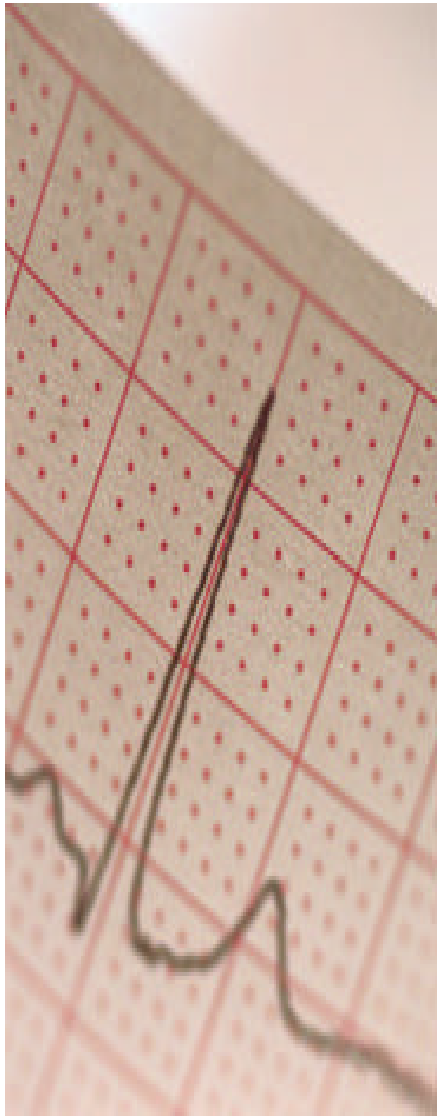
HIPAA EarlyView™

target your weaknesses with this powerful self-evaluation tool



Performing A Security Assessment

Third National HIPAA Summit October 24-26, 2001

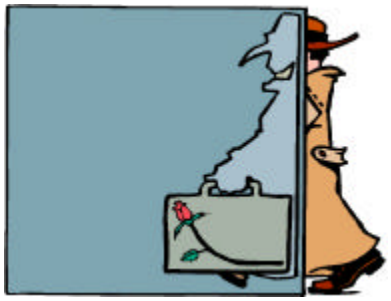
Rosemary B. Abell

Regional HIPAA Practice Director

Keane, Inc.

NCHICA

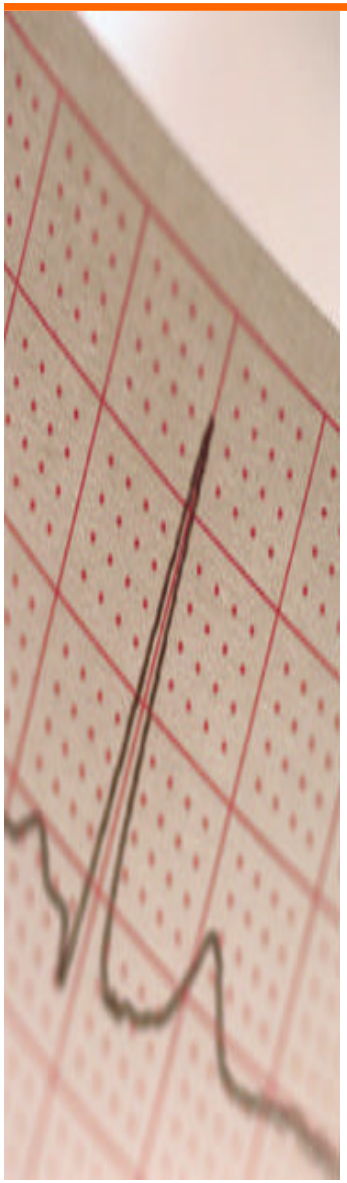
North Carolina Healthcare Information and Communications Alliance, Inc.



KEANE

we get IT done.

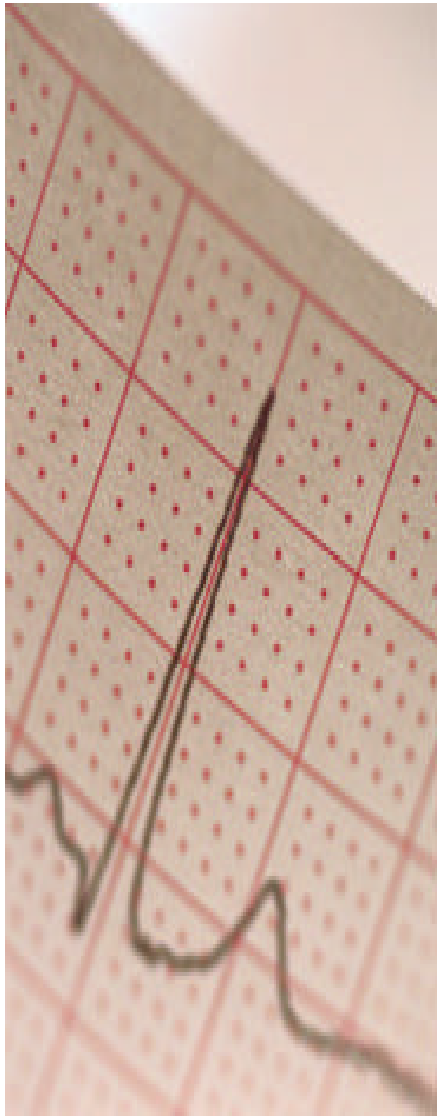
Overview



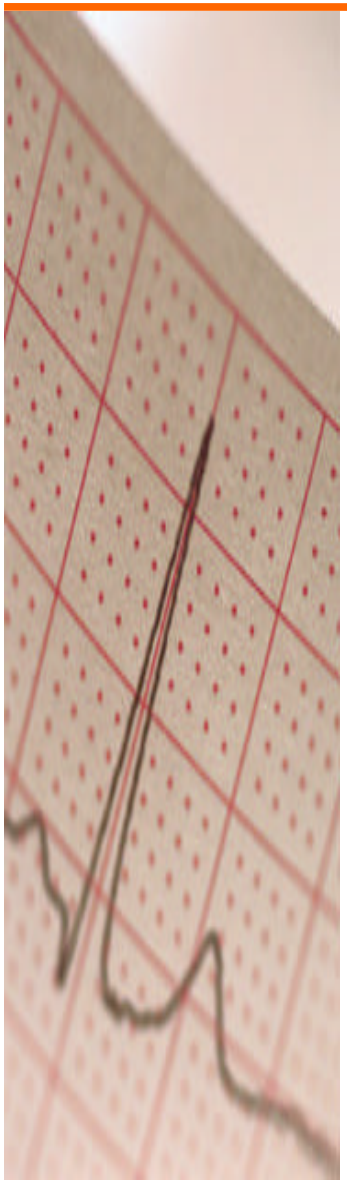
- The Data Security issue – what do we need to do?
- How are we going to do It?
- Case Study

HIPAA Security Assessment

What To Do?

