Security Risk Assessments:

Meaningful Use and HIPAA Perspectives

Wednesday, August 26, 2015

Adam Kehler, HIT Privacy & Security Specialist

Nicholas Heesters, JD, CIPP,

HIT Privacy & Security Specialist

Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES

Quality Insights
Quality Innovation Network

Disclaimer

- The information included in this presentation is for informational purposes only and is not a substitute for legal advice.
- Please consult your attorney if you have any particular questions regarding specific legal issues.

Agenda

- Introduction
- Goals
- Meaningful Use and HIPAA
- Myths & Facts
- What is a Risk Analysis?
- Definitions
- Elements of a Risk Analysis
- Risk Management
- Next Steps

Introduction

Adam Kehler, CISSP
Privacy and Security Specialist
PA REACH East & West
akehler@wvmi.org

Introduction

- PA REACH East & West
  - Regional Extension Center for Meaningful Use
  - Created by HITECH Act of 2009
  - Provide assistance to organizations attempting to achieve Meaningful Use

West Pennsylvania East
REACH
Regional Extension &
Assistance Centers for HIT

LEGAL AND COMPLIANCE REQUIREMENTS

Legal and Compliance Requirements

- HIPAA/HITECH
- Meaningful Use
- FISMA (HIX, HIE, ACO, NIH Grants)
- Medicare/Medicaid Systems

Meaningful Use

- In Stage 1, eligible professionals (EPs) must 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.
- In Stage 2, EPs need to meet the same security risk analysis requirements as Stage 1, but must also address the encryption/security of data at rest.
- Note: a security risk analysis needs to be reviewed and updated for each reporting period for Stage 1 and Stage 2.

HIPAA Security Rule

- “Under the HIPAA Security Rule, you are required to conduct an **accurate and thorough analysis** of the potential risks and vulnerabilities to the **confidentiality, integrity, and availability** of ePHI. Once you have completed the risk analysis, you must take any additional “reasonable and appropriate” steps to reduce identified risks to reasonable and appropriate levels. (45 CFR 164.308(a)(1)(ii))”

MYTHS & FACTS

Myths & Facts

- Myth or 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.

Myths & Facts

- Myth or Fact:
  - 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.

Myths & Facts

- Myth or Fact:
  - 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.

Myths & Facts

- Myth or Fact:
  - I have to outsource the security risk analysis.

False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.

Myths & Facts

- Myth or Fact:
  - I only need to do a risk analysis once.

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

Under meaningful use, reviews are required for each EHR reporting period.

WHAT IS A SECURITY RISK ANALYSIS?

What is a Security Risk Analysis?

- There is no single method or “best practice” that guarantees compliance
- But most risk analysis and risk management processes have steps in common.
- OCR and NIST have provided guidance and recommendations.

What is a Security Risk Analysis?

- In medical terms:
  - Just as you use a diagnosis and other clinical data to plan treatment, you will use the risk analysis to create an action plan to make your practice better at protecting patient information.
  - Privacy and security are like chronic diseases that require treatment, ongoing monitoring and evaluation, and periodic adjustment.

Definition of Vulnerability

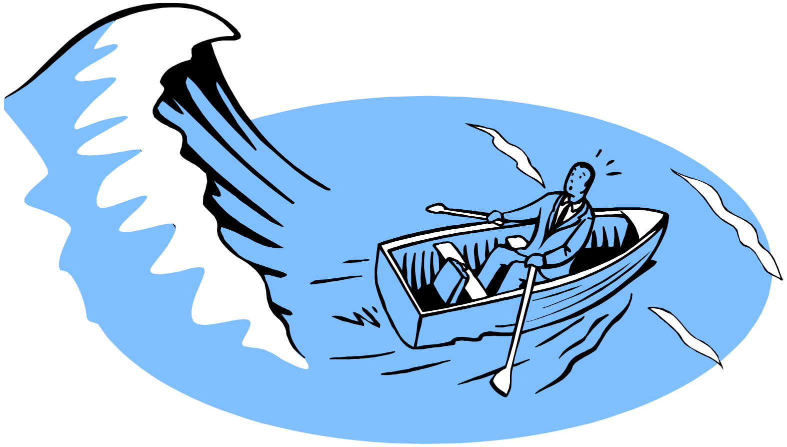
- **Vulnerability** is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

