HIPAA SUMMIT WEST

San Francisco, California

June 21, 2001

Implementing a HIPAA Compliance Strategy: Balancing Inside Resources with Consulting and Outsourcing Services

Bret S. Bissey
Chief Compliance Officer & Chief Privacy Officer
Deborah Heart and Lung Center

D. Patrick Lewis, Esquire
Founder and Director
Health Security Solutions

STRATEGY

- Definition:

The science and art of using forces to execute approved plans as effectively as possible

In House -- Outsource

- What are we good at?
- What expertise do we have?
- How much time do we have to dedicate to this?
- How much $$ do we have to spend on this?
- If we do outsource, it should be a specialist
- What is the cost of “thinking” that we know what we are doing?
- Do you hire a Carpenter to do Cardiac Surgery?

What are we good at?

- If you do not have the expertise in-house to accomplish a required function - admit it now.
- An active debate must begin and constantly be updated regarding what your skill sets are regarding Privacy and Security

Model Guidance

- We are anticipating to receive “guidance” regarding how to plan/manage/implement/measure HIPAA.
- An ideal place to look at your organization’s skill sets (follow the OIG’s Model Compliance Plan Structure)

OIG MODEL COMPLIANCE PROGRAM

- Provides Guidance
- Suggests at least 7 “elements”
- However, no two programs should ever be identical - “one size should not fit all providers” - WHY???
- How HIPAA fits into an existing Compliance Plan will vary by Provider

BASIC COMPLIANCE PLAN ELEMENTS

- Policies and Procedures
- Management of Program
- Education and Training
- Staff Communication Channels
- Monitoring and Auditing
- Discipline
- Corrective Actions

Policies and Procedures

- **Security Requirement -** Administrative Procedures
- **Privacy Requirement -** Policies and Procedures
- Is this something we can handle internally?
- What will/could we miss by doing it internally?

MANAGEMENT OF PROGRAM

- **Security Requirement -** assigned responsibility
- **Privacy Requirement -** must designate a Privacy Official

Issue: Does it make good business sense to have Compliance Officer also be the Privacy Officer???

Education and Training

- Security Requirement - must educate and train
- Privacy Requirement - must educate and train

What are skills of employees - do you have someone that can do this effectively?

Does it make sense to have an expert give the news?

Education

- You need a good speaker who understands the issues and can communicate to all of the employees (use case studys that everyone can relate to)
- If you don’t have this resource inside hire someone to give the education
- You want an educated staff
- Develop an education schedule

Education of Potential Fines/Risks

- Senior Management and the Board need to be made aware of the magnitude of potential liability in regards to Non Compliance with the regulations
- The message should be very stern to the leadership - **FEAR**

Staff Communication Channels

- Security Requirements - Reporting Procedures, Event Reporting
- Privacy Requirements - Compliant Processing

Issue: How sophisticated is the existing structure? Affirmative Duty to Report Statement, Non-retaliation Policy, Hotline, Employee Acknowledgments, etc..

Monitoring and Auditing

- Security Requirements - Internal Audit
- Privacy Requirement - Assure appropriate accounting for any and all disclosures

Issue: Does current structure (Internal Audit) have the ability (knowledge and resources) to appropriately provide this function? Much different than traditional compliance (documentation) auditing.

MONITORING

How are the HIPAA Initiatives going to be managed in your organization on a daily basis??

Staff education must be effective to assure everyone understands this is a change in culture within your organization

MONITORING

- How do I validate that my efforts are enough?
- How do I know that we are “compliant”
- External Assessment?
- Gap Analysis?
- When do you have the Gap Analysis done?

Discipline

- Security Requirements - Sanctions must be evident
- Privacy Requirements - Sanctions must be evident

Historically from the OIG's perspective they want to make sure that compliance plans "have teeth in them."

(make sure policies address your procedures)

Disciplinary Actions

- The employees need to know that your organization is serious about this initiative.
- Employees should know that this is an expected requirement of their position.
- Non Compliant behavior should be handled seriously and reflected in your policies and procedures.

Corrective Actions

- Security Requirement - response procedures, testing and revisions
- Privacy Requirement - duty to mitigate

Issue: How well an organization's culture accepts and incorporates these mandates will determine how they manage issues.

This process may differ from the traditional compliance program in terms of time to react.

Responsible Individuals

HIPAA mandates the appointment of a Privacy Officer.

Does this imply that a Privacy Officer can do it all? What are the other non-HIPAA responsibilites of the PO?

Who else in the organization should be involved?

Who can foster an **environment of change**? Look for the best person not a title!!!

RESOURCES

- People
- Technology
- $$$$$$

Must be committed by the Board, Senior Management to an acceptable level or you will struggle

Develop and sell your plan including budget to the decision makers!!!

Outcomes/Goals

What does your organization want to achieve???

- (1) Meet these ***** HIPAA requirements

or

- (2) Improve operations, enhance efficiencies and improve patient relations

Are you doing this for the right or the wrong reason???

MEASUREMENT

- You need to establish threshold(s) or goals which need to be meet and frequently analyze them.
- Measures should be unique to your organization.
- Compliance is many times difficult to measure.

Vision

- All employees need to know that secure and confidential patient information is really important to your organization.
- You need to “sell” this vision.

Closing Thoughts

- Don’t be afraid to be innovative
- Don’t overestimate your knowledge on this topic
- Don’t be afraid of making mistakes, as long as you learn from them
- Try to take a Positive approach to these requirements.