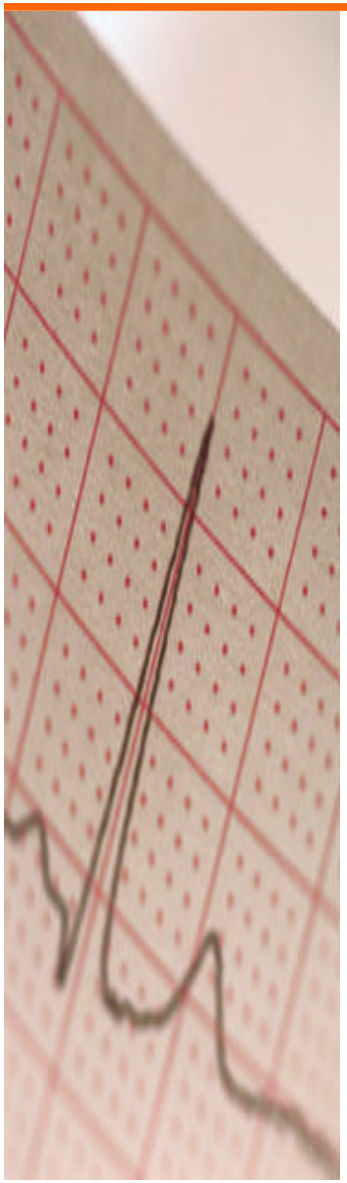


Why conduct a Security Assessment?



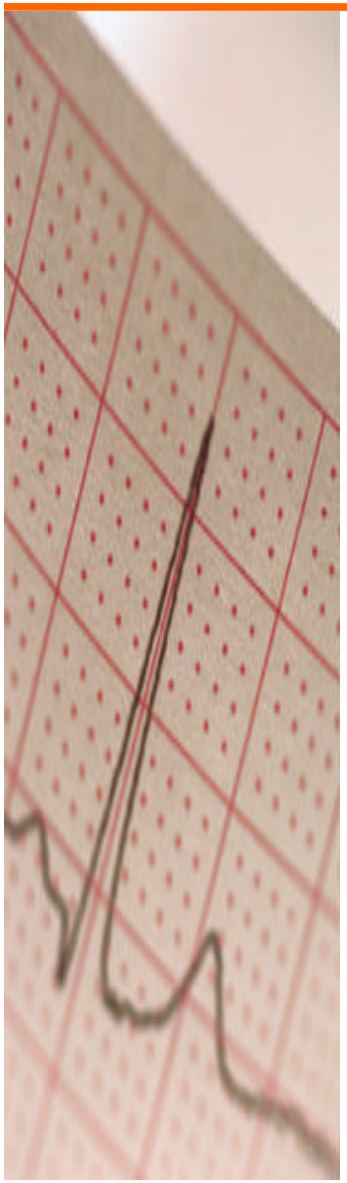
- Provide an understanding of the impact of HIPAA legislation on business operations and technology infrastructure
  - Identify gaps between current business and technical environments compared to the requirements of HIPAA
  - Evaluate the significance of the vulnerabilities (Risks) in the context of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

Goals of the Risk Assessment



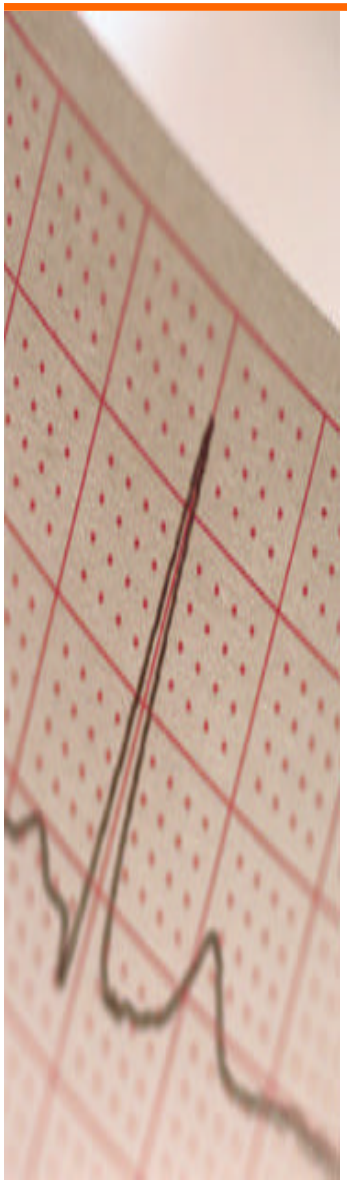
- The questions you are trying to answer in the risk assessment are:
  - What could compromise the confidentiality,integrity and availability of the health information in our possession?
  - If that information is compromised what is the impact to our business or to the individual?
  - What is the probability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

What do we need to do?



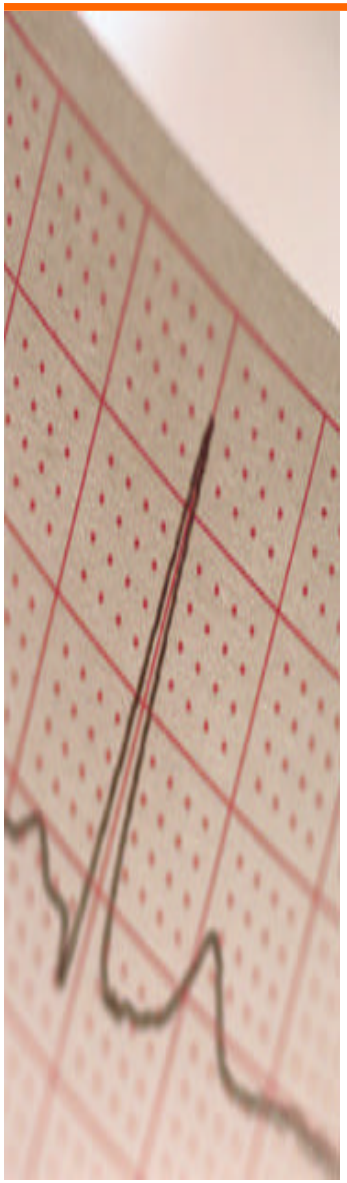
1. Plan
2. Gather Data
3. Analyze Data
4. Assess Risk

