HIPAA
ADMINISTRATIVE SIMPLIFICATION

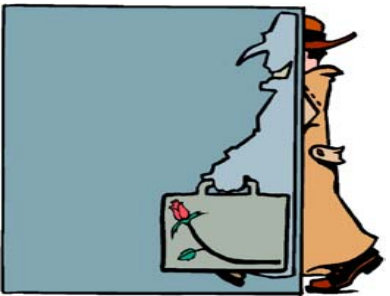
HIPAA Security

A Quantitative and Qualitative Risk Assessment

Rosemary B. Abell

Director, National Healthcare Vertical

Keane, Inc.



HIPAA Summit VII

September 14-16, 2003

Overview

- The Data Security issue –
  - Why listen to this presentation?
  - What do we need to do – Security Gap Assessment?
- Gap Analysis VS Risk Assessment
  - Goals of a Risk Assessment
  - How to perform a Risk Assessment
- Lesson Learned

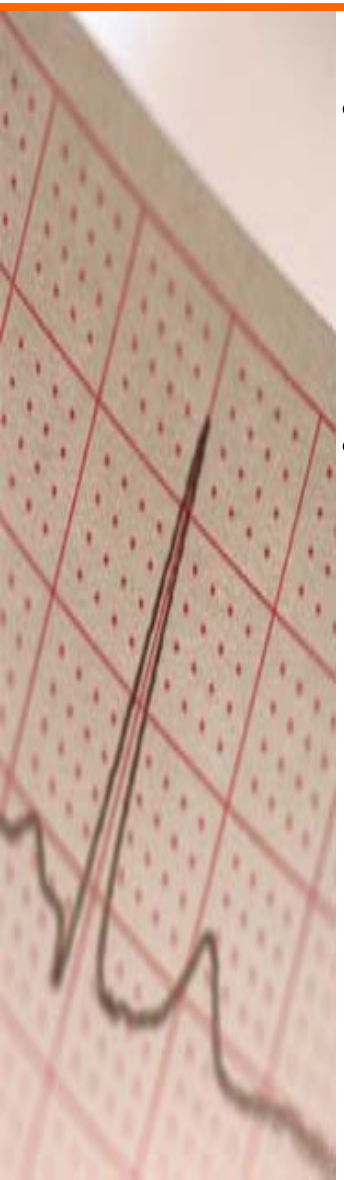
HIPAA Security

Why are you here?

Things to Think About?

- What grade would you get on your security plan if your DOI commissioner walked into your organization today?
- If you found out you had a security breach, what 3 areas come to mind?
- What tools and process do you use to explain to your senior management that you really studied your security plan?

Things to Think About?



- When you are in the witness box, how many of you can say that someone else certified your network?
- If it came across the national news that there are truck full of paper claims laying on the highway, how many of you would pick up the phone and call your management to see if it was your organization?

HIPAA Security

What To Do?

Why conduct a Security Assessment?

- Provide an understanding of the impact of HIPAA legislation on business operations and technology infrastructure
  - Identify gaps between current business and technical environments compared to the requirements of HIPAA
  - Evaluate the significance of the vulnerabilities (Risks) in the context of the organization's operations

What do we need to do?

1. Plan
2. Gather Data
3. Analyze Data
4. Assess Risk

Plan

- Kickoff meeting to provide an understanding of the security assessment process
  - Identify the people involved, confirm staff to be interviewed
  - Identify the security assessment approach
  - Identify the steps to be taken
  - Review high level milestones

Gather Security Data

- Customize security assessment questionnaire for HIPAA specifications
- Assign appropriate questions to representatives from functional areas
- Interview representatives from functional areas using the applicable questionnaires
- Record data

Conduct Gap Analysis

- Compile results of questionnaires
- Identify gaps
- Develop gap analysis report to reveal gaps in compliance between the current environments and the HIPAA requirements

HIPAA Security

Gap Analysis
VS
Risk Assessment?

Gap Analysis vs. Risk Assessment

- The gap analysis compares where we are to where we need to be in relation to HIPAA compliance. It helps determine the areas where the organization has vulnerabilities
- The risk assessment will be used to evaluate the significance of the vulnerabilities in context of the organization's operations

Risk Assessment

- The questions you are trying to answer in the risk assessment are:
  - What could compromise the confidentiality,integrity and availability of the health information in our possession?
  - If that information is compromised what is the impact to our business or to the individual?
  - What is the probability that it will happen?

How to perform a Risk Assessment

- The Risk areas rank the relative impacts of “not compliant” responses to the organization.
  - Qualitative Risks: based on values associated with each of the questions asked in the assessment questionnaire. If a “not compliant” answers implies a solution that typically requires a significant effort to achieve compliance, it carries a high qualitative. Medium and low qualitative risk values are assigned for those with correspondingly lower typical efforts. When summarized for a section, this value gives an indication of the average level of effort that will be needed for compliance activities.
  - The Quantitative Risks reflect the counts of “not compliant” responses within the set of questions for a regulation section. The counts associated with each of the High/Medium/Low risk values for each section since sections have different numbers of questions. When summarized for a section, this value shows volume of identified compliance gaps.
    - More than 50% non-compliant responses = High
    - 33%- 50% non-compliant responses = Medium
    - Less that 33% non-complaint responses = Low

Other Considerations

Input into the Risk Assessment:

- Purpose of process/system/ department
- Number of users
- Types of users, internal, external, on-site, remote, contract
- Type of access, level and scope of access
- Frequency of use
- Knowledge level of users

Other Considerations

Input into the Risk Assessment:

- Number of locations/sites
- Physical environment
- Types of security controls
- Interdependencies and interfaces
- Type of information and risks for confidentiality, integrity and availability
- Type of threats (intentional or unintentional)

Example:

Section: Administrative Safeguards

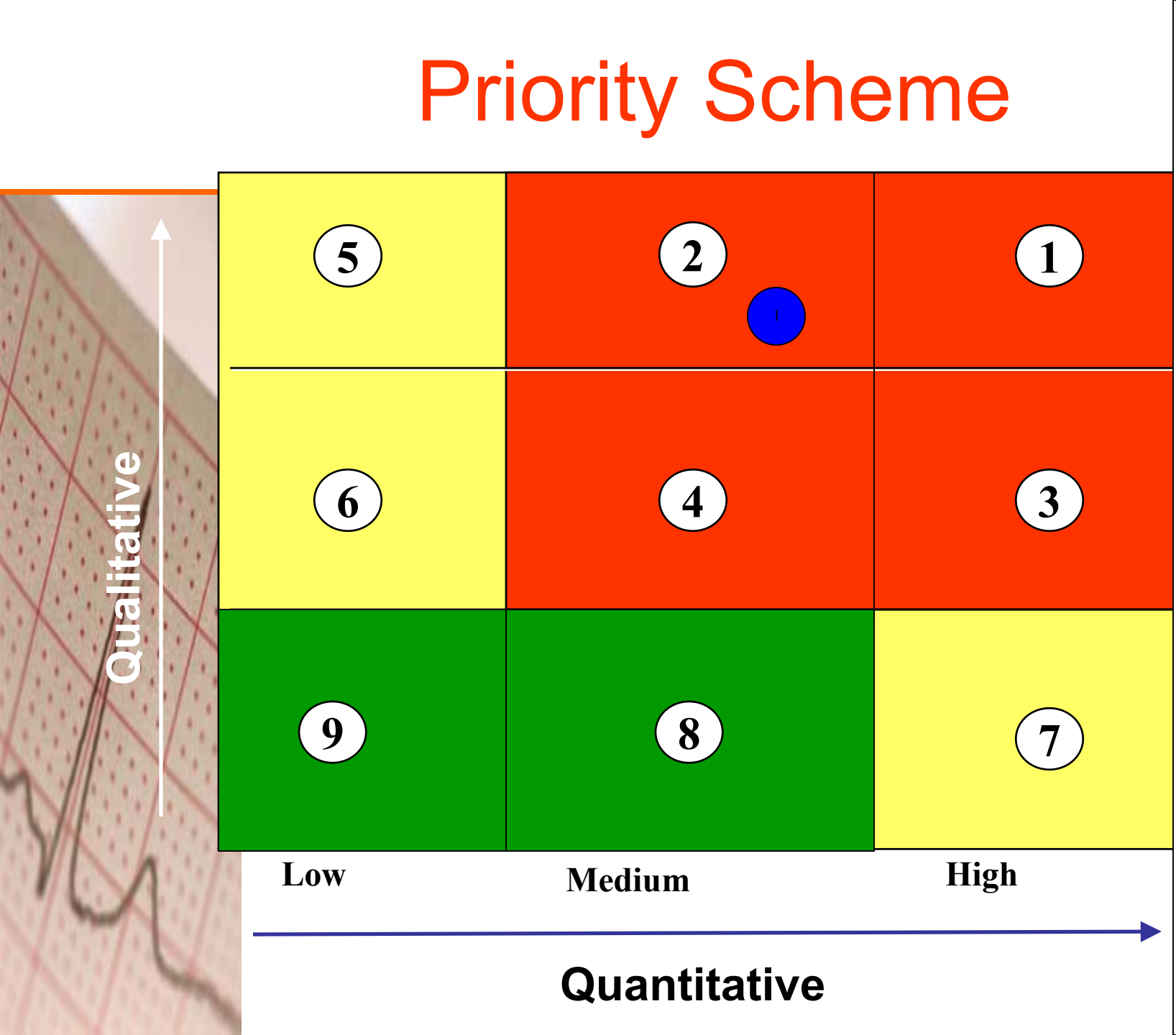
Standard: (1) Information Access Management

Implementation: Access Establishment and Modification (Addressable)

Department; Common Department Findings

Findings	Recommendations	Risk
The departments indicated that it did not know whether health care access requirements are reviewed as a result of internal policy changes. The departments indicated that it did not know whether health care access requirements are reviewed as a result of organizational restructuring or change. The qualitative risk is High. The quantitative risk is Medium since 2 of 6 responses were negative.	Recommended solutions are: Policies and procedures must be developed and implemented to require review of health care access requirements as a result of internal policy changes and organizational restructuring or change. All staff must be trained on the policies and procedures	Qualitative = Quantitative =

Priority Scheme



Lessons Learned

- Create a well-defined approach
- Obtain executive commitment
- Assign one responsible individual
- Provide awareness and education
- The assessment does not execute itself
  - It must be administered and controlled
- Upfront planning pays many dividends
  - More timely and accurate response

Thank You !

Rosemary B. Abell

Director, National Healthcare Vertical

Keane, Inc

Rosemary_B_Abell@Keane.com

(919) 767-2235