

NYeC


NEW YORK eHEALTH
COLLABORATIVE



Health Homes Implementation Series: NYeC Privacy and Security Toolkit

16 February 2012

Agenda

- What are the New York eHealth Collaborative (NYeC) and the Regional Extension Center?
 - What are Health Homes?
 - Privacy and Security of Protected Health Information (PHI) Rules
 - 42 CFR Part 2
 - HIPAA Privacy and Security Rules and HITECH
 - Meaningful Use Objectives
 - Privacy and Security Risk Mitigation Process
 - Scope of the Privacy and Security Toolkit
 - Tools 
 - Resources
1. CyberSecurity Guide
 2. NYeC Meaningful Use Fact Sheet
 3. NYeC Privacy and Security Training for the Practice – PowerPoint
 4. ONC HIT Security Risk Assessment Questionnaire v3.0 032911
 5. ONC HIT Security Risk Assessment Questionnaire v3.0 032911 REC Update
 6. Information Security Policy Manual

New York eHealth Collaborative

- NYeC is a not-for-profit organization working to improve healthcare for all New Yorkers through health information technology
- **Through the Regional Extension Center (REC) we promote the adoption and use of electronic health records (EHR)**
 - Educate the public on the benefits of EHRs
 - Assist providers transitioning from paper to electronic records
 - Assist providers to qualify for Meaningful Use reimbursements
- **Build the SHIN-NY (State Health Information Network – New York) a secure network for sharing electronic medical records across the state**
 - Allow providers to share information
 - Promote collaborative care so doctors work as a team to benefit the patient
- **Develop statewide policies regarding HIT**
 - Convene stakeholders and build consensus
 - Collaborate with NYS Department of health

Health Homes

- The **Health Home provision** authorized by the Affordable Care Act by CMS
- Simultaneous pursuit of **three goals**:
 - improving the **experience of care**
 - improving the **health of populations**
 - **reducing per capita costs of health care** (without any harm whatsoever to individuals, families, or communities)

Person-centered system of care for Medicaid beneficiaries with multiple or severe chronic conditions to better coordinate and manage their services.

- <http://www.cms.gov/smdl/downloads/SMD10024.pdf> .

Health Home Capabilities



Health Home Capabilities

- Provide quality-driven, cost-effective and culturally appropriate **person and family centered** health home services
- Coordinate and provide access to **preventative and health promotion** services
- Must develop a **care plan** for each individual that coordinates all clinical and non clinical services and supports to address the person's health related needs
- Use **HIT** to link services, facilitate communication between and among providers, individuals and caregivers and provide feedback to practices
- Establish continuous **quality improvement programs**, and collect and report data that support the evaluation of health homes

EHRs for Behavioral Health

- Behavioral Health HIT **Issues**
- Only **8 percent** of all behavioral health providers have fully implemented electronic records while 40% of physicians are using EHRs.
 - Behavioral health field should be able to **communicate** with the rest of the health care system.
 - All patient information should be recorded since one medication or disorder can often **impact** another - **comorbidity**
 - 2009 Behavioral Health/Human Services Information Systems Survey, conducted by the nonprofit Centerstone Research Institute.
 - <http://www.iwatchnews.org/2011/03/30/3844/proposed-bill-aims-expand-health-it-funds-mental-health-providers>

Security Policies and Processes

Data Breach – Loss of Patient Information

LINCOLN MEDICAL AND MENTAL HEALTH CENTER

SEARCH

PRINTER FRIENDLY | EMAIL A FRIEND | TRANSLATE THIS PAGE

A MEMBER HOSPITAL OF
HHC NEW YORK CITY HEALTH AND HOSPITALS CORPORATION
nyc.gov/hhc

Home
About Lincoln Hospital
Clinical Services
Neighborhood Family Health Centers
For Patients & Visitors
News & Events
[News and Press Releases](#)
[Calendar of Events](#)
[Community Newsletters](#)

Notification from Lincoln Hospital

Sometime between March 16 and 24, 2010, a weekly shipment of seven duplicate compact disks (CDs) in the custody of FedEx, were lost while being transported to Lincoln Hospital. These CDs were created by Siemens Medical Solutions USA, Inc. ("Siemens"), a company that performs billing and claims processing for Lincoln. The missing CDs contained some protected health and personal information of patients including name, address, social security number, medical record number, patient number, health plan information, date of birth, dates of admission and discharge, diagnostic and procedural codes and descriptions, and possibly a driver's license number if provided.

Both FedEx and Siemens conducted an immediate investigation to locate the CDs, and Siemens notified the hospital that the CDs were missing. Siemens was promptly directed to suspend further transport of CDs by carrier. And policies have been put in place to ensure that a similar incident does not recur.

Seven CDs with patient data lost

[VIEW THE TOUR](#)

QUICK LINKS

- [Contracting Opportunities](#)
- [Employment Opportunities](#)

STATE OF NEW YORK DEPARTMENT OF HEALTH

Security Policies Timeline

Privacy and Security of health information rules

1. 42 CFR Part 2 early 1970s

- “A program may not disclose any information that identifies a patient as being in a drug/alcohol program or as having a drug or alcohol problem.”

1. HIPAA Privacy Rule: 1996 - Compliance April 2003

- Protected Health Information (PHI)
- Covered Entities and Business Associates
- Uses and Disclosures

3. Security Rule: April 20, 2005

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

4. HITECH: February 17, 2009

- Breach Notification
- Business Associates

Federal Health Privacy Law

42 CFR Part 2

42 CFR Part 2 **1st** health privacy law – prior to HIPAA

- Federal law that governs the **confidentiality and disclosure** of alcohol and drug abuse patient records
 - General Rule “a **program may not disclose any information that identifies a patient** as being in a drug/alcohol program or as having a drug or alcohol problem.”
 - Enacted in the early 70s when Congress associated a **stigma with substance abuse** and that the fear of prosecution deterred people from entering treatment.
 - HHS Substance Abuse and Mental Health Services Administration (SAMHSA) Center for Substance Abuse Treatment <http://www.samhsa.gov>
- **Note** – New York State law determines mental health (HIV, genetic, domestic violence) privacy protection requirements

Providers covered in 42 CFR Part 2

- Providers must meet the definition of “**program**” and be “**federally assisted**”
 - A “**program**” includes any person or organization that provides, and holds itself out as providing, **alcohol or drug abuse** diagnosis, treatment or referral for treatment
 - A program is “federally assisted” if it
 - Is assisted by the IRS through a grant of tax exempt status
 - Receives federal funds in any form
 - Is authorized to conduct business by the federal government
 - Is conducted directly by the federal government or by a state or local government that receives federal funds




42 CFR Part 2

Elements Required for Patient Consent

Part 2 requires **written patient consent** for most **disclosures** of protected information with some exceptions.

A written consent to a disclosure under the Part 2 regulations must be in writing and include all of the following items (42 CFR § 2.31):

- 1) **program or person** permitted to make the disclosure;
- 2) **individual or organization** to which disclosure is to be made;
- 3) name of the **patient**;
- 4) **purpose of the disclosure**;
- 5) Amount and what kind of **information** to be disclosed;
- 6) **signature of the patient or other authorized person**
- 7) **date** on which the consent is signed;
- 8) **Revocation statement**: that consent is subject to revocation at any time
- 9) date, event or condition upon which the consent will **expire** if not revoked before.



Items
included
in
written
consent

Health Information Privacy

Health Information Privacy

Substance Abuse Confidentiality Regulations

Applying Substance Abuse Confidentiality Regulations to Health Information Exchange: FAQ Meeting August 4th The joint meeting regarding SAMHSA and ONC's recent release of FAQ's for Applying Substance Abuse Confidentiality Regulations to Health Information Exchange will be August 4th from 8:30 a.m.-12:00 p.m. The meeting will provide those interested an opportunity to offer input on the utility of the FAQs. To RSVP, email Ms. Dolkie Encarnacion at Dolkie.Encarnacion@samhsa.hhs.gov, or call 240-276-1660.