Plan



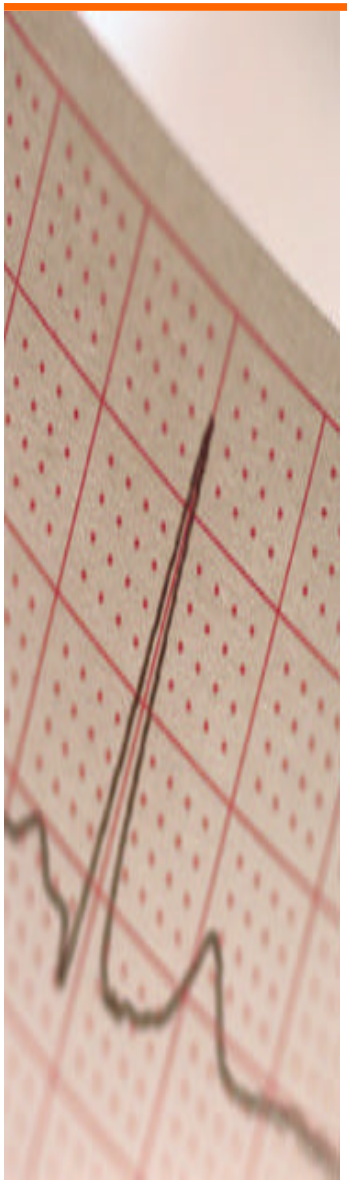
- Kickoff meeting to provide an understanding of the security assessment process
  - Identify the people involved, confirm staff to be interviewed
  - Identify the security assessment approach
  - Identify the steps to be taken
  - Review high level milestones

Gather Security Data



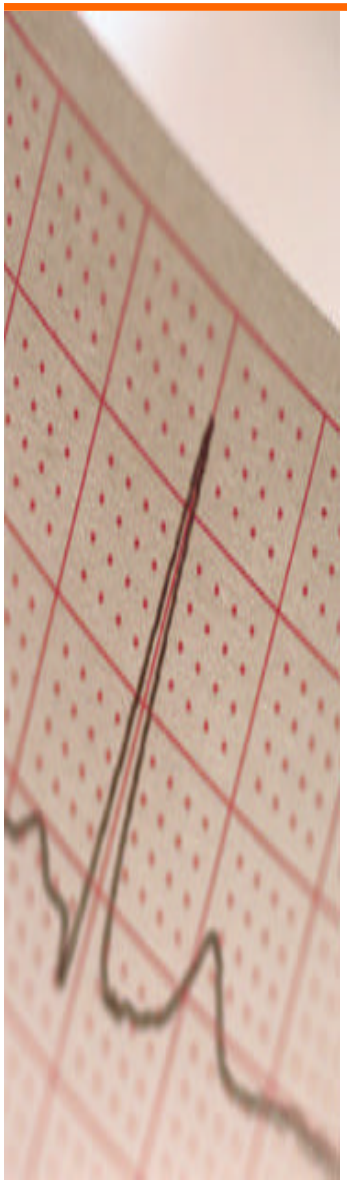
- Customize security assessment questionnaire for HIPAA specifications
- Assign appropriate questions to representatives from functional areas
- Interview representatives from functional areas using the applicable questionnaires
- Record data

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

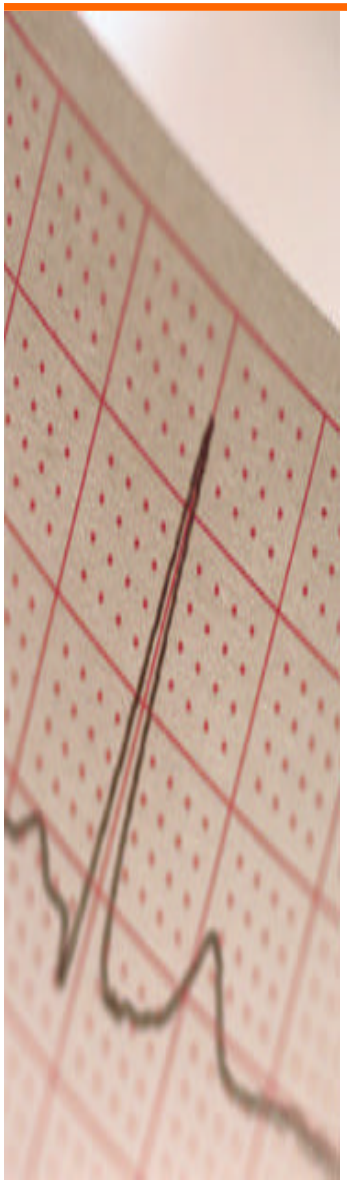
Gap Analysis - Considerations



Results from Gap Analysis should factor:

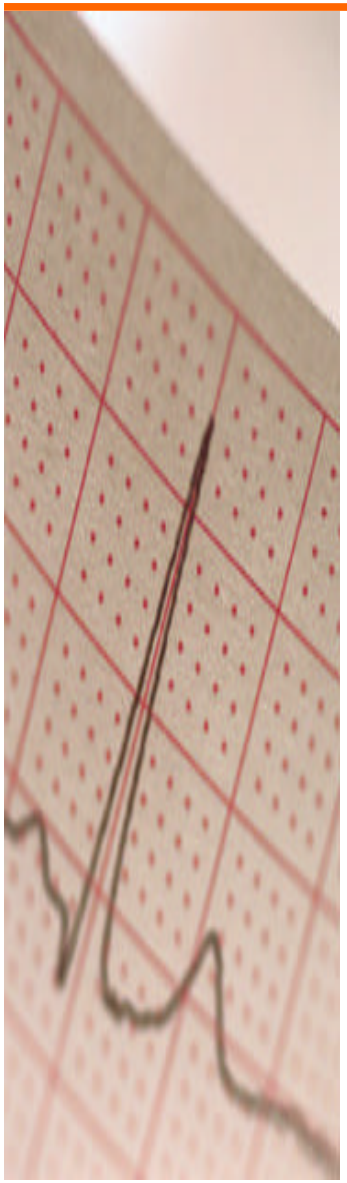
- Purpose of process/system/ department
- Number of users
- Types of users, internal, external, on-site, remote, contract
- Type of access, level and scope of access
- Frequency of use
- Knowledge level of users
- Number of locations/sites
- Physical environment
- Types of security controls
- Interdependencies and interfaces
- Type of information and confidentiality, integrity and availability risks
- Type of threats intentional or unintentional)

Assess Risk



- Each Health Care entity must:
  - Assess potential risks and vulnerabilities to the individual health data in its possession in electronic form
  - Develop, implement and maintain appropriate security measures

