The Fifteenth National HIPAA Summit: Special Edition

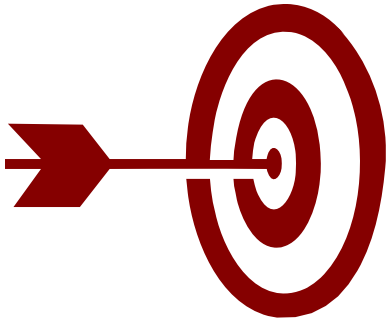
Healthcare Privacy and Security Training and Professional Certification

Managing your Institution-Specific HIPAA Compliance Policies and Procedures Cutting Edge Issues

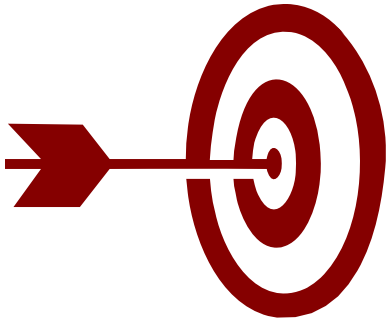
Thursday, December 13, 2007

Compliance and Policies

- Facts:
  - Compliance is a continuous process
  - Businesses change
  - Processes continue to evolve
  - New technologies are implemented
  - Policies, if followed and implemented can protect the institution.
  - Compliance today does not mean compliance tomorrow.