- **View the Agenda.** (pdf file | 130 kbytes) | Posted on 07/27/2010
- **Watch the Webcast** | Recorded August 4, 2010
- **Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)** (pdf file | 81 kbytes) | **Cover Page** (pdf file | 26 kbytes) | Posted on 06/16/2010

Privacy and e-Consent in Three Countries (pdf file | 731 kbytes)

The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs (pdf file | 192 kbytes)

Confidentiality of Alcohol and Substance Abuse Patient Records regulation (42 CFR Part 2)

HHS, Office for Civil Rights - HIPAA

HHS, Office of National Coordinator (ONC)

SAMHSA is a Federal services agency established in 1992 to focus attention, programs, and funding on improving the lives of people with or at risk for mental and substance abuse disorders
website - www.samhsa.gov

HIPAA Privacy Rule

HIPAA Privacy Rule – Compliance 2003

- Privacy Rule protects all “individually identifiable health information” held or transmitted by a **Covered Entity (CE) or its business associate** in any form or media (electronic, paper, or oral); called “**protected health information**” (PHI).
- Some requirements under HIPAA include
 - Notice of privacy practices
 - HIPAA compliant authorizations
 - Policy and procedure manual
 - Business associates contracts
- Under 42 CFR Part 2 consent policies should be in place

HIPAA Related Terminology

- **Protected Health Information (PHI)** is:
 - Information that relates to an
 - Individual's past, present or future physical or mental health or condition,
 - Provision of health care to the individual, or
 - The past, present or future payment for the provision of health care to the individual,
 - identifies the individual or can reasonably be used to identify the individual

- **Covered Entity** is any organization or corporation that directly handles Personal Health Information ([PHI](#)) or Personal Health Records ([PHR](#)).
 - Hospitals
 - Doctors' offices
 - Health Plans
 - Healthcare providers
 - Healthcare Clearinghouses
- **Business Associates** are any organization or person working in association with or providing services **to a covered entity** who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR). (e.g. Billing service, IT staff, transcription service)

Protected Health Information (PHI)

**Individually
Identifiable
Information**

(Name, Address, DoB)

PHI

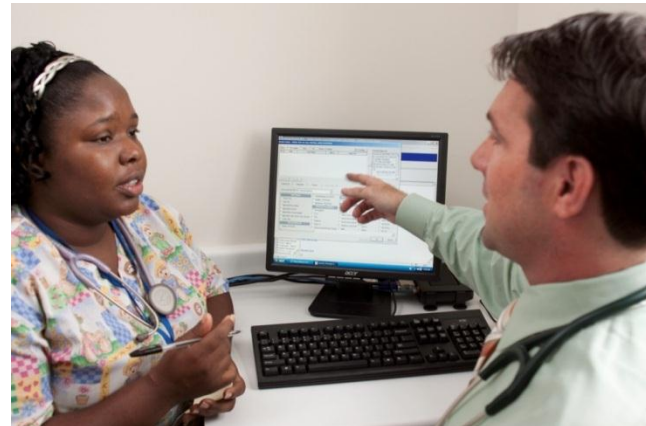
**Medical
Information**

(Scheduling, Billing, Health
Record)

How 42 CFR Part 2 differs from HIPAA

- HIPAA generally permits the disclosure of protected individually identifying health information **without patient consent** for purposes of treatment, payment or health care operations,
- 42 CFR Part 2 requires **written consent** of patient is required for most disclosures of information protected under Part 2, with some exceptions.

42 CFR Part 2 has more stringent consent and disclosure rules



Part 2 Patient Consent Process

- Health Home consent process
 - The assigned Health Home is required to secure **patient consent** forms to **officially enroll** all Health Home members in a Health Home program
 - The signed consent form **allows** their **patient information to be shared with Health Home partners**, including a Regional Health Information Organization (RHIO), if applicable
 - The signed consent form documents a patients enrollment in the program.
 - Sample NY State consent form <http://www.health.ny.gov/forms/doh-5055.pdf>

42 CFR Part 2 and HIPAA Guidance

- Three documents **compare 42 CFR Part 2 and HIPAA** requirements
 1. “The Confidentiality of Alcohol and Drug Abuse Patient Records and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs” June 2004
 2. “Frequently Asked Questions – Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)” 2010
 3. SAMHSA 42 CFR Part 2 FAQ on health IT issues II - second set

http://www.integration.samhsa.gov/financing/SAMHSA_42CFRPART2FAQII_-1-,_pdf.pdf

<http://www.samhsa.gov/healthprivacy/>

Prepared by SAMHSA , ONC and contractors - not as legal advice – informational use only.

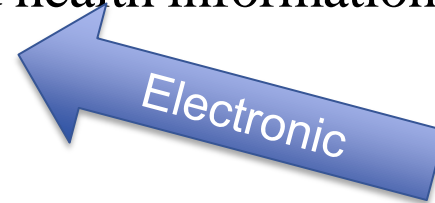
US Department of HHS, Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment



HIPAA Security Rule

HIPAA Security Rule 2005

- The HIPAA Security Rule applies to stored and transmitted **ePHI**
- Protects against reasonable anticipated **threats or hazards** to security or integrity of **ePHI** – electronic protected health information.
- Security rule safeguards
 - **Physical Safeguards** are the physical measures taken to protect a covered entity's ePHI and related **buildings and equipment** from natural and environmental hazards, and unauthorized intrusion.
 - **Technical Safeguards** are the **technology** utilized to protect ePHI
 - **Administrative Safeguards** are the administrative actions taken to **manage** the selection, development, implementation, and maintenance of security measures to protect ePHI. Risk analysis is one of the safeguards



Electronic Protected Health Information ePHI



- **Electronic Protected Health Information (ePHI)** under HIPAA a subset of PHI, means any information that identifies an individual and relates to at least one of the following:
 - The individual's past, present or future **physical or mental health**.
 - The provision of **health care** to the individual.
 - The past, present or future **payment for health care**.
 - Information is deemed to **identify an individual** if it includes either the individual's **name or any other information** that could enable someone to determine the individual's identity

Under the Security Rule “electronic” Protected Health Information is added.

HITECH Rule

HITECH Act 2009 Strengthens HIPAA

- HITECH Act part of ARRA
- Strengthens and expands HIPAA Privacy and Security in several key areas:
 - Federal security **breach notification requirement**
 - required notification of affected individuals, the Secretary, and in certain cases – the media. Business associates must notify covered entities that a breach has occurred.
 - heightened enforcement
 - New **rights of individuals**
 - New **restrictions on use and disclosure** of protected health information (PHI)
 - Direct **regulation of business associates (BA)** (includes HIEs) and who must
 - abide by HIPAA regulations on data security,
 - follow privacy provisions in ARRA
 - be directly **accountable for failure to comply** with HIPAA Privacy Rule provisions through contracts with covered entities

HITECH – New Patient Rights

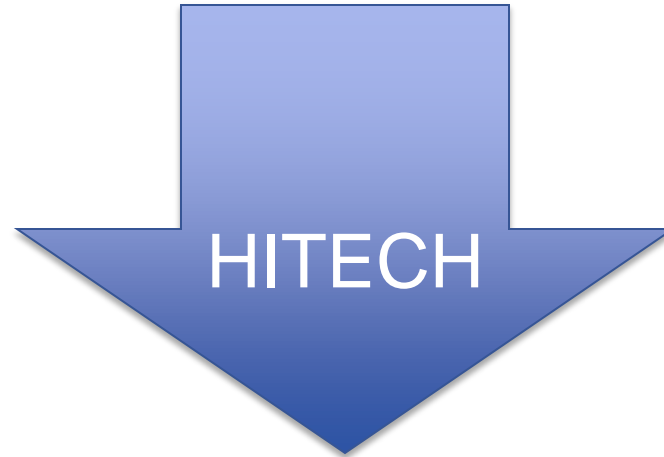
- **Rights of Individuals**

- Covered entities are required to give **copies of an individuals record to them, in electronic form**
 - Covered entities are required **upon request to account of all disclosures** of individual's protected health information made for treatment, payment or health care operations **during prior 3 years**
 - **Covered entities may not share** information with the individual's health plan for payment or health care operations **if the individual is paying full cost of the service** (upon request)
-
- Prior to HITECH Covered Entities (CEs) had been exempt of these accounting requirements

HITECH–Direct Application of HIPAA to Business Associates

- ARRA and HITECH made major changes in the treatment of “**Business Associates.**”
- Business Associates are now subject to HIPAA privacy and security requirements (or HIPAA penalties) in the same manner as a Covered Entity.
 - Business Associates had only been obligated to comply with privacy rules to the extent required in their **contracts with covered entities.**
- Covered entities may now be liable for the actions of their Business Associates (in limited settings.)
- RHIOs and HIEs are to be treated as Business Associates.