Gap Analysis vs. Risk Assessment

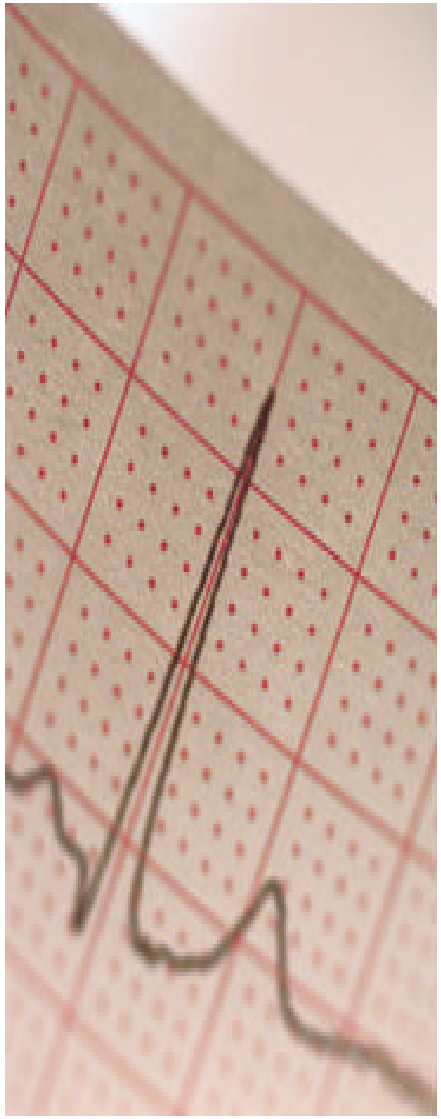


- The gap analysis compares where we are to where we need to be in relation to HIPAA compliance. It helps determine the areas where the organization has vulnerabilities

- The risk assessment will be used to evaluate the significance of the vulnerabilities in context of the organization's operations

HIPAA Security Assessment

How To Do It?

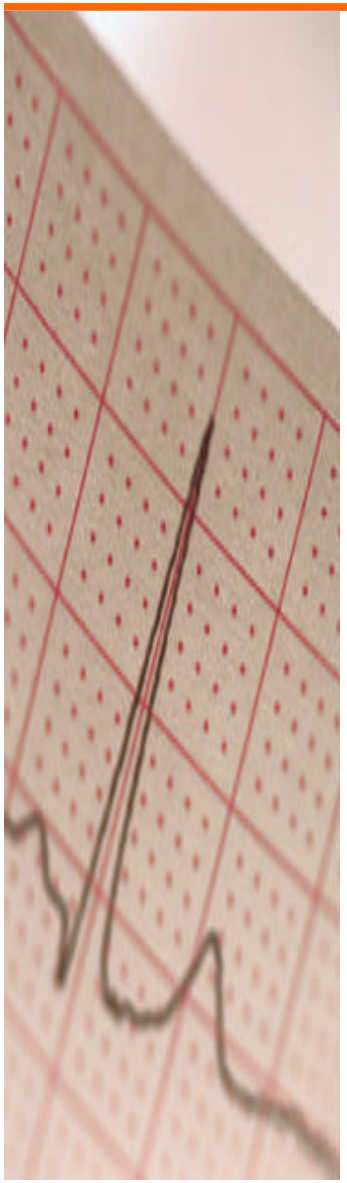


HIPAA EarlyView™

target your weaknesses with this powerful self-evaluation tool

Available as Zipped file download on the NCHICA secure Web site – www.nchica.org

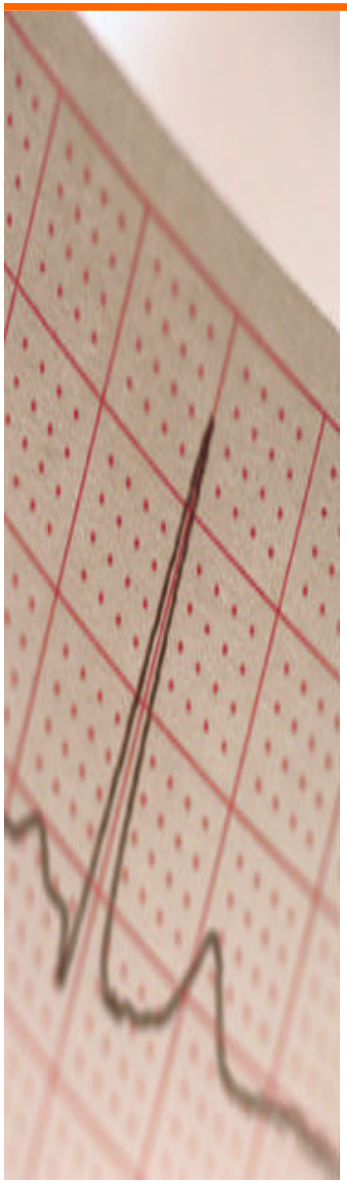
HIPAA EarlyView™ Security



HIPAA EarlyView™ (HEV)

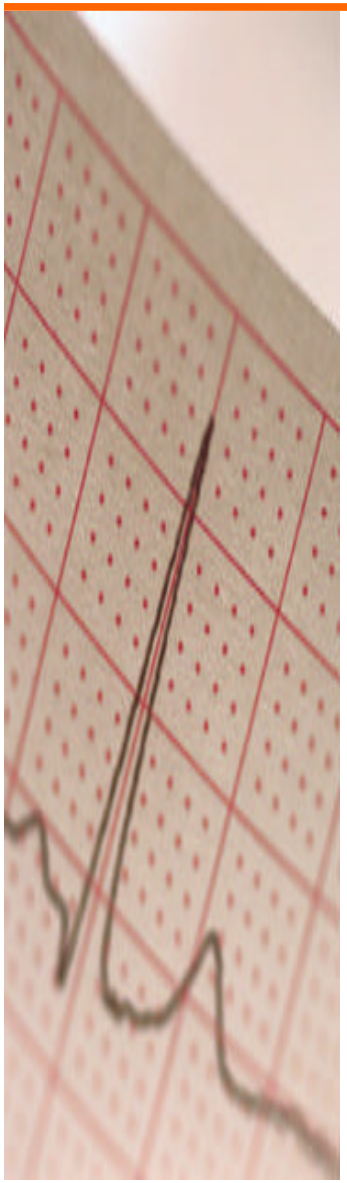
- What it is
- What it isn't
- Deployment in Large Organization
  - Deployment Options
  - Case Study
  - Lessons learned

