HIPAA Risk Assessment Tool for Physician Practices

May 10, 2011

Overview / Agenda

- Risk Factors
  - Identify compliance questions
  - Assign weight to questions
  - Develop risk level parameters
- Risk Analysis
  - create and distribute survey
  - incorporate responses
- Summary of Results
- Statistics

Risk Factors: Identification – Privacy

- Example: Risk Area
  - Section One– Area One: NPP
  - Section One – Area Three: Authorizations
- Example: Risk Factors:
  - Question 1 – NPP Distributed
  - Question 6 – NPP Posted
  - Questions 1 & 2 – Authorizations reviewed for validity

Risk Factors: Identification – Security

- Example: Risk Area
  - Section Three: Individual Authentication of Users
  - Section Three: Physical Security & Disaster Recovery
- Example: Risk Factors:
  - Question 1 – Unique individual identifier
  - Question 10 – Account canceled when employee leaves
  - Question 6 – Burglar alarm monitored by police
  - Question 9 – Disaster recovery plan in place

Risk Factors: Weight –Privacy

- Assign a weight to each risk factor.
  - For example: greatest liability
    - Question 1 – NPP distribution = 3
    - Question 7 – NPP updated, valid = 3

Risk Factors: Weight – Security

- Assign a weight to each risk factor for checklist questions.
  - For example: greatest liability
    - Question 1 – Unique identifier for each user = 3
    - Question 10 – Account canceled when employee leaves = 3

Risk Factors: Levels of Risk – Privacy

- Develop parameters for determining compliance levels across each compliance question.

  Example: Section One – Area Three– Questions 1 & 2 – Authorizations reviewed for validity

  - Level I : Process clearly identified and p/p submitted
  - Level II – Process not clearly identified or p/p not submitted
  - Level III – Process not identified and p/p not submitted

Risk Factors: Levels of Risk – Security

- Develop parameters for determining compliance levels across each compliance question.
  - Risk Level I – "Doing it Now," "Not Needed," or "Does not Apply"
  - Risk Level II – "In the Future"
  - Risk Level III – "Too Expensive," "Don't Know"
  - NOTE: For "Orange" highlighted questions only, responses of "Does Not Apply," "Not Needed," "Too Expensive" or "Don't Know" = Automatic Risk Level III

Risk Analysis: HIPAA Audit Survey

- Create HIPAA Audit Survey Tool
  - Determine which questions to ask
  - Organize questions by significant areas
- Distribute Survey to practice groups/sites

Risk Analysis: Incorporating Responses

- Collect survey responses from practice groups/sites
- Use parameters (from each compliance level) to evaluate answers to each survey question
- Insert results into “Risk Analysis” tab (of Risk Assessment Tool) for each practice group/site

Risk Analysis: Incorporating Responses Example

- Privacy: (Example – NPP)
  - Section One, Area One
    - Question 1
    - Question 6
- Security: (Example – Unique Identifier)
  - Section Three, Individual Authentication of Users
    - Question 1
    - Question 10

Summary of Results

- Analyze results from the “Summary” tab
  - By area/section
    - 2 privacy sections
    - 1 electronic security section
  - By practice group/site

- Determine audit focus based upon summary analysis

Statistics

- May utilize statistics to determine the order of the audit schedule
- May integrate graphs for comparison across groups or risk factors

Questions?

Marian Hughlett, CHC, CHRC
Privacy Officer, University of Louisville
Office: (502) 852-4533
marian.hughlett@louisville.edu

Robin L. Wilcox, CPA, CHC, CCEP
Institutional Compliance Officer, University of Louisville
Office: (502) 852-1371
robin.wilcox@louisville.edu