HIPAA Security Training

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

Presentation Overview

- Introduction
- Culture of Health Care
- Training Requirements & Delivery

Introduction

John Parmigiani

- CTGHS National Director of HIPAA Compliance Services
- HCS Director of Compliance Programs
- HIPAA Security Standards Government Chair/ HIPAA Infrastructure Group
- Directed development and implementation of security initiatives for HCFA (now CMS)
  - Security architecture
  - Security awareness and training program
  - Systems security policies and procedures
  - E-commerce/Internet
- Directed development and implementation of agency-wide information systems policy and standards and information resources management
- AMC Workgroup on HIPAA Security and Privacy;Content Committee of CPRI Security and Privacy Toolkit; Editorial Advisory Boards of *HIPAA Compliance Alert's HIPAA Answer Book* and *HIPAA Training Line;* Chair,*HIPAA-Watch* Advisory Board; *Train for HIPAA* Advisory Board

ctg HealthCare Solutions

Culture

Culture of Health Care

- Poor history of adopting standards
- Limited resources for security
- Privacy is not a market differentiator
- Most believe the risk is low
- Up until HIPAA, few incentives
- Can't have privacy without security

Question: *How long does it take to change an organization's culture?*

HIPAA = Culture Change

ctg HealthCare Solutions

Organizational culture will have a greater impact on security than technology.

Must have people optimally interacting with technology to provide the necessary security to protect patient privacy. Open, caring-is-sharing environment replaced by "need to know" to carry out healthcare functions.

Culture Change

ctg HealthCare Solutions

What is the most effective way to change an organization's culture?

Training (Hands-on), Education (Knowledge), and Awareness (Top of Mind)

Training Requirements

Workforce Training

- **Privacy and security* training to:**
  - **Entire workforce by compliance date**
  - **New employees following hire**
  - **Affected employees after material changes in policies**
  - **Both general and targeted**
  - **Need to document**

**can combine, since symbiotic relationship*

Workforce Training…

- Training must be in the entity's privacy and security policies and practices (not just HIPAA)
- "Workforce" includes employees, volunteers, trainees and others whose work is under the provider's control.
- Hospital medical staff are not workforce, but privacy training for physicians is advisable.
- Method of training is not specified (videos, handouts, tapes, etc.)

Topical Areas

HIPAA Security Training Requirements:

- Individual security responsibilities
- Virus protection
- Monitoring login success and failure
- Incident reporting
- Password management

Topical Areas

ctg HealthCare Solutions

Others topics may include:

- **Policies and Procedures** (with respect to protecting health information)
- **Confidentiality, Integrity, Availability (CIA)**
- **Sensitivity of health data**
- **Threats to information security**
- **Countermeasures** (Physical, technical, operational)
- **