What it is



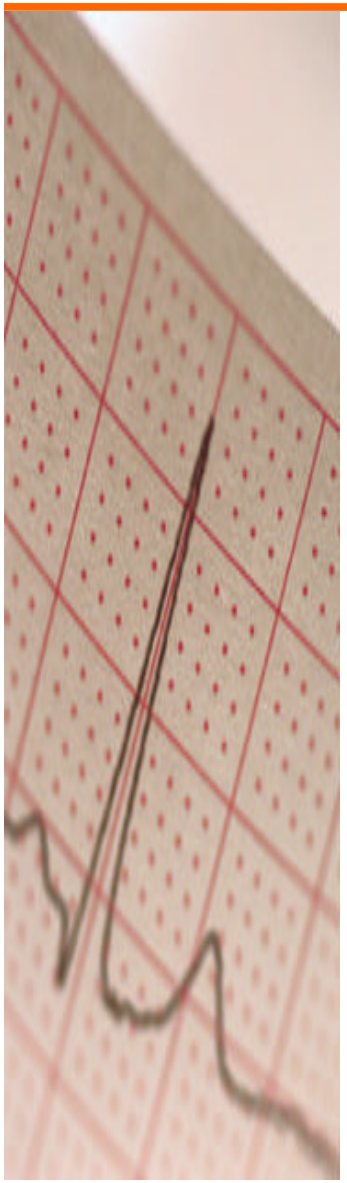
- *A "First Glance"* at an organization's readiness to comply with the proposed HIPAA Security Regulations
- *A self-assessment* that provides assistance to an organization seeking insights into the proposed HIPAA regulation
- *A guideline* in the formulation of a response appropriate to a particular organization's situation

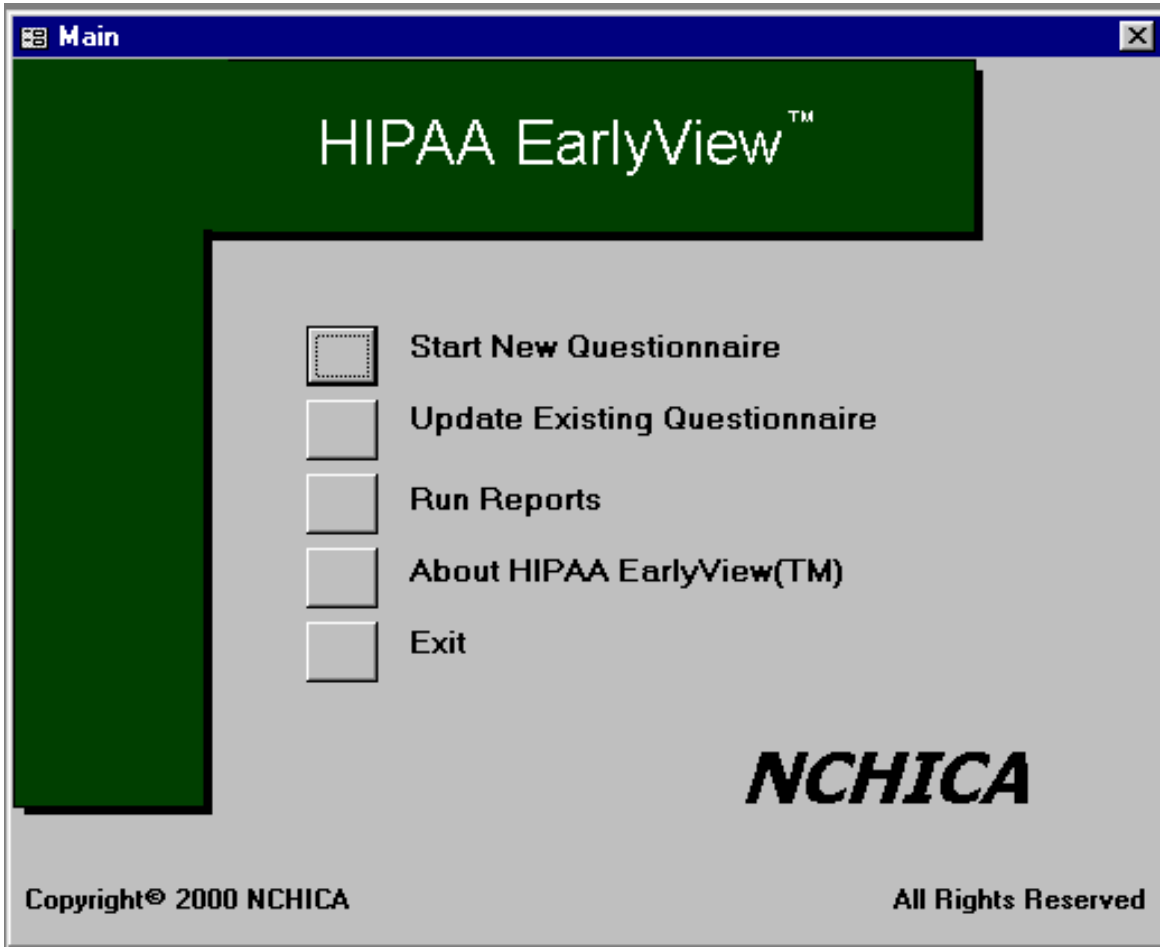
What it isn't



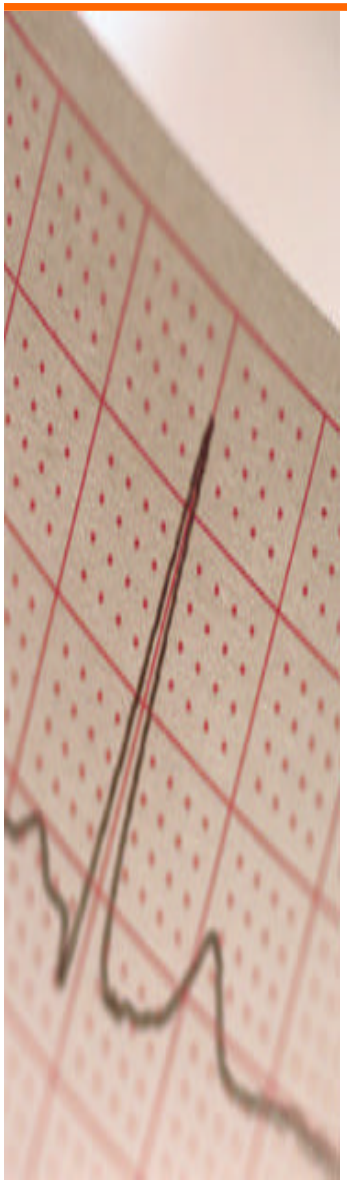
- *A "Silver Bullet"* to eradicate the implications of the HIPAA security regulations
- *A self-conducting tool* that automates all Security Data Assessment requirements
- *A black box* – if you put garbage in, you'll get garbage out