Examples of Vulnerabilities

- Examples of vulnerabilities
  - Technical
    - Unpatched systems
    - Weak, default, or no passwords
    - PHI on unencrypted media
    - Poorly configured firewalls or servers
    - Open wireless networks or using weak encryption
  - Non-Technical
    - Lack of security awareness training
    - Lack of or ineffective policies and procedures

Definition of Threat

- A **Threat** may be defined as: “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”

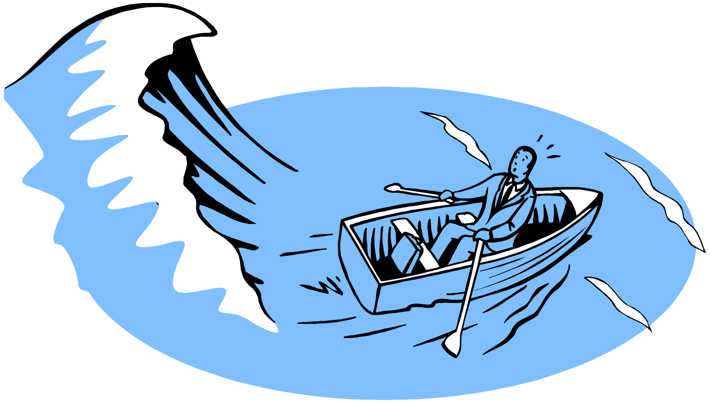


Examples of Threats

- Examples of threats:
  - Natural
    - Flood, earthquake, tornado, ice storm, fire
  - Human
    - Outsiders such as hackers, patients
    - Workforce members, contractors
    - May be intentional or unintentional (i.e. inadvertent modification, deletion, or disclosure of information)

Definition

- A **Risk** can then be defined as: *“The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur.*



What is Security Risk Analysis?

- “An accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.”

ELEMENTS OF A SECURITY RISK ANALYSIS

Elements of A Risk Analysis

- As defined by OCR/NIST:
  - Step 1: Define the scope
  - Step 2: Data collection
  - Step 3: Identify and document potential threats to ePHI
  - Step 4: Assess current security measures
  - Step 5: Determine the likelihood of threat occurrence
  - Step 6: Determine the potential impact of threat occurrence
  - Step 7: Determine the level of risk
  - Step 8: Finalize documentation
  - Step 9: Regular risk analysis

Elements of A Risk Analysis

- Step 9: Continuous Risk Analysis
- A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation
  - For example, evaluate security risks when you:
    - Have experienced a security incident
    - Have change in ownership, turnover in key staff or management
    - Are planning to incorporate new technology to make operations more efficient
    - Are making changes to your servers or network devices
    - Are changing workflows

Risk Management

- Develop an action plan based on risk level, priority, budget, business drivers
- Determine “reasonable and appropriate” safeguards that will mitigate the risk to an acceptable level
- Consider administrative, physical, and technical safeguards; policies and procedures; and organizational standards.

Resources

- HealthIT.gov
  - Guide to Privacy and Security of Health Information
  - Mobile Device Privacy and Security
  - Privacy and Security Training Games
  - Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices
  - Security Risk Assessment Tool
- The Office of Civil Rights
  - Guidance on Risk Analysis Requirements under the HIPAA Security Rule
- The National Institute for Standards in Technology (NIST)
  - SP 800-30 Guidance for Conducting Risk Assessments
  - SP 800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule
  - HIPAA Security Rule Toolkit
- Your Regional Extension Center - Privacy & Security Toolkit

Resources

- Security Trends
  - OCR HIPAA Enforcement Data
    - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
  - Reports of breaches affecting 500 or more individuals
    - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
  - Verizon Data Breaches Investigation Report
    - http://www.verizonenterprise.com/DBIR/2013/
  - Symantec Annual Threat Report
    - http://www.symantec.com/security_response/publications/threatreport.jsp

