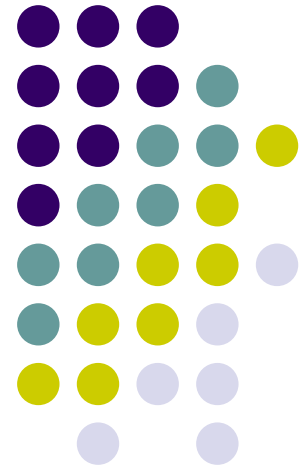


Effective Integration of HIPAA Information Security with Privacy Compliance

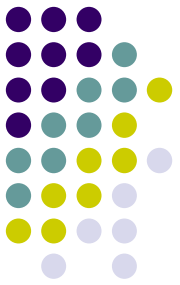
Richard B. Boyer, Privacy Officer

Jody S. Hawkins, Information Security Officer

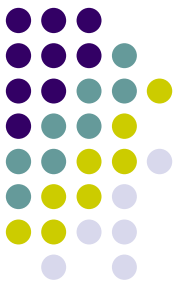
Children's Medical Center Dallas



Agenda



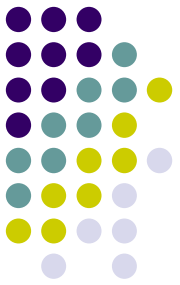
- Introduction and Objectives
- Children's background information
- Important considerations for effective integration of security with existing privacy initiatives
- Using lessons learned from Privacy to successfully implement HIPAA Security Compliance
 - Policy and Procedural changes
 - Effective Communications Plan
 - Training Plan
- Questions and Answers



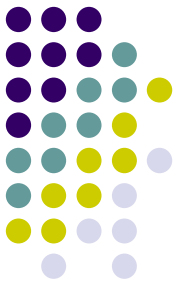
Objectives

- Explain areas where the necessary changes needed for Security compliance may be implemented in a more efficient way than with HIPAA Privacy
- Demonstrate the benefits of systematic cooperation between Privacy Officer, Information Security Officer and other departments responsible for compliance activities
- Show important areas where we can effectively integrate Privacy and Security efforts

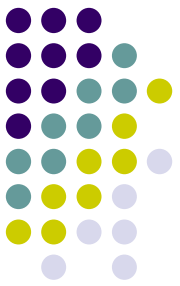
Background on Children's Medical Center Dallas



- **Private – Not for profit, located in Dallas, TX**
- **325 operating patient-beds with 61 critical care and 264 medical/surgical beds**
- **Fourth largest pediatric hospital in the United States.**
- **A system of nearly 50 outpatient specialty clinics providing a comprehensive range of care to children with specialized medical needs**
- **Children's Dallas cares for more than 325,000 children each year. One out of every seven children in North Texas is treated at the hospital. (17,229 inpatient admissions in 2003)**
- **The nation's busiest pediatric emergency room. In 2003 there were more than 98,000 emergency visits.**
- **The nation's first pediatric day-surgery program with two dedicated surgery facilities for inpatient and outpatient surgeries with more than 10,000 day-surgeries performed in 2003.**
- **A major pediatric kidney, liver and heart transplant center with more than 36 transplants in 2003.**
- **Access to the most advanced medical research and treatments available through its affiliation as the primary pediatric teaching facility for UT Southwestern Medical Center at Dallas.**



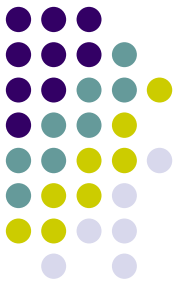
Important Consideration Factors for Integrating Security and Privacy



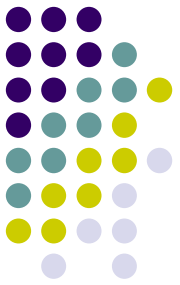
Important Consideration Factors

- Several Privacy concerns may have been handled with Information Security implementations in 2003
 - System/Application Access Limitations
 - Physical Safeguards
 - Audit Functions (technical)
- HIPAA as a whole should appear seamless to the end users
 - Single HIPAA “hotline” for questions and reporting incidents for Privacy and Security
 - Constant communications between Privacy Officer, ISO and CCO