Main Menu




Main
HIPAA EarlyView™
Start New Questionnaire
Update Existing Questionnaire
Run Reports
About HIPAA EarlyView(TM)
Exit
NCHICA
Copyright© 2000 NCHICA
All Rights Reserved

Report Example



Question Listing by HIPAA Requirement and Implementation

HIPAA Table A

HIPAA Requirement Certification

HIPAA Implementation

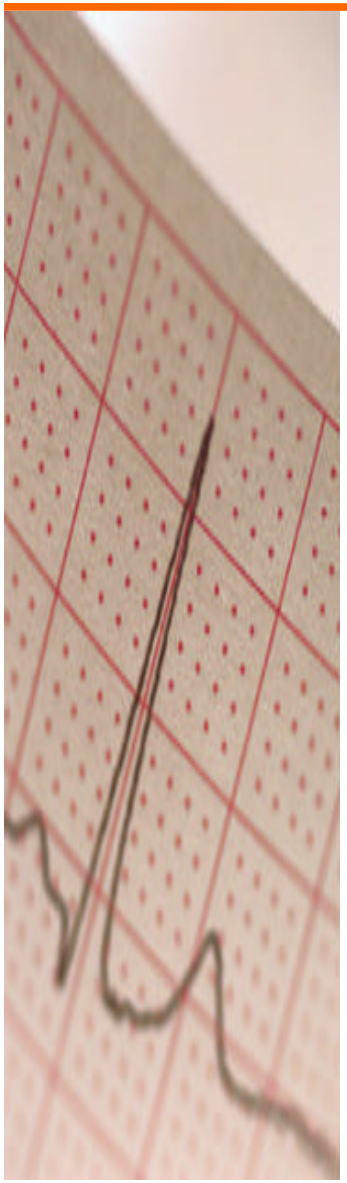
Question Number	Detailed Question
1	Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?
2	Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?
3	Does your organization maintain a technical evaluation history for BOTH information systems AND networks?
4	Does your organization require that BOTH information systems AND networks are reviewed after any additions or significant modifications to design?
5	Does your organization document all steps taken to ensure and maintain security compliance?

HIPAA Requirement Chain of trust

HIPAA Implementation

Question Number	Detailed Question
6	Does your organization require that a chain of trust partner agreement be signed with all third parties that process protected health information?
7	Does your organization explicitly state requirements for ensuring confidentiality and integrity of data in any chain of trust agreements?
8	Does your organization explicitly state requirements for availability of data in all chain of trust agreements?
9	Does your organization maintain the right to audit the security measures of third parties who process protected health information?

Security Questions



This form is used by a facilitator to conduct the HIPAA Security Questionnaire. It is designed to be used to capture all required information. Comments should be forwarded to DataSecurity@NCHICA.ORG. Thanks!

Question 1

Questionnaire Name: sample1

Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?

Answer: (•) Yes ( ) No ( ) N/A ( ) Unanswered

Due Diligence Demonstrated: [ ] Check if YES

Comments: evaluation done by test org - june 1999

Refer To:

Document Name: tech eval

Doc Type: Paper

Document Location:

Periodically Reviewed? No

Next Review Date (MM/DD/YYYY):

Point of Contact: Mr. Contact

Contact Phone: (999) 999-9999 Ext. 1234

Contact Title: boss

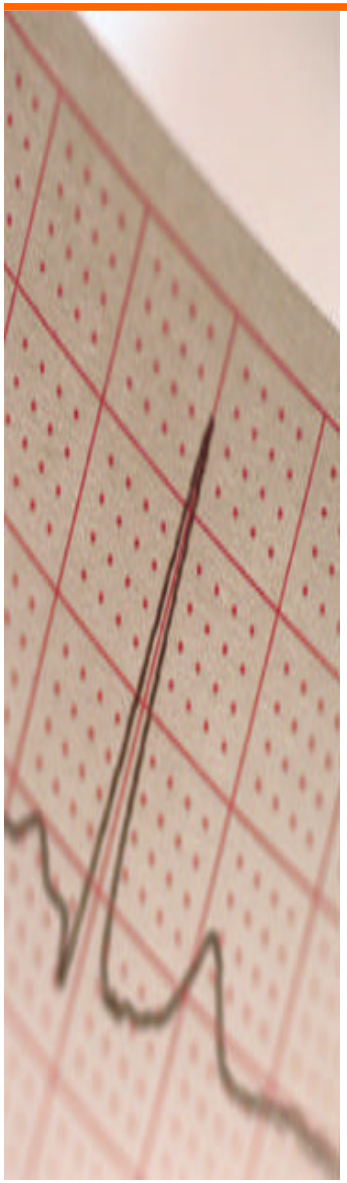
Contact E-Mail: boss@sample.com

Contact FAX: (999) 999-9999

Answer Date (M/D/Y): 6/9/00

Readdress Requirement: [ ]

Report Example



Questions answered with "NO"