2015 Phase 2 HIPAA Audits

Nicholas P. Heesters, Jr., JD, CIPP
Health IT Privacy & Security Specialist, Quality Insight of Delaware – REC
877.987.4687, Ext. 136 | nheesters@wvmi.org | www.dehitec.org

HIPAA Audits: Timeline

- 2009 HITECH Act Mandates HIPAA Audits
- 2012 HIPAA Audits (Phase 1)
- 2013 Evaluation of HIPAA Audits (Phase 1)
- 2014 HIPAA Audits (Phase 2) Delayed
- 2015 HIPAA Audits

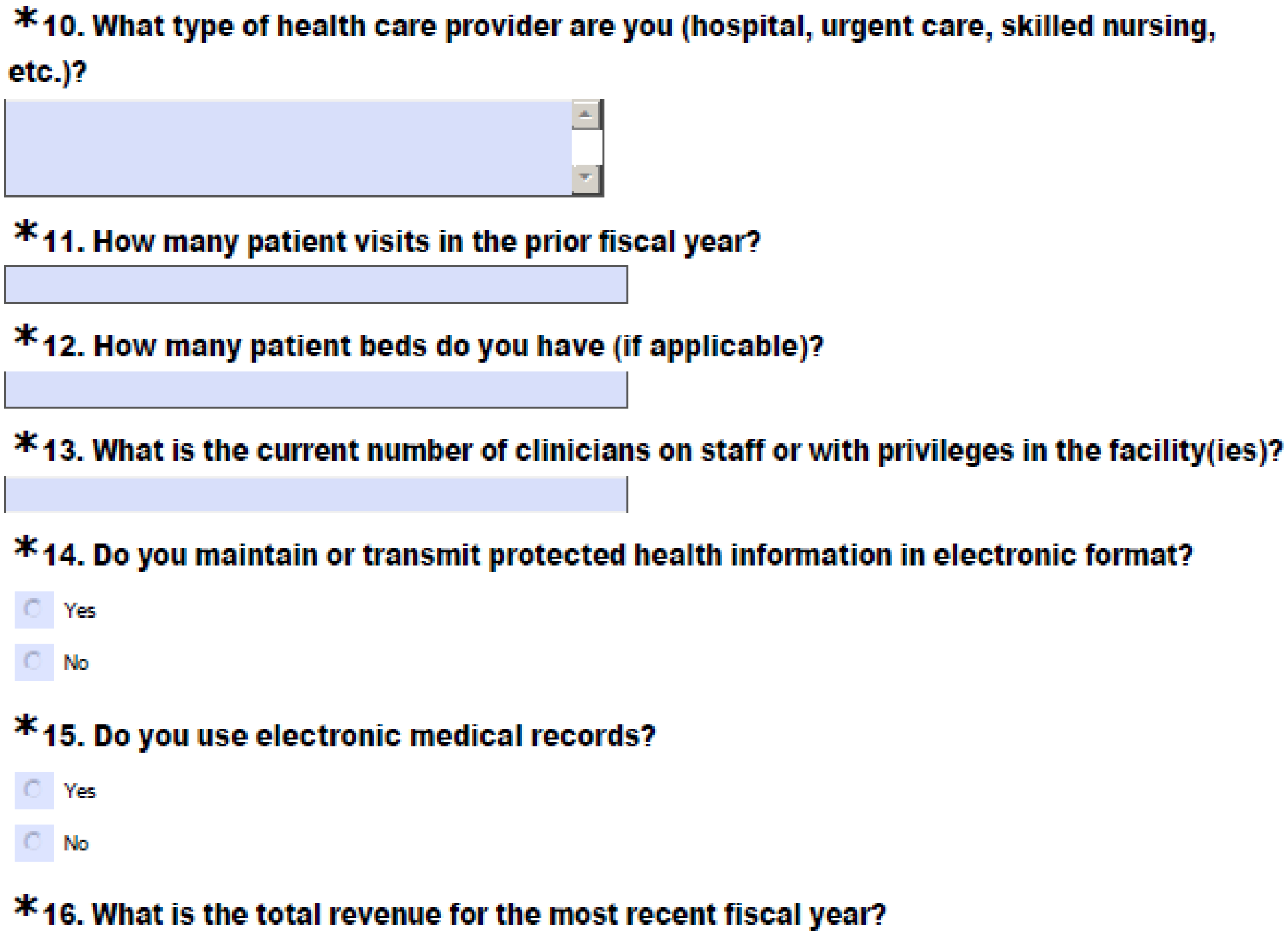
HIPAA Audits: Phase 2

- Who can be audited?
- Covered Entities
  - Healthcare clearing houses
  - Healthcare plans
  - Providers (individual and organizational)
    - Dental, behavioral health, physicians, laboratories, etc.
- Business Associates

HIPAA Audits: Phase 2

- Phase 2 HIPAA Pre-Audit Survey
  - HIPAA pre-audit surveys were mailed in May 2015
  - Information requested included an entity’s size, business location(s), services, revenue, number of patient visits or insured lives, use of EHR system(s), and best contacts

HIPAA Audits: Phase 2



*10. What type of health care provider are you (hospital, urgent care, skilled nursing, etc.)?

*11. How many patient visits in the prior fiscal year?

*12. How many patient beds do you have (if applicable)?

*13. What is the current number of clinicians on staff or with privileges in the facility(ies)?

*14. Do you maintain or transmit protected health information in electronic format?

○ Yes

○ No

*15. Do you use electronic medical records?

○ Yes

○ No

*16. What is the total revenue for the most recent fiscal year?

HIPAA Audits: Phase 2

- Phase 2 Audit Differences
  - Audits will focus on findings from Phase 1 audits
  - Audits will be conducted in-house (OCR resources, not contractors)
  - Audits will be primarily “desk” audits; although OCR indicated that it may pursue more on-site audits

HIPAA Audits: Phase 2

- Audit Response Expectations
  - **Completeness**: Data requests will specify content and document submission requirements
  - **Timeliness**: Only responses submitted on-time will be considered
  - **Currency**: Submitted documentation must be current as of the date of the data request