Important Consideration Factors

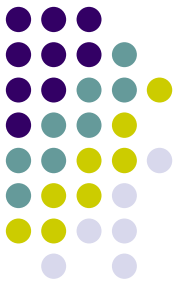


- Workforce should not have to repeat processes for Security that have already been accomplished for Privacy if those processes can be combined
 - Learning Management Systems
 - Location of posted policies “HIPAA at Childrens”
 - HIPAA awareness activities
 - Audits, Reports, and Investigations for Privacy and Security can be handled together for a clearer picture of compliance

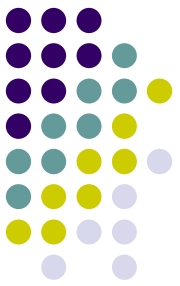


Using lessons learned from Privacy to successfully implement HIPAA Security Compliance

Areas of Opportunity for Utilizing Lessons Learned



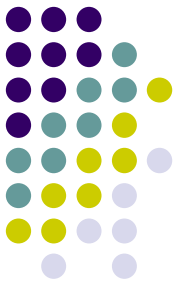
- **Policy and Procedure Development**



Policy and Procedures

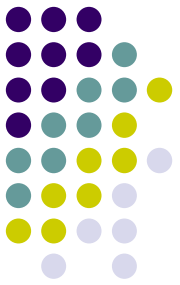
- ISO and Privacy Officer Review Privacy P&P rollout strategy and results to evaluate strengths and areas for improvement
- Ensure that everyone is clear on the review and approval process for P&P
- Eliminate overlap by clearly defining P&P ownership by category (Privacy or Security)
 - Cross reference between Privacy and Security Policies where applicable
 - Update Privacy Policies as Security Policies are implemented
- Watch out for redundant redundancy
- It is better to have a weaker policy that you can follow than to write a strict policy you know will be consistently violated

Areas of Opportunity for Utilizing Lessons Learned



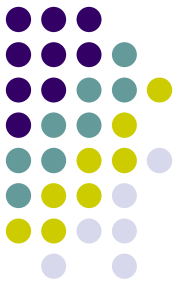
- Policy and Procedure Development
- **Effective Communications Plan**

Effective Communications Plan

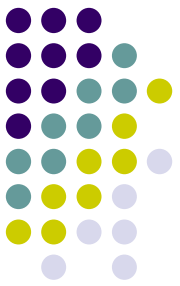


- Remember that to staff... HIPAA is HIPAA is HIPPA – meaning the majority of them do not understand the difference between Privacy, Transactions/Code Sets and Security
- 4 C's of employee communications
 - Clear
 - Concise
 - Consistent
 - Correct
- Utilize Multiple Media resources to deliver the message
- Stress importance of compliance as an overall organization goal rather than a departmental mandate

Areas of Opportunity for Utilizing Lessons Learned

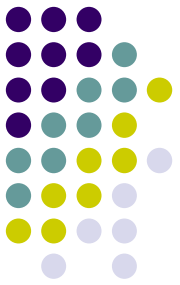


- Policy and Procedure Development
- Effective Communications Plan
- **Training Plan**



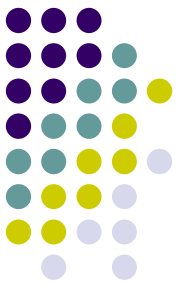
Training Plan

- “piggy back” where possible
 - Capitalize on successful methods when rolling out Security training
- Success of Training effort is quality indicator for your Communications Plan
- Consider implementing a Privacy Refresher with Information Security HIPAA training

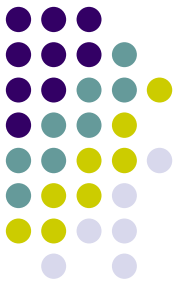


Summary and Questions

Summary



- There is no “silver bullet” to guarantee success for Security implementation, but building on the experiences of preparing for the April 2003 Privacy compliance date can provide a good road map
- Security compliance should complement the overall HIPAA compliance effort and not live in a vacuum
- There are opportunities to utilize “lessons learned from Privacy to improve the approach and success of Security implementation; especially in the areas of P&P development, communications planning and training of the workforce



Questions????