sample1

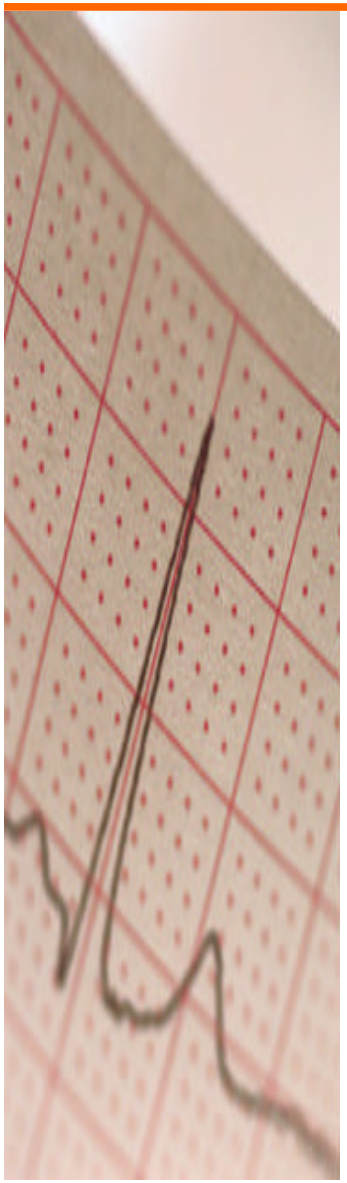
HIPAA Table A

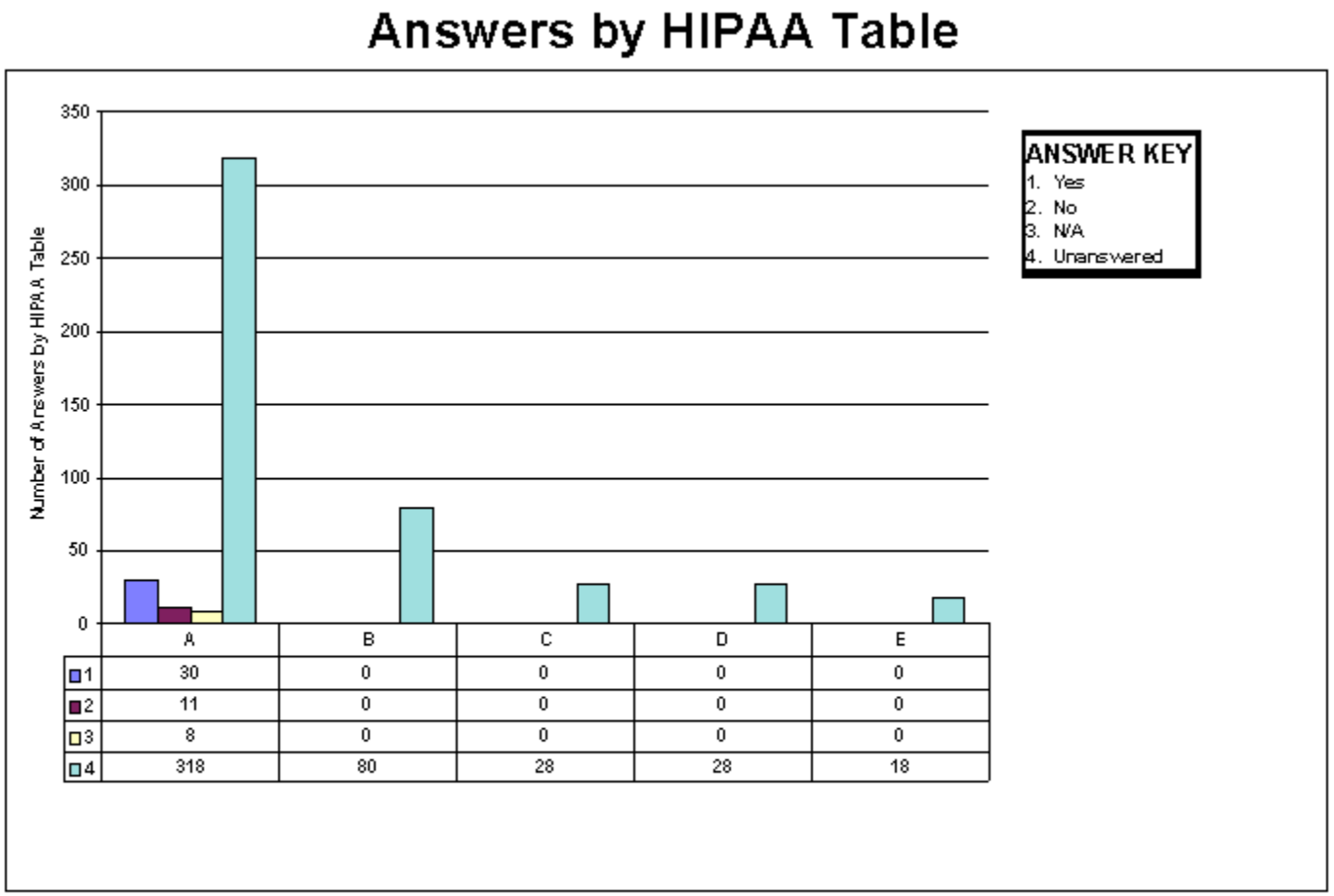
HIPAA Requirement Certification

HIPAA Implementation

Question Number	Detailed Question	Refer To:	Contact	Contact Phone
2	Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?	Susan Reference		