HITECH – Health Information Organizations (RHIOs) & Health Information Exchange (HIE)



- RHIOs and HIEs are to be treated as “business associates” under HIPAA.
- They are now required to directly comply with key HIPAA regulatory provisions.

Increased Enforcement of Security Breaches under HITECH

- HITECH first

National security breach notification law.

- Required to **notify affected individuals of a breach** of “unsecured” health information

Not a breach

- If DE identified data - doesn't require notification
- If data is rendered “unusable, unreadable or indecipherable to unauthorized individuals,” using a technology or methodology specified by HHS – not a breach

- Enforcement has increased and performed by the State Attorney General
- A Business Associate is directly accountable for failure
 - Civil penalties have increased
 - Criminal penalties may be imposed

Meaningful Use Core Measure 15 Risk Analysis

Meaningful Use of an EHR

The CMS Medicare and Medicaid EHR incentive programs provide a financial reward to eligible professionals for the **meaningful use** of certified EHRs to achieve health and efficiency goals.

The criteria for meaningful use will be staged in three steps over the course of five years.

Stage 1 meaningful use is now in place as presented in the 2010 CMS Final Rule.

	Core Objectives	Menu Objectives
Meaningful Use Objectives	15 Required	5 out of 10 Selected

Meaningful Use Core Set #15: Protect Electronic Health Information

Objective:

- Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Measure:

- Conduct or review a security risk analysis as per 45 CFR 164.308 (a) (1) and implement security updates as necessary and correct identified security deficiencies as part of the management process.

Exclusions:

- None

HIPAA Security Risk Analysis

- Under the Security Rule - Administrative safeguards:
 - § 164.308(a)(1)(ii)(A) *Risk analysis (required)*. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity
 - § 164.308(a)(1)(ii)(A) *Risk management (required)*. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)

HIPAA Compliance and MU 15

HIPAA

Breach
Notification
Standards

Privacy
Rule

Security
Rule

Meaningful Use 15
lives here as part of
the security rule.

Privacy and Security and Risk Mitigation Process

- Training of Health Home participants on the use of Privacy and Security tools to effectively protect the confidentiality of health information
 - The practice will be *informed* about the privacy and security and risk mitigation requirements for meeting meaningful use objectives.
 - The Implementation team will conduct a *privacy and security assessment* during the implementation stage in order to identify security related issues that need to be addressed by the practice.
 - They will conduct a *risk analysis* to determine current risk, and put into place an effective *risk mitigation strategy*.
 - *Security policy documentation will be updated* with the practice rules and regulations that have been put into place and responsibility for their implementation at the practice will be determined.
 - Practice *staff will be trained* and educated about the practice's security approach and requirements.

Security Culture

- Passwords - strong
- Anti-Virus Software – up to date
- Firewall
- Control Access to Protected Health Information
- Control Physical Access to network
- Limit Network Access
- Plan for the Unexpected
- Good Computer Habits
- Mobile Devices should be Protected

Establish a
“Security
Culture”

Train your workforce and establish
Policies and Procedure



OCR and Breaches 9/2009 – 12/2010

- The **Office for Civil Rights (OCR)** is the U.S Department of Health and Human Services civil rights and health privacy rights law enforcement agency
- What is a breach?
 - Impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information – this poses a significant risk of financial, reputational, or other harm to the affected individual.
 - Under HITECH, notification after a breach is required.
- Breaches
 - 7.8 million patients affected by ≥ 500 breaches
- Common causes of breach in 2010:
 - Theft
 - Loss of electronic media or paper records containing protected health information
 - Intentional unauthorized access to, use, or disclosure of protected health information
 - Human error
 - Improper disclosure

All caused by people not technology issues

OCR Audits



- Enforcement
- HITECH act requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards.
- OCR contracted with KPMG to complete random audits of 150 covered entities and business associates between November 2011 and December 2012.
- The purpose of the audits is to ensure compliance with the HIPAA Privacy and Security Standards as amended by the HITECH Act.

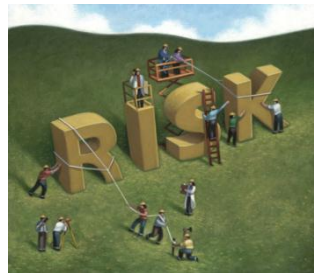
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>

Privacy and Security Toolkit

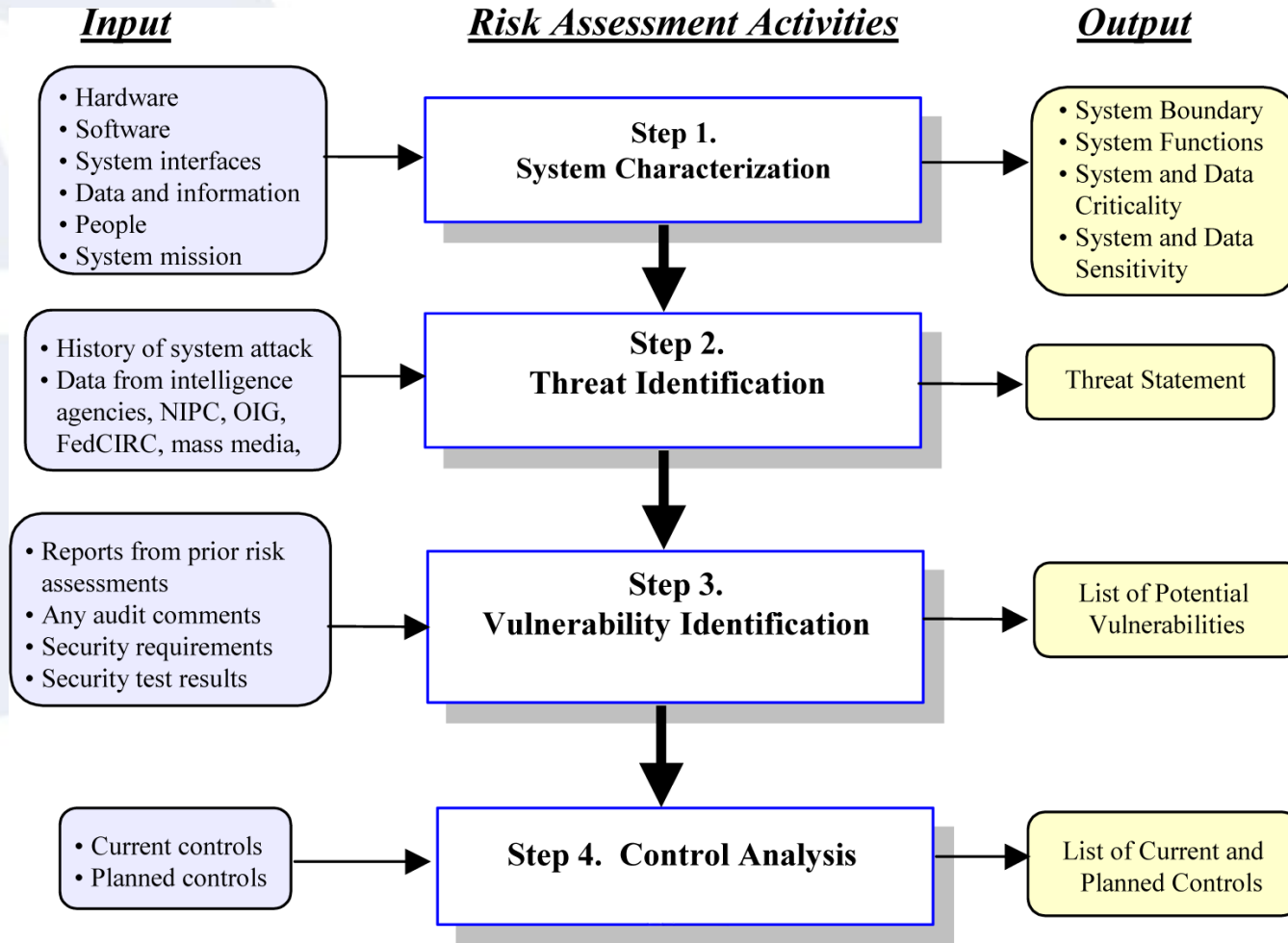
Scope of the Privacy and Security Toolkit

The tools included in the Privacy and Security Toolkit serve as guidance for educating stakeholders about the privacy, security and risk mitigation guidelines to be followed at provider practices.

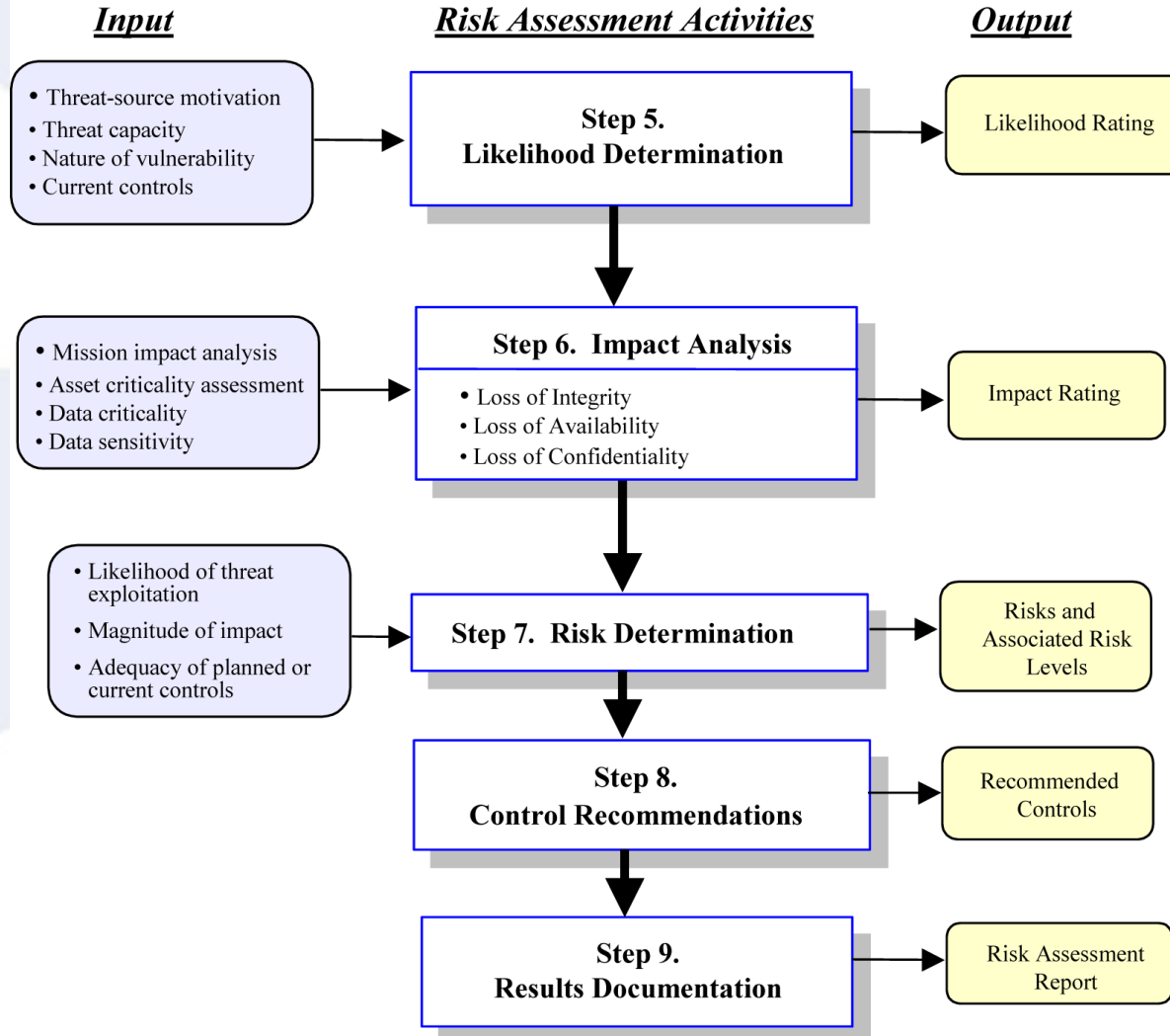
- The objective of the documents and tools is to increase *awareness* about the recommended safeguards for compliance and to implement *strategies* in order to protect electronic health information (ePHI) that is created or maintained by the certified Electronic Health Record (EHR) technology.
- The goal is implementation of appropriate *technical capabilities* and *protective measures* in order to *reduce risk* to an acceptable level.



Risk Assessment Phase 1

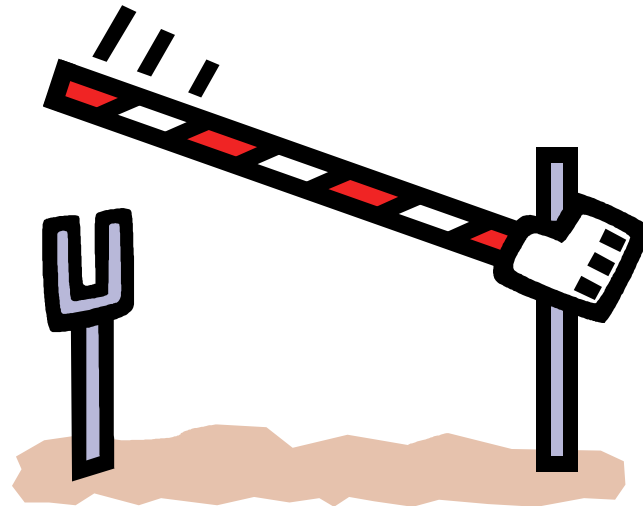


Risk Assessment Phase 2



Control Recommendations

- Arrange the threats/vulnerabilities in order of risk.
- Address the highest risk items first.
- Don't neglect operational impact.



NYeC Privacy and Security Toolkit

NYeC Toolkit

- Tools to address core measure 15 and conduct a risk analysis at a medical practice
 - CyberSecurity Guide
 - NYeC Meaningful Use Fact Sheet
 - NYeC Privacy and Security Training for the Practice – Slides
 - ONC HIT Security Risk Assessment Questionnaire
 - ONC HIT Security Risk Assessment Questionnaire – REC Update
 - Information Security Policy Manual

 - Note - Behavioral health privacy and security requirements that exceed those for a medical practice are not included in the toolkit.

CyberSecurity Guide

- The CyberSecurity Guide - 10 Best Practices for the Small Healthcare Environment,
- first take on the key security points to keep in mind when protecting EHRs.
- issued by the US Department of Health and Human Service (HHS) through the Office of the National Coordinator (ONC)

CyberSecurity Guide

11/22/2010

Practice 2: Install and Maintain Anti-Virus Software

The primary way that attackers compromise computers in the small office is by installing similar software on the computers.

How can users recognize a computer virus infection?

- Some typical symptoms of an infected computer include:
- System will not start normally (e.g., "blue screen of death")
 - System repeatedly crashes for no obvious reason
 - Internet browser goes to unwanted web pages
 - Anti-virus software appears not to be working
 - Many unwanted advertisements pop up on the screen
 - The user cannot control the mouse/pointer

protect from the newest computer viruses daily generates reminders about these updates...
data may be stolen, destroyed, or

V 1.0 November, 2010
NYeC
NEW YORK eHEALTH
COLLABORATIVE

CYBERSECURITY

The protection of data and systems in networks that connect to the Internet

**10 Best Practices
For The Small Healthcare Environment**

11/22/2010

Practice 3: Use a Firewall

Unless a small practice uses an EHR system that is totally disconnected from the Internet, it should have a firewall to protect against intrusions and threats from outside sources. While anti-virus software will help to find and destroy malicious software that has already entered, a firewall's job is to prevent intruders from entering in the first place. In short, the anti-virus can be thought of as infection control while the firewall has the role of disease prevention.

A firewall can take the form of a software product or a hardware device. In either case, its job is to inspect all messages coming into the system from the outside (either from the internet or from a local network) and determine, according to pre-determined criteria, whether the message should be allowed in.

Configuring a firewall can be technically complicated, and hardware firewalls should be configured by trained technical personnel. Software firewalls, on the other hand, are often pre-configured with common settings that tend to be useful in many situations. Software firewalls are included with some popular operating systems, providing protection at the installation stage. Alternatively, separate firewall software is widely available from computer security vendors, including most of the suppliers of anti-virus software. Both types of firewall software normally provide technical support and configuration guidance to enable successful configuration by users without technical expertise.

When should a hardware firewall be used?

Large practices that use a local area network (LAN) should consider a hardware firewall. A hardware firewall sits between the LAN and the internet, providing centralized management of firewall settings. This increases the security of the LAN, since it ensures that the firewall settings are uniform for all users.

If a hardware firewall is used, it should be configured, monitored, and maintained by a specialist in this subject.

¹ An unlikely case, but theoretically possible.

CyberSecurity Guide

The guide includes a list of ten (10) areas of security requirements and a checklist for you to confirm that your practice is following security recommendations.

The 10 best practices highlighted are:

- Use strong passwords
- Install and Maintain Anti-Virus Software
- Use a Firewall
- Control Access to Protected Health Information
- Control Physical Access
- Limit Network Access
- Plan for the Unexpected
- Maintain Good Computer Habits
- Protect Mobile Devices
- Establish a Security Culture

best
practices

Cyber Security Guide

There are **checklists** at the end of the guide that identify important basic security practices

- Password
- Anti-Virus
- Firewall Access
- Control Physical Access
- Network Access
- Backup and Recovery
- Maintenance
- Mobile Devices

checklists

Cyber Security Guide Sample Checklist

Practice 1: Password Checklist

- Policies are in place prescribing password practices for the organization.
- All staff understand and agree to abide by password policies.
- Each staff member has a unique username and password.
- Passwords are not revealed or shared with others.
- Passwords are not written down or displayed on screen.
- Passwords are hard to guess, but easy to remember.
- Passwords are changed routinely.
- Passwords are not re-used.
- Any default passwords that come with a product are changed during product installation.
- Any devices or programs that allow optional password protection have password protection turned on and in use.



Password checklist

Strong passwords **should**:

- Be at least 8 characters in length
- Include a combination of upper case and lower case letters, at least one number and at least one special character, such as a punctuation mark
- Be changed often, at least quarterly.



Privacy & Security Fact Sheet for Meaningful Use

Meaningful Use is all about helping patients. What does privacy and security have to do with it?

Meaningful Use is all about helping patients. However patients have let it be known that they have concerns regarding the privacy and security of their health information. Responding to comments regarding the Meaningful Use final rule, CMS stated that "...maintaining privacy and security is crucial for every eligible provider (EP), eligible hospital or Critical Access Hospital (CAH) that uses certified EHR technology."¹

Are there any privacy or security requirements for complying with Meaningful Use in order to receive incentive money?

Yes. "Protect electronic health information created or maintained by the certified EHR through the implementation of appropriate technical capabilities"², is one of the Core Objectives Eligible Providers must meet under the Medicare and Medicaid Electronic Health Record Incentive Program.

How can I meet the objective of protecting ePHI under the Meaningful Use Incentive Program?

The measure of meeting the core objective of protecting ePHI created or maintained by a certified EHR system is for an organization to "conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process."³

My EHR vendor is certified (or guarantees they will be certified) by one of the ONC certifying bodies. By using a certified EHR system, won't I meet the Meaningful Use security objectives?

¹ Medicare and Medicaid Programs, Electronic Health Record Incentive Program, Final Rule, Federal Register 75:144 (28 July 2010) p. 44369.

² 42 CFR 483.6(a)(13) (2010).

³ Id.

No. The measure of meeting the objective of protecting ePHI created or maintained by a certified EHR is to conduct or review a security risk analysis. Periodic risk analysis and a risk management program are required pursuant to the HIPAA Security Rule. Compliance with the HIPAA Security Rule was mandated to be complete for most Covered Entities by April 2005.

For Meaningful Use purposes, a security risk analysis of the certified EHR technology must be conducted or reviewed; the results of which should be incorporated into the organization's overall risk analysis and risk management program.

What if I never completed a risk analysis and do not have a risk management program (or have not reviewed our risk analysis for a long period of time) as required by the HIPAA Security Rule?

In July 2009, the Secretary of HHS delegated the enforcement of the HIPAA Security Rule to the Office of Civil Rights (OCR). The Deputy Director of Privacy of the OCR stated that "security audits will check that organizations have completed a risk assessment and implemented appropriate administrative, physical and technical safeguards."⁴ The OCR is expected to begin random audits to ensure organizations are compliant with the HIPAA Security Rule in the near future.

Are there penalties if I am audited and found to not be compliant with the HIPAA Security Rule?

Yes. Criminal and civil penalties can be levied against organizations and/or individuals for violations of HIPAA Privacy and Security Rules. Monetary penalties for a breach of HIPAA Privacy and Security Rules range from \$100 to \$50,000 per violation. Additionally, state attorneys general are now authorized to bring civil actions against HIPAA violators on behalf of state residents.

What should I do to ensure I am in compliance with the Meaningful Use privacy and security Core Objective as well as HIPAA Privacy and Security Rules?

Your local Regional Extension Center, the New York eHealth Collaborative (NYeC), has staff that is ready to assist you. Contact NYeC today to learn of the full range of services available to you regarding compliance requirements for all Meaningful Use Objectives, HIPAA Privacy and Security Rules and other healthcare quality improvement initiatives.

⁴ Anderson, Howard, "HIPAA Audit Update: OCR's Susan McAndrew," Healthcare Info Security Web, 21 May 2010.

The **NYeC Privacy and Security Meaningful Use Fact Sheet** will help prepare your practice for the Privacy and Security Stage 1 Meaningful Use criteria.

This gives an overview of the privacy and security requirements.

Some sample questions include:

1. Meaningful Use is all about helping patients. What does privacy and security have to do with it?
2. Are there any privacy or security requirements for complying with Meaningful Use in order to receive incentive money?
3. How can I meet the objective of protecting ePHI under the Meaningful Use Incentive Program?
4. My EHR vendor is certified (or guarantees they will be certified) by one of the ONC certifying bodies. By using a certified EHR system, won't I meet the Meaningful Use security objectives?

NYeC Privacy and Security Training for the Practice

“NYeC Privacy and Security Training for the Practice” is a PowerPoint training deck about security awareness that discusses HIPAA Privacy, Security and HITECH rules, risk analysis, and network security.

All staff at the practice that work with ePHI should view this training presentation.

It does not include additions for behavioral and mental health confidentiality rules.

HIT Security Risk Assessment Questionnaire

- The **ONC HIT Security Risk Assessment Questionnaire** was released by the ONC in early 2011 to address the Meaningful Use core measure for the assessment of security risk. The REC Update version includes suggested additions made by REC members of the Privacy and Security Community of Practice workgroup.
- The **ONC HIT Security Risk Assessment Questionnaire – REC Update** starts with the ONC Questionnaire and contains additional guidance supplied by the HITRC Privacy and Security work group.
- The ONC Risk Assessment is the *centerpiece* of the Privacy and Security Toolkit.
- This four step process enables respondents to identify and mitigate their risks against pre-identified threats and vulnerabilities.

HIT Security Risk Assessment Questionnaire

- This risk assessment tool is a starting point for *identifying cybersecurity risks* to the organization.
- The tool is designed to enable respondents to *identify their level of risk* against pre-identified threats and vulnerabilities.
- It references publications issued by the National Institute of Standards and Technology (NIST) Special Publications as guidance for a security risk assessment including SP800-66 and SP 800-300.

These reference documents can be found at

<http://csrc.nist.gov/publications/PubsSPs.html>

HIT Security Risk Assessment Questionnaire

- There are 7 tabs in this spreadsheet tool.
 1. The first tab instructs you on how to *complete the forms*
 2. The second tab introduces *risk guidance* and identifies the Nine Primary Risk Assessment Steps found in the NIST Special Publication SP800-66
 3. The third tab is an *inventory* of people and technology assets that touch ePHI.
- Current revision: HIT Security Risk Assessment Questionnaire v3.0
032911.xls

HIT Security Risk Assessment Questionnaire

4. The fourth tab includes security issues that are addressed in *screening questions* for the practice. The threat vulnerability statement associated with the question indicates the problems that may result if the security issue is not addressed.
5. and 6. The fifth and sixth tabs address *People and Processes, and Technology* at the organization that work with ePHI. Recommended and existing controls measures at the practice are identified, as well as the likelihood and impact of risk exposure.
7. The last tab is a *takeaway list* which is an *accumulation of the high and medium risk findings, and remediation* from the prior tabs. These are the risk analysis results.

ONC HIT Security Risk Assessment Questionnaire – Tab 1

TextBox 1 fx

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	HOW TO COMPLETE THE FORMS																	
2	<u>Introduction</u>																	
3	Completion of this tool will assist a practice in complying with Meaningful Use and the HIPAA Security Rule, but it is not a guarantee of compliance with either. Practices are still																	
4	obligated to comply with the specific requirements of each rule. Use of this tool will provide an overall view of the state of security and provide suggestions for remediation of																	
5	deficiencies. A complete risk assessment must address each asset type separately, which this tool does not do.																	
6																		
7	This Risk Assessment Tool contains a four-step process designed to enable respondents to identify their level of risk against pre-identified threats and vulnerabilities. The tool is designed for																	
8	ease of use and user-friendliness. Cells that populated on one table will be automatically populated on subsequent tabs to ensure accuracy and simplicity. The US Department of Health and																	
9	Human Services(HHS), Office for Civil Rights (OCR) references components of the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-66 and 800-30 as																	
10	guidance for a security risk assessment. NIST SP 800-66 is an introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and																	
11	NIST SP 800-30 is a risk management guide for information technology systems.																	
12																		
13	Background information on the nine primary steps to the risk assessment methodology outlined in NIST SP 800-66 and in NIST SP 800-30 is available on the next tab, labeled 800-66 Risk																	
14	Guidance . These steps offer helpful background information on the assessment steps, how they interact with one another and basic descriptions of risk and the components of risk, such as																	
15	threats and vulnerabilities. Internet links to NIST SP 800-66 and SP 800-30 are also provided for those seeking additional information.																	
16																		
17	<u>Purpose</u>																	
18	The purpose of a risk assessment is to identify conditions where Electronic Protected Health Information (EPHI) could be disclosed without proper authorization, improperly modified, or																	
19	made unavailable when needed. This information is then used to make risk management decisions on what reasonable and appropriate safeguards are needed to reduce risk to an																	
20	acceptable level.																	
21																		
22	This Risk Assessment Tool is intended to be a starting point for identifying cybersecurity risks to your organization.																	
23																		
24	<u>The Risk Assessment Tool Four-Step Process</u>																	
25	The following four-step process is provided for using the Risk Assessment Tool :																	
26																		
27																		
28																		
29																		
30																		
31																		
32																		
33																		
34																		
35																		
36																		
37																		
38																		
39																		
40																		
41																		
42																		
43																		
44																		
45																		
46																		
47																		
48																		
49																		
50																		
51																		
52																		
53																		
54																		
55																		
56																		
57																		
58																		
59																		
60																		
61																		
62																		
63																		
64																		
65																		
66																		
67																		
68																		
69																		
70																		
71																		
72																		
73																		
74																		
75																		
76																		
77																		
78																		
79																		
80																		
81																		
82																		
83																		
84																		
85																		
86																		
87																		
88																		
89																		
90																		
91																		
92																		
93																		
94																		
95																		
96																		
97																		
98																		
99																		
100																		

Ready 100%

HIT Security Risk Assessment Questionnaire: Tab 2

SP 800-66 – Risk Guidance - introductory resource guide for implementing the HIPAA Security Rule.

This risk guidance document delineates the steps to be taken to identify risk for an organization. Some of the steps can be conducted concomitantly.

Nine Primary Risk Assessment Steps

1. Scope the Assessment
2. Gather Information
3. Identify Realistic Threats
4. Identify Potential Vulnerabilities
5. Assess Current Security Controls
6. Determine the Likelihood and the Impact of a Threat Exercising a Vulnerability
7. Determine the Level of Risk
8. Recommend Security Controls
9. Document the Risk Assessment Results.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	NIST SP 800-66 RISK GUIDANCE																	
2	How to Conduct the Risk Assessment:																	
3	Risk assessments can be conducted using many different methodologies. There is no single methodology that will work for all organizations and all situations. The following steps represent																	
4	key elements in a comprehensive risk assessment program, and provide an example of the risk assessment. It is expected that these steps will be customized to most effectively identify risk																	
5	for an organization based on its own uniqueness. Even though these items are listed as steps, they are not prescriptive in the order that they should be conducted. Some steps can be																	
6	conducted simultaneously rather than sequentially.																	
7																		
8	1. Scope the Assessment.																	
9	The first step in assessing risk is to define the scope of the effort. To do this, it is necessary to identify where EPHI is created, received, maintained, processed, or transmitted. Ensure that																	
10	the risk assessment scope takes into consideration the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and																	
11	backup media).																	
12																		
13	2. Gather Information.																	
14	During this step, the covered entity should identify: The conditions under which EPHI is created, received, maintained, processed, or transmitted by the covered entity. It should also																	
15	identify the security controls currently being used to protect the EPHI.																	
16																		

This is a sampling of the steps as they appear in NIST SP 800-66 Risk Guidance

This is a sampling of the steps as they appear in NIST SP 800-66 Risk Guidance

SP 800-300 - risk management guide for information technology systems

Tab 3 Step 1 – Inventorying of Assets

- In this step you list devices at the practice that are touched by ePHI and whether they store, process or transmit the ePHI. Those devices that process ePHI, are categorized as either a People or Process assets or as a Technology asset.

Inventory Assets (Preparation)

Purpose: This tab may be helpful to respondents in determining what to consider in the population of assets in Steps 2a and 2b. The tab provides a space to list all potential assets and whether they process EPHI. If the asset processes EPHI, then decide if the asset is best suited as a People and Process asset or a Technology asset.

The following template, consistent with Step 1 of NIST Special Publications 800-66 and 800-30.

Using the Inventory Assets Tab:

The respondent should take a moment to carefully consider and reflect upon their complete asset inventory, then list the assets in the initial column. The respondent can then utilize the next column to consider whether or not the asset processes EPHI. If the asset does not process EPHI, then the asset does not need to be listed or considered for this analysis any further. If, however, the asset DOES process EPHI, then indicate the best category for the asset in the last column.

Respondents should distinguish assets in the following way:

People and Processes: Any asset(s) which processes, transmits or stores **Electronic Personal Health Information (EPHI)**. The assets may be used in an operational or administrative capacity, for business purposes or for sustainment of operations. As long as the asset usage impacts EPHI usage, then it should be listed in the tool.

Examples could include devices such as Desktop PCs, Fax Machines, Photo Copiers, Scanners, Mobile Computing Devices, Cell Phones/Smart Phones, Storage Servers, Monitors, Phones, Pagers, Network Connections, Internet Routers, Printer(s), Teleconferencing Equipment, Dictaphones, Software, Medical Equipment, Specialized Medical Devices (such as X-Ray, EKG, or EEG) or Portable Storage devices such as Thumb Drives.

NOTE: policies, procedures, organizational standards and guidance should all be considered and included in the Business Asset section.

Technology: This would be a list that exclusively contains the software package(s) which process EPHI. This may be any computer program from specialized medical software to the Microsoft Office suite of products such as Excel, Word or Access. Any software or computer program which processes, transmits or stores EPHI would be categorized in this section.

NOTE: If an asset does not process, store, or transmit EPHI, then it is NOT necessary to consider or include that asset on this list. The only consideration is whether or not EPHI is a factor in the usage of the asset.

Tab 4 Step 2 – Screening Questions

Users determine the degree to which their operations address the Threat-Vulnerability Statement – choosing from Addressed, Partially Address, or Not Addressed with space for comments.

- The response column is where the practice notes how the question is being addressed.
- The line items are parallel to the items in step 2a and 2b, but with a more user-friendly description.

Screening Questions (Step 1)

Purpose: The following tab is offered as a means for determining the degree to which threats and associated vulnerabilities apply to their organization’s assets. While this tab is an optional feature in the risk analysis, it is strongly recommended that the respondents utilize this workspace as these questions will assist in additional responses on Steps 2a and 2b.

Steps for Using the Screening Questions Tab (Step 1):

When examining each of the individual questions below, consider the question and your organizations current posture. Please select from the drop-down list as to whether your organization Addresses, Partially-Addresses or Does Not Address the security issue in question. There is no correct or incorrect response. The purpose of the risk analysis effort is to gauge the information security practices within medical facilities and where to best direct resources to remediate the areas of greatest concern. When the selection is made, the corresponding ‘Exposure Potential’ column in Steps 2a or 2b will automatically populate with the words, ‘High’, ‘Medium’ or ‘Low’ as a means of assisting the respondent in calculating their risk.

There will be a pre-selected Threat-Vulnerability Statement which will correspond to the question; *no action* is required for this cell. The respondent is offered this statement in consideration of what, if any, response they would like to offer in the last cell- Notes/Comments. The respondent may populate in this cell, any concerns they have or counter-measures they currently utilize relative to the question topic and Threat-Vulnerability Statement. This space is strictly a voluntary space and no action is required on the part of the respondent if they choose not to utilize this option. The pre-populated Threat-Vulnerability Statement will appear again in Steps 2a and 2b.

NEXT STEP: After completing the questions on this tab, please proceed to the tab labeled People and Processes (Step 2a).

Topic	Question	Response	Threat Vulnerability Statement	Notes/Comments
1. Security Program				
1.1 Roles & Responsibilities	[1.1] Has your organization formally appointed a central point of contact for security coordination? a) If so, whom, and what is their position within the organization? b) If there has not been a person appointed as the central point of contact, have security responsibilities been assigned to multiple individuals throughout the organization?		Management has not defined responsibilities for the information security program. [TVS001]	
	[1.2] Do you work with third parties, such as IT service providers, that have access to your patient's information?		Security breaches occur when dealing	

Tab 5 and 6

Step 2a People | Step 2b Processes & Technology

			Perform Control Analysis		Exposure		Assess Risk	
Business Asset (Anything processing, computing, storing or transmitting EPHI, one asset per cell)	Threat-Vulnerability Statement	Recommended Control Measures	Existing Control	Existing Control Effectiveness	Exposure Potential	Likelihood	Impact	Risk Rating
Security Program	Management has not defined responsibilities for the information security program. [TVS001]	All information security responsibilities are clearly documented . ¹ This is to ensure timely, safe and effective handling of all situations, administration user accounts- including additions, deletions, and modifications. ² [RCM001]	Enter answer	Select	Select	Select	Select	Calculated
Security Program	Security breaches occur when dealing with third parties due to a lack of security considerations in the related third party agreement. [TVS002]	Agreements with third parties, such as IT vendors, which involve accessing, processing, communicating with or managing the organization's information or information processing facilities, or adding products or services to information processing facilities cover all relevant security requirements ¹ Contracts between business associates and covered entities address administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of information ⁴ . [RCM002]						

Lists the Threat-Vulnerability Statement and Recommended Control Measures that are examples of threats in ePHI environments, and controls to mitigate these threats

Perform Control Analysis

Existing Control – measure taken to mitigate threats.

- ❑ **Enter** the *corrective actions* to mitigate threat/vulnerability

Control Effectiveness – Choose the degree in which counter measures address the threat vulnerability

- ❑ **Select** from – *Effective, Partially Effective, Not Effective*

Exposure

Exposure Potential – **Prepopulated** from Step 1 with very likely, likely, not likely (No action)

Assess Risk

Likelihood – **Select** from – very likely, likely, not likely

Impact Rating – consequences of a security event to the medical practice

- ❑ **Select** from - *high, medium, low*

Risk Rating – **automatic calculation** based on *impact rating and likelihood*. (no action)

Tab 7 – Step 4 – Findings and Remediation

Findings-Remediation (Step 3)

Purpose: This tab is the final stage of the data collection process. It is designed to develop a list of Business Assets or Applications that store, transmit, or process EPHI. These Business Assets help to identify the scope of what needs to be assessed and addresses Risk Assessment Step 9 of NIST SP 800-66 and 800-30.

Steps for Using the Findings-Remediation Tab (Step 3):

NOTE: All columns with the exception of the 'Additional Steps' column, are automatically populated based upon user input provided in the preceding tabs (Steps 1, 2a and 2b). Please allow a few moments for this tab to populate with the data from the previous tabs.

Risk Found - This column requires *no action* by the respondent and will self-populate from risks identified as being either MEDIUM or HIGH in the Risk Rating column from the previous Steps 2a and 2b tabs. If the risk is deemed LOW, then this is insignificant need not be considered further in the overall Risk Matrix.

Risk Rating - This column requires *no action* by the respondent and will self-populate from risks identified as being either MEDIUM or HIGH in the Risk Rating column from the previous Steps 2a and 2b tabs. Risk Rating would be the rating accompanying the Asset or Application. Only the Asset or Application in Steps 2a and 2b tabs as Medium or High are to be displayed and rated on this chart.

Existing Control Measures Applied - This column requires *no action* by the respondent and will self-populate from the Existing Control Measures are listed in the previous Step 2 (both Step 2a and 2b from the previous tabs). This is what corrective actions practitioner is taking, if any corrective actions are taken, to mitigate and reduce the threat or vulnerability. Control Measures can be an Alarm System, Sprinkler System or Computer Access restrictions and will be listed again in this space.

Recommended Control Measures - This column contains the Recommended Control Measures which self-populated in Steps 2a and 2b on the previous tabs. This column requires *no action* by the respondent and will self-populate.

Additional Steps: The response is a judgment by the practitioner as to what supplemental measures may be taken, within the current availability of resources, to achieve a sound state of security and to ensure the continuation of operations. There is no right or wrong answer. This is an opportunity for the respondent to consider and document any additional measures they wish to take to address and reduce the risk.

NEXT STEP (OPTIONAL): The final step in this risk assessment process is to talk to your local Regional Extension Center (REC) for clarification and additional information.

Number of High Risks 0

Number of Medium Risks 0

Total Number of High and Medium 0

High and Medium Risks Findings and Remediation

Risks Found (High and Medium Only)	Risk Rating	Existing Control Measures Applied	Recommended Control Measures	Additional Steps
------------------------------------	-------------	-----------------------------------	------------------------------	------------------

People and Processes				
Technology				

Tab 7 – Step 4 – Findings and Remediation

This worksheet is mostly pre-populated

The number of high and medium risks are counted

Items below are automatically calculated. The user doesn't enter data.

- **Risk found** – Those with risk found to be Medium and High risks in 2a and 2b
- **Risk rating** – The rating from 2a and 2b
- **Existing control measure applied** – corrective actions to mitigate
- **Recommended control measures**

Additional steps – ADDED by user – can list the supplemental measures that the practitioner plans to take

This becomes a take-away sheet where the risks identified in the prior steps are gathered.

REC Update Changes to the ONC Tool

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Practice Summary														
2															
3	Last Revision Date														
4	Contributors (persons involved with the assessment)														
5															
6	Practice Information														
7	Practice Name														
8	Contact Information (Practice Point of Contact)		Name:												
9	Office Locations		Email:												
10			Phone:												
11	FHR Information														

Added a Practice summary tab seen above.

Added columns to the findings-remediation tab to document the steps being taken and the timeframe to mitigate the risks that are being addressed.

15						
19	Number of High Risks	0				
20	Number of Medium Risks	0				
21	Total Number of High and Medium Risks	0				
23	High and Medium Risks Findings and Remediation					
24	Risks Found (High and Medium Only)	Risk Rating	Existing Control Measures Applied	Recommended Control Measures	Owner	Remediation Steps
25	People and Processes					
62	Technology					
101						
102						
103						
104						

Information Security Policy Manual for the Practice

- The Information Security Policy Manual should be customized and updated frequently with the specific privacy and security safeguards and risk mitigation techniques implemented at the practice.
- These safeguards emanate from the output of the ONC HIT Security Risk Assessment Questionnaire in the prior step. Copies of the manual should be available for practice staff to reference. New staff should be familiarized with the manual as part of privacy and security training

Information Security Policy Manual for the Practice

INFORMATION SECURITY POLICY
POLICY AND PROCEDURE



Last Revision Date

Document Owner

Information Security Policy

Company Name or Logo		Policy and Procedure	
Title: NETWORK CONNECTIVITY	P&P #: IS-1.3		
Approval Date: Date	Review: Annual		
Effective Date: Date	Information Technology		

Network Connectivity

Dial-In Connections

Access to Practice information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. Direct inward dialing without passing through the access control system is prohibited.

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

Dial Out Connections

Practice provides a link to an Internet Service Provider. If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place.

Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Privacy Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones

Information Security Policy

- Blackberry type devices
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

Permanent Connections

The security of Practice systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Practice systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

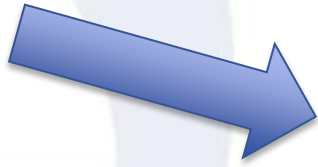
Emphasis on Security in Third Party Contracts

Access to Practice computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Practice Information Security Policy have been reviewed and considered.
- Policies and standards established in the Practice information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Practice computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon

Information Security Policy - Instructions

- Instructions



INFORMATION SECURITY POLICY INSTRUCTIONS

The Information Security Policy Template that has been provided requires some areas to be filled in to ensure the policy is complete. Once completed, it is important that it is distributed to all staff members and enforced as stated. It may be necessary to make other adjustments as necessary based on the needs of your environment as well as other federal and state regulatory requirements.

Items highlighted in **Red** within the template are required and items highlighted in **yellow** may require some adjustments based on your environment. Each highlighted item has a number afterwards which is referenced below to assist you in the completion of this policy template.



Number	Value	Description
1	Company Name/Logo	Company name or logo of organization.
2	Last Revision Date	Last revision date of the Information Security Policy.
3	Document Owner	Document owner of the policy. This is usually someone at an executive level.
4	Approval Date	Date that the policy has been officially approved
5	Effective Date	Effective date of the policy. This can be a different than the approved date if needed.
6	Company Name	Company/Practice name. No logo used for this particular part of the policy.
7	Outside Agencies	List any outside agencies or organizations, if applicable, whose laws, mandates, directives, or regulations were included in the policy, i.e. CMS, DHHS, VHA, etc.
8	Privacy Officer	List the name and phone number of the person designated as the Privacy Officer.
9	CST Team	List the title and name of the individuals that will become part of Confidentiality and Security Team.
10	Contractor Access	For contractors that enter the building, specify what identifying

Information Security Policy Manual for the Practice

Policies and procedure templates for inclusion in the practice manual include:

- IS-1.0 Introduction
- IS-1.1 Employee Responsibilities
- IS-1.2 Identification and Authentication
- IS-1.3 Network Connectivity
- IS-1.4 Malicious Code
- IS-1.5 Encryption
- IS-1.6 Building Security
- IS-1.7 Telecommuting
- IS-1.8 Specific Protocols and Devices
- IS-1.9 Retention / Destruction of Paper Documents
- IS-1.10 Disposal of External Media / Hardware
- IS-2.0 Emergency Operations Procedures
- IS-3.0 Emergency Access "Break Glass" Procedures
- IS-4.0 Sanction Policy
- IS-5.0 e-Discovery Policy "Production and Disclosure"
- IS-5.1 e-Discovery Policy "Retention"
- IS-6.0 Breach Notification Procedures
- Appendix A: Network Access Request Form
- Appendix B: Confidentiality Form
- Appendix C: Approved Software
- Appendix D: Approved Vendors
- Appendix E: Breach Assessment Tool

NYeC Privacy and Security Toolkit

We at NYeC have developed this toolkit as a framework for educating stakeholders about the privacy, security and risk mitigation guidelines to be followed at provider practices.

Sharon Bari

Training Specialist

New York eHealth Collaborative

sbari@nyehealth.org

646 619 6503

Thanks to

Katie O'Neill

Senior V. P. and HIV/AIDS Projects Director

Legal Action Center

Resources

- HHS Health Information Privacy
<http://www.hhs.gov/ocr/privacy/index.html>
- HHS Frequently Asked Questions:
<http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>
- HHS Office for Civil Rights (OCR)
<http://www.hhs.gov/ocr/office/index.html>
- HITECH Act Reports to Congress
<http://www.hhs.gov/ocr/privacy/hitechrepts.html>
- OCR Enforcement
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html>

Resources

- American Health Information Management Association (AHIMA)
<http://www.ahima.org/resources/>
- Healthcare Information and Management Systems Society
www.himss.org
- HCPRO HIPAA Update Blog <http://blogs.hcpro.com/hipaa/>
- National Institute of Standards & Technology – EHR Testing Requirements:
http://healthcare.nist.gov/use_testing/effective_requirements.html
- SAMHSA <http://www.samhsa.gov/healthprivacy>

DISCLAIMER: NYeC has provided the information contained in the toolkit to guide practices and Medicaid Health Homes (collectively, Providers) through the process of complying with Meaningful Use and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. Use of the toolkit is meant to increase awareness of recommended safeguards and to alert Providers to potential deficiencies in the management and protection of electronic health information. Conformity with the practices outlined in these materials does not guarantee compliance with any particular component of HIPAA or Meaningful Use and should not be considered legal advice. Use of this toolkit does not ensure a Provider's compliance with applicable Federal and State laws; Providers should consult an attorney for individualized legal advice on adherence to such laws

HH Implementation Session 3: Optimizing the Practice Workflow

Presenters: Dr. Alan Silver, Medical Director, IPRO

Jaclyn Brinson, Program Manager, NYeC

Date & Time: Wednesday, March 7, 2012 2:30 pm eastern time

Registration Link: <https://cc.readytalk.com/r/ra9jluql5eu2>

All training sessions (recordings and registrations) will be made available on the Medicaid website.

http://www.health.ny.gov/health_care/medicaid/program/medicaid_health_homes/ohitt_ehr_webinars.htm

HH Implementation Session 4: EHR 101

Presenter: Denise Reilly, Executive Director, eHealth Network of Long Island

Date & Time: Thursday, March 8, 2012 10:00 am eastern time

Registration Link: <https://cc.readytalk.com/r/1taxzb51nwfs>

All training sessions (recordings and registrations) will be made available on the Medicaid website.

http://www.health.ny.gov/health_care/medicaid/program/medicaid_health_homes/ohitt_ehr_webinars.htm