging to meet. The later in the game you start, the more challenges you will have securing the technical expertise to serve you. A carefully crafted HIT plan developed today will pay substantial dividends tomorrow.

*Information security must be a continuous effort encompassing policy, process, procedure, education, monitoring and enforcement to be responsive to evolving threats. NYSTEC's Health IT Security services also include:*



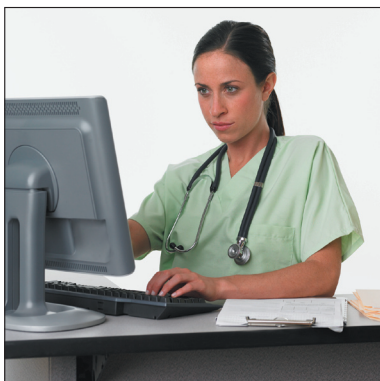
**Vulnerability Analysis & Compliance Solutions** – Before you can protect your EHR information, you must first understand your assets, networks and infrastructure, and their security weaknesses. NYSTEC uses a variety of effective methods to assess your infrastructure and network vulnerabilities, including risk analysis, network scanning, traffic analysis, current practice review, backdoor analysis, and wireless network audits. While it is important to identify and respond to weaknesses and risks, it is far more important to build security into the organization's design, implementation and support efforts.

**Information Security Policy** – A well-developed and well-documented policy is the heart of a strong information security protocol. NYSTEC evaluates your existing policies and recommends new policies, including acceptable use, data encryption, role-based access controls, network separation, monitoring, data ownership, remote access, virus protection, and availability requirements.

**Security Architecture Design** – A secure computing environment combines a sound policy with robust security architecture. NYSTEC helps clients develop a strong and cost-effective security architecture by combining knowledge of industry-leading solutions and an independent approach to evaluating and selecting products that secure the environment, comply with new HITECH-driven HIPAA requirements, and are manageable and supportable.

**Deploying and Monitoring New Security Controls & Processes** – Once a policy is created and vetted, it must be implemented using tools that facilitate your daily operations and processes. NYSTEC provides deployment and monitoring services including secure network engineering, firewall management, proxy configuration, intrusion detection, log analysis, automated response, virus signature distribution, and encryption.

**Mobile Device & Wireless Security** – NYSTEC can help you secure your use of mobile computing devices and wireless networks. From smart wireless design to encryption of mobile device data, NYSTEC can help you maximize the benefits of this new technology while mitigating the associated risks.



**System Review & Updates** – Computing environments change constantly. This calls for continuous review and revision of your environment and security system, including periodic policy and process review, ongoing scanning, updated education and training, and new security product reviews.

**Education & Training** – Policy is only effective when the people responsible for its application are knowledgeable. NYSTEC's user education and training for HIT security spans many levels of understanding depending on your needs, including "how to" classes, detailed classroom instruction, executive briefings, and computer-aided instruction.

*To learn more about our Health IT Security services, please e-mail Peter Poleto at [ppoleto@nystec.com](mailto:ppoleto@nystec.com).*

**Bringing Clarity to Complex Technology Projects**

www.nystec.com  
888-9NYSTEC

**NYSTEC**  
Your Independent Technology Advisor