Report Example

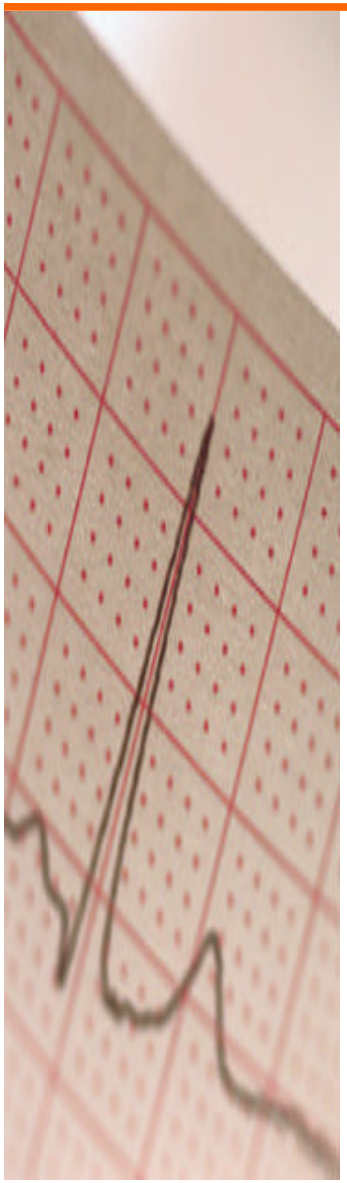




Monday, June 12, 2000

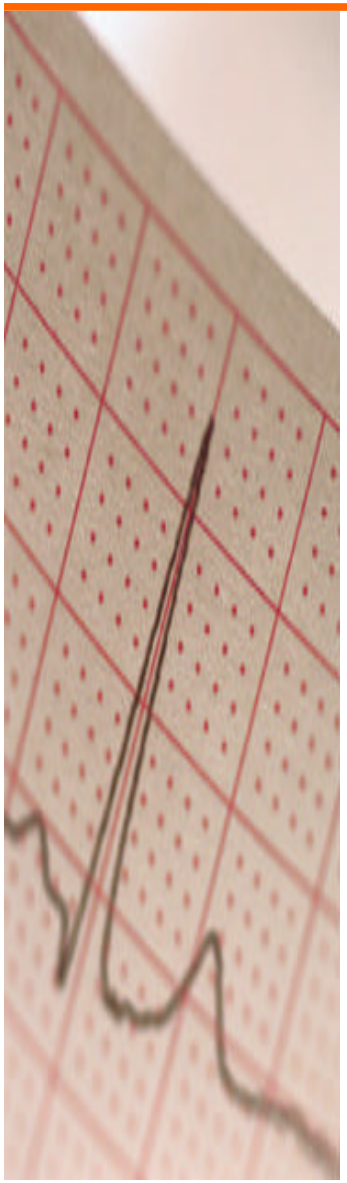
sample1

Deployment Options



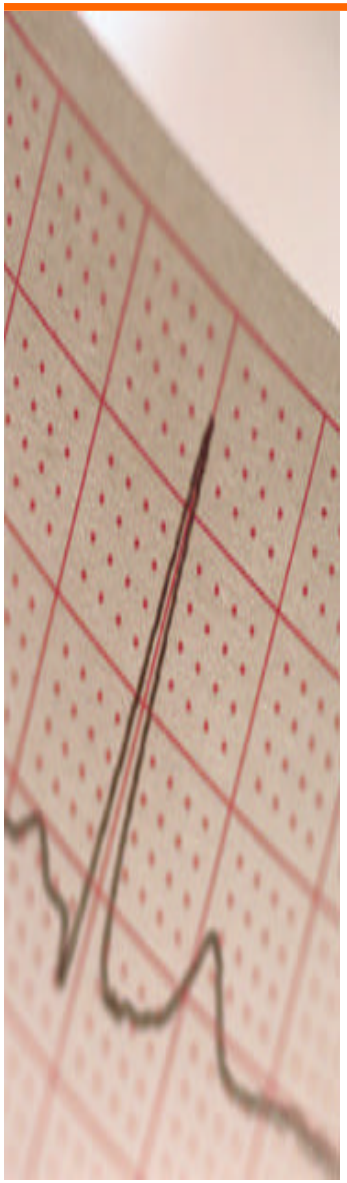
- Minimal Control
  - Subject Matter Experts are assigned questions and enter data directly into the tool
- Minimal Control combined with training and awareness effort
- Fully Managed and Executed Data Security Assessment

Case Study: Conducting the survey utilizing the tool



- Deployment in a large, disperse organization
- The approach requires that an experienced individual conducts direct interviews with Subject Matter Experts (SMEs) and records the answers for each question into the tool

Executing the Data Security Assessment



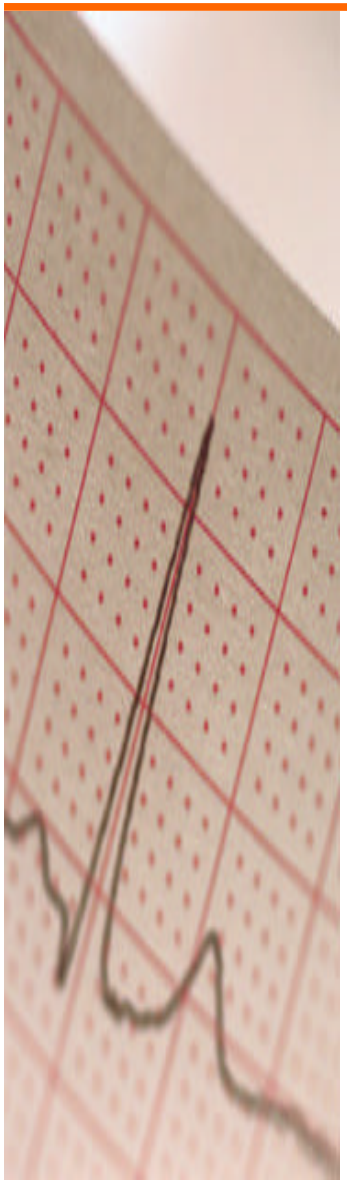
1. ***Plan:*** Determine the lines of business or departments that will participate in the assessment

2. ***Gather Data:*** Conduct the survey utilizing the tool

3. ***Analyze Data:*** Review the results of the survey and perform a gap analysis for each department or line of business that indicates vulnerabilities utilizing the reports provided with the tool or other reports created by your organization

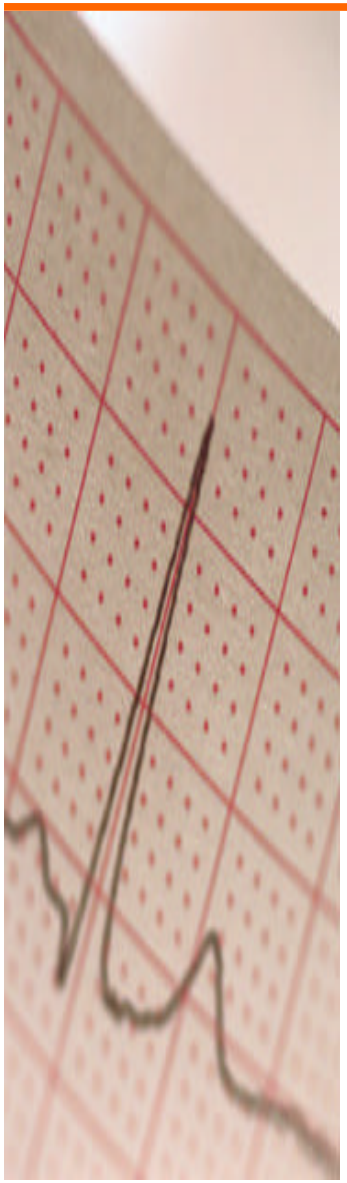
4. ***Assess Risk:*** Perform a risk assessment for each line of business or department to determine the priority and sequence of how these gaps will be addressed for the entire organization

Lessons Learned



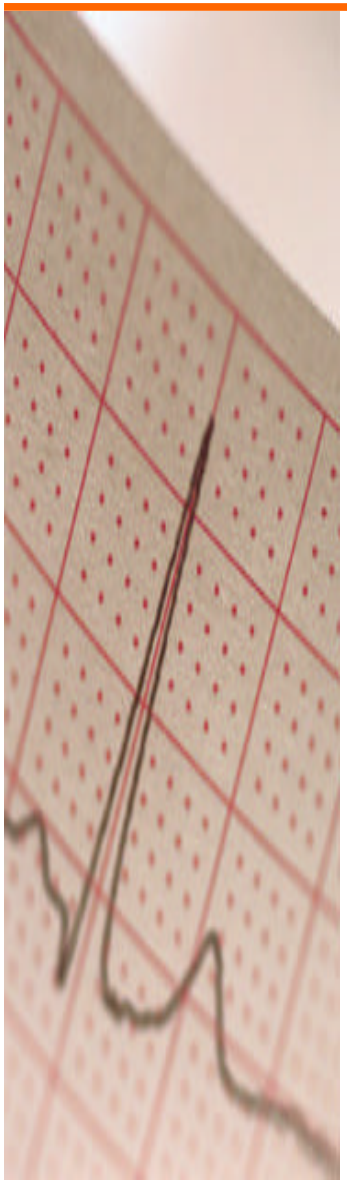
- Create a well-defined approach
- Obtain executive commitment
- Assign one responsible individual
- Provide awareness and education

Lessons Learned



- 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

Regional HIPAA Practice Director

Keane, Inc

Rosemary_B_Abell@Keane.com

(919) 767-2235