April 14, 2003- A Watershed Date in HIPAA Privacy Compliance:

Where Should You Be in HIPAA Security Compliance and How to Get There…

John Parmigiani
National Practice Director
HIPAA Compliance Services
CTG HealthCare Solutions, Inc.

HIPAA Security Standards

- Are based upon good business practices
  and
- Have these basic characteristics:
  - *Comprehensive*
  - *Flexible*
  - *Scalable*
  - *Technology Neutral*

Good Security Practices

- **Access Controls- restrict user access to PHI based on need-to-know**
- **Authentication- verify identity and allow access to PHI by only authorized users**
- **Audit Controls- identify who did what and when relative to PHI**

So…Security is Good Business

ctg HealthCare Solutions

- "Reasonable measures" need to be taken to protect confidential information (due diligence)
- A balanced security approach provides due diligence without impeding health care
- Good security can reduce liabilities- patient safety, fines, lawsuits, bad public relations
- Can have security by itself, but *Cannot have Privacy without Security!*

Steps Toward Compliance

Serendipity Effect of Privacy Compliance

- Complying with the Security Rule should be fairly easy if you have done the preliminary work for Privacy- PHI flow, risk assessments
- Implementation of "safeguards" to protect the privacy of PHI
- Balance through synchronization and symmetry

Immediate Steps

ctg HealthCare Solutions

- Assign responsibility to **one** person-CSO and establish a compliance program
- Conduct a risk analysis
- Deliver security training, education, and awareness in conjunction with privacy
- Develop/update policies, procedures, and documentation as needed
- Review and modify access and audit controls
- Establish security incident reporting and response procedures
- Make sure your business associates and vendors help enable your compliance efforts

Security Compliance Program Steps

ctg HealthCare Solutions

1. Appoint an official to oversee the program
2. Set standards of expected conduct
3. Establish training, education, and awareness program
4. Create a process for receiving and responding to reports of violation
5. Audit and monitor for compliance on an on-going basis
6. Take appropriate corrective actions

Risk Analysis

- What needs to be protected?
  (Assets – Hardware, software, data, information, knowledge workers/people)
- What are the possible threats?
  (Acts of nature, Acts of man)
- What are the vulnerabilities that can be exploited by the threats?
- What is the probability or likelihood of a threat exploiting a vulnerability?
- What is the impact to the organization?
- What controls are needed to mitigate impacts/ protect against threats

Information Security Policy

- The foundation for an Information Security Program
- Defines the expected state of security for the organization
- Defines the technical security controls for implementation
- Without policies, there is no plan for an organization to design and implement an effective security program
- Provides a basis for training

Audits

- Data Owners periodically receive an access control list of who has access to their systems and what privileges they have
- Users are randomly selected for audit
- Audit data is provided to their managers
- Warning banners are displayed at logon to any system or network ("No expectation of privacy")
- Audit logs are stored on a separate system and only the Information Security Officer has access to the logs
- Audit trails generated and evaluated

Incident Reporting and Response

- Can staff identify an unauthorized use of patient information?
- Do staff know how to report security incidents?
- Will staff report an incident?
- Is there one telephone number that staff can call to report any type of incident?
- Are there trained and experienced employees responsible for collecting and preserving evidence?
- Is the procedure enforced?

ctg HealthCare Solutions

Security Compliance Questions???

Security Compliance Questions

ctg HealthCare Solutions

- Have you designated a single individual as the Information Security Official?
- Have you developed an Information Security Policy?
- Have you conducted a Risk Analysis and have the documentation to prove it?
- Have you conducted a detailed technical analysis of network controls?
- Have you established meaningful Audit Controls?
- Have you updated Contingency Plans?

Security Compliance Questions…

- Have you developed Security Incident Reporting and Response Procedures?
- Have you reviewed Human Resources Policies relating to Workforce Security?
- Have you reviewed Information Access Management Policies?
- Have you established Device and Media Controls?
- Have you developed a Facility Security Plan that ensures physical safeguards for PHI?

Security Compliance Questions…

ctg HealthCare Solutions

- Have you developed a Policy on Workstation Use and Security?
- Have you developed an Information Security Training, Education, and Awareness Program?
- Have you instituted Authentication for all members of the Workforce?
- Have you developed Business Associate Contracts?

Thank You

Questions?

john.parmigiani@ctghs.com / 410-750-2497