  - **Concise**: Extraneous data may make it difficult for auditor to assess submitted documentation
  - **Accuracy**: there will not be an opportunity for auditors to request clarifications

HIPAA Audits: Phase 2

- Audit Focus Security
  - Risk Analysis
    - Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI
      - Vulnerability: Flaw or weakness in system security which can lead to a security breach
      - Threat: Potential to exercise a vulnerability
        - » Natural (floods, earthquakes, etc.)
        - » Human (malicious attacks, inadvertent deletion, etc.)
        - » Environmental (power failure, chemical spill, etc.)
      - Risk: Likelihood a threat can exploit a vulnerability resulting in an impact

HIPAA Audits: Phase 2

- Audit Focus Security
  - Risk Analysis (continued)
    - Steps:
      - Identify scope, gather data, identify threats and vulnerabilities, assess current measures, determine likelihood of threat occurrence, determine impact of threat occurrence, determine level of risk, identify security measures and document
    - Annually or as needed (e.g., biennially, every 3 years)
    - NIST SP 800-30
    - Ensure that a current and up to date security risk analysis is in place and documented
    - Ensure that the risk analysis categorizes risk and is not solely a gap analysis or checklist

HIPAA Audits: Phase 2

- Audit Focus Security
  - Risk Management
    - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule.
    - Steps
      - Develop and implement a risk management plan
      - Implement security measures
      - Evaluate and maintain security measures
    - Ensure that the risk management policy includes the process for correcting deficiencies identified by the risk assessment
    - Security measures must be reviewed and updated to ensure reasonable and appropriate protection of ePHI

HIPAA Audits: Phase 2

- Risk Management Considerations
  - Size, complexity and capabilities
  - Technical infrastructure, hardware, and software security capabilities
  - Security measure costs
  - Probability and criticality of potential risks to ePHI