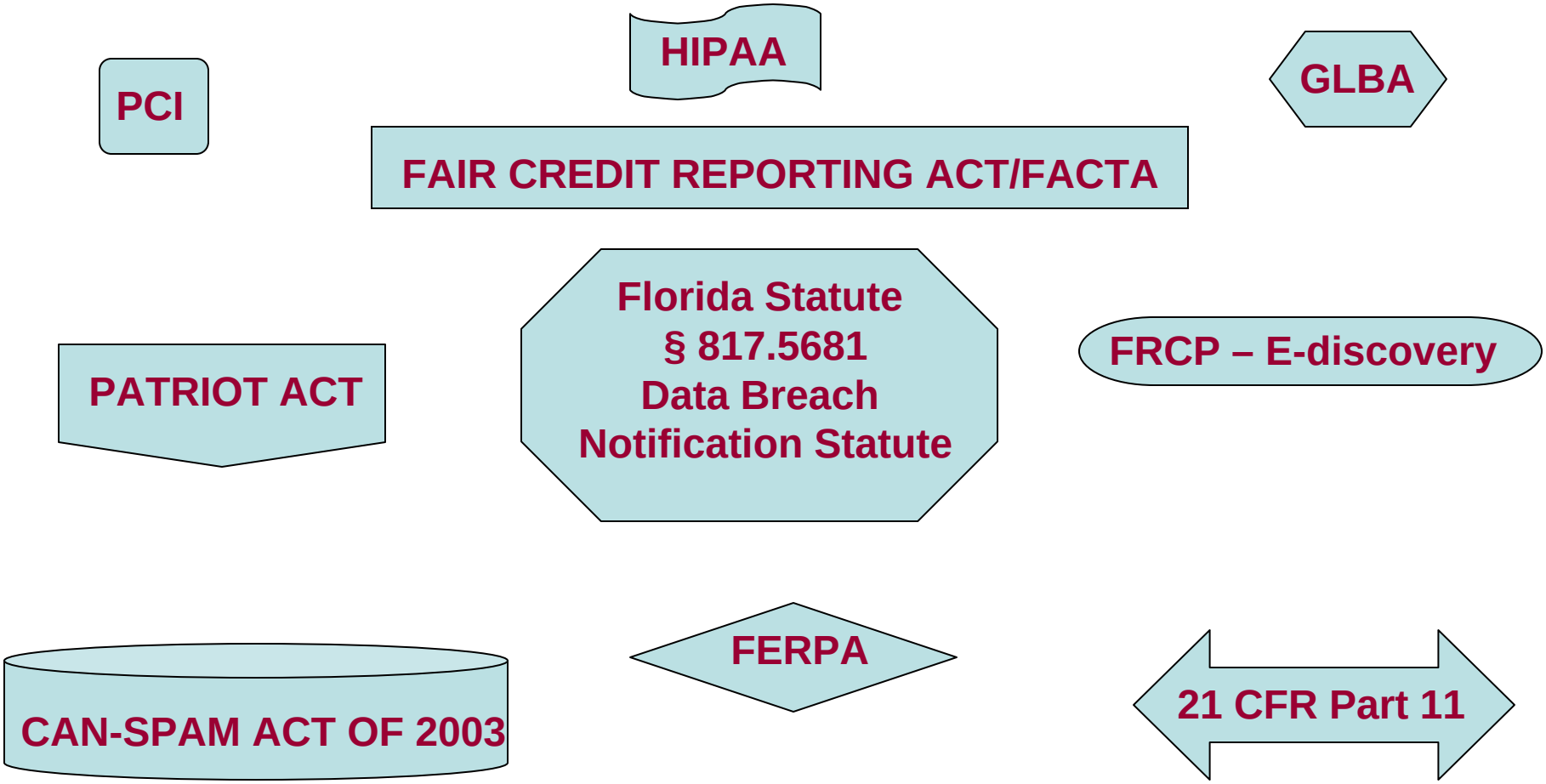


Policies are moving Targets and must be revised to meet the challenges of the changing business and regulatory environments.



Cutting Edge Policies State/Federal

The ever-changing regulatory environment….



Regulatory Issues
Sensitive Information

- Identity Theft/ Medical Identity Theft
  - Increasing problem at Healthcare providers
  - Fraud
- Financial (Organizational) Data - (Confidential)
- Research data
- Intellectual Property (Research papers/innovations)
- Email
  - Student, Faculty and Staff (sent and received)
- JCAHO
- FDA
- Billing Compliance

Data Breach Notification Laws

- As of January 2007 – 35 states have enacted such laws to disclose security breaches involving personal information.

- Such laws are intended to protect consumers and hold organizations liable for the protection of personal information.

Institutional Response

- Ideally you need institutional privacy and information security practices
- Move away from the “siloed”, purely compliance approach
- It’s all about facilitating effective business processes and reducing risk
- Considerable opposition from “entrenched” areas
- This approach can only succeed with “**hands on**” C-level leadership
  - *and evolution into an appropriate governance structure*

Institutional Response

- Develop and implement an Enterprise Incident Response Plan
- Test the Enterprise Incident Response Plan to make sure it works
- **Create procedures that allow the organization to respond in a timely, thoughtful and savvy manner that minimizes damage to the reputation and image of the institution.**

WORD TO THE WISE

It is far less costly to prevent a data breach than it is to respond to one!

According to SC Magazine and the Ponemon Institute, the estimated cost of a data breach is $182 per compromised record in addition to the indirect costs for lost employee productivity and opportunity costs related to customer loss which may add up to over $10 million dollars.

2008 CPT Changes
How will it affect your Policies?

- Did you know that third party payors will pay for E-visits beginning in 2008?
  - An e-visit is an electronic alternative to a traditional office visit.

- Does your organization have policies that govern e-mail communications between physicians and their patients?
- Do you have a secure mail system or portal that allows for the exchange of encrypted E-PHI?
- Do you have policies to address what types of documentation are required to bill for an e-visit and what documentation must be maintained and for how long?

•*NOTE: Unencrypted email should not include PHI or other sensitive information such as HIV, STDs, Substance Abuse, Domestic Violence or Psychotherapy Notes.*

Policies & Compliance

- Keep it current
- Only implement policies with which your organization can comply
- Stay abreast of all current state and federal legislation that will affect your business
- Continually monitor your institution for new sites of service, changes in organizational structure, and new business units and practices
- Monitor your policies for compliance and adjust as needed.
- Disseminate changes and train the masses.
- Training and education are key to successful compliance programs.

Questions……..

Contact Information:

Sharon A. Budman, MS Ed, CIPP
Ishwar Ramsingh, MBA, CISSP, CISA, CISM

Phone: 305-243-5000