HIPAA Audits: Phase 2

- Audit Focus Security
  - Anchorage Community Mental Health Services (Dec. 2014)
    - ACMHS failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality integrity, and availability of e-PHI held by ACMHS (See 45 C.F.R. § 164.308(a)(1)(ii)(A))
    - ACMHS failed to implement policies and procedures requiring implementation of security measures sufficient to reduce risks and vulnerabilities to its e-PHI to a reasonable and appropriate level (See 45 C.F.R. § 164.308(a)(1)(ii)(B))
    - HHS has agreed to accept, and ACMHS has agreed to pay HHS, the amount of $150,000

HIPAA Audits: Phase 2

- Audit Focus Security
  - Affinity Health Plan (Aug. 2013)
    - AHP failed to assess and identify the potential security risks and vulnerabilities of EPHI stored in photocopier hard drives.
    - AHP agrees to pay HHS the amount of $1,215,780
  - Idaho State University (May 2013)
    - ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from 4/1/07 until 11/26/12
    - ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from 4/1/07 until 11/26/12
    - ISU agrees to pay HHS the amount of $400,000

HIPAA Audits: Phase 2

- Audit Focus Privacy
  - Notice of Privacy Practices (NPP)
    - How the covered entity may use and disclose PHI.
    - The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.
    - The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of PHI.
    - Whom individuals can contact for further information about the covered entity's privacy policies.
    - Omnibus Rule updates required in 2013

HIPAA Audits: Phase 2

- Audit Focus Privacy
  - Patient Access to Health Records
    - An individual’s right to access his or her PHI is a critical aspect of the Privacy Rule, which naturally extends to an electronic environment.
    - The Privacy Rule establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their PHI, to the extent it is maintained in the designated record set(s) of a covered entity.
    - Ensure that policies and supporting documentation are in place regarding actual patient access requests and outcomes.

HIPAA Audits: Phase 2

- Audit Focus Privacy
  - Cignet Health (Feb. 2011)
    - Cignet failed to provide 41 individuals timely access to obtain a copy of their PHI in the designated record sets maintained by Cignet. These failures constitute violations of 45 C.F.R. § 164.524. Cignet's failure to provide each individual with access constitutes a separate violation of 45 C.F.R. § 164.524, and each day that the violation continued counts as a separate violation of 45 C.F.R. § 164.524.
    - Pursuant to the authority delegated by the Secretary of the United States Department of Health and Human Services (HHS) to the Director of the Office for Civil Rights (OCR), I am writing to inform you that the civil money penalty (CMP) of $4,351,600 against Cignet Health is final.

HIPAA Audits: Phase 2

- Audit Focus Breach Notification
  - Breach: the acquisition, access, use, or disclosure of PHI in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the PHI.
  - Any impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised.
  - Exclusions:
    - Unintentional access by authorized workforce member acting in good faith
    - Inadvertent disclosure by authorized workforce member to authorized workforce member of the same organization
    - Good faith belief that an impermissible disclosure to an unauthorized person could not reasonably be retained

HIPAA Audits: Phase 2

- Audit Focus Breach Notification
  - Four Factor Risk Assessment
    - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
    - The unauthorized person who used the PHI or to whom the disclosure was made
    - Whether the PHI was actually acquired or viewed
    - The extent to which the risk to the PHI has been mitigated
  - Safe-Harbor for Secured PHI
    - Electronic PHI: destruction, encryption
    - Paper PHI: destruction

HIPAA Audits: Phase 2

- Audit Focus Breach Notification
  - Ensure that breach notification policies are in place and documented including the 2013 Omnibus Rule four factor risk assessment
  - Ensure that supporting documentation is available regarding breach investigations including:
    - Actual breach notices sent
    - Timelines of breach activities
    - Breach notification determinations

HIPAA Audits: Phase 2

- Audit Focus Breach Notification
  - Skagit County, Washington (Mar. 2014)
    - Skagit County failed to provide notification as required by the Breach Notification Rule (See 45 C.F.R. § 164.404) to all of the individuals for whom it knew or should have known that the privacy or security of the individual’s ePHI had been compromised as a result of the breach incident
    - Skagit County agrees to pay HHS the amount of $215,000
  - Adult and Pediatric Dermatology (Dec. 2013)
    - The Covered Entity did not fully comply with the administrative requirements of the Breach Notification Rule to have written policies and procedures and train members of its workforce regarding the Breach Notification requirements
    - The Covered Entity agrees to pay HHS the amount of $150,000.00

HIPAA Audits: Future

- Audit Focus Security
  - Device and Media Controls
    - Disposal
    - Media Re-use
    - Accountability
    - Data Backup and Storage
  - Transmission Security
    - Integrity Controls
    - Encryption
- Audit Focus Privacy
  - Implemented Safeguards
    - Physical, written, verbal
  - Training

HIPAA Audits: Future

- During a January 2015 media briefing, OCR Director Samuels stressed HIPAA compliance areas including:
  - Comprehensive Risk Analysis and Risk Management Practices
  - Ignoring identified threats and hazards
  - Insufficient policies and procedures
  - Training of workforce members

HIPAA Enforcement

- Civil:
  - $100 to $50,000 per breach ($1.5 million calendar year cap; was $25,000 pre-HITECH)
- Criminal:
  - $50,000 - $250,000 fine and/or 1–10 years in federal prison
- State attorneys general permitted to civilly sue on behalf of affected residents

Resources

- Additional Resources:
  - http://www.hhs.gov/ocr/privacy/
  - http://scap.nist.gov/hipaa/
  - http://healthhit.gov
  - http://www.himss.org/library/healthcare-privacy-security/toolkit
- My contact information
  - Nick Heesters – QIDE REC
  - Office: 877.987.4687 x136
  - Email: nheesters@wvmi.org
  - Web: www.dehitrec.org

Quality Insights of Delaware REC Where Quality and Health Information Technology Converge

NJ Health Information Technology Extension Center

- Offer two types of Privacy and Security services: an online privacy and security assessment tool or an in-depth privacy and security analysis.
- Cost varies depending on eligibility with the EHR Incentive Program.
  - If provider is eligible under one of the grant programs, services are free.
  - If not eligible, costs vary from a one time fee of $100 to a fee of $2,000 or $3000, depending on the size of the practice and services performed.
- Contact Balavignesh Thirumalainambi, MS, MBA, CPHIMS, CHTS – CP, Meaningful Use Director, Chair - Meaningful Use CoP Advisory Committee at ONC, BalaT@njhitec.org or info@njhitec.org
- Website: www.njhitec.org

NJ-HITEC™
Your Trusted Advisor for Meaningful Use & Health IT

Louisiana Health Information Technology Resource Center

- Privacy and Security services:
  - Learn how HIPAA security rules apply to your practice
  - Ensure that your practice has a long-term plan for remaining compliant with HIPAA rules
  - Receive privacy and security “best practices”
- To learn more about the LHIT Resource Center and full/custom service packages, call: 225.334.9299 or e-mail rec@lhcqf.org

LOUISIANA HEALTH
INFORMATION TECHNOLOGY
RESOURCE CENTER

Quality Insights HIT Team – State Contacts

- **Delaware:** Kathy (Rivard) Wild
  - krivard@wvmi.org
  - 877.987.4687, Ext 108
- **Louisiana:** Chris Gatlin
  - christine.gatlin@hcqis.org
  - 225.248.7035
- **New Jersey:** Carolyn Hoitela
  - carolyn.hoitela@area-J.hcqis.org
  - 732.238.5570
- **Pennsylvania:** Joe Pinto
  - jpinto@wvmi.org
  - 877.346.6180, Ext. 7817
- **West Virginia:** Paula Clark
  - pclark@wvmi.org
  - 304.346.9864, Ext. 3483

Question & Answer Session

Thank you for joining us.

Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES

Quality Insights
Quality Innovation Network

Please take a brief moment to complete the evaluation at the conclusion of this session.

This material was prepared by Quality Insights, the Medicare Quality Innovation Network-Quality Improvement Organization for West Virginia, Pennsylvania, Delaware, New Jersey and Louisiana under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. Publication number QI-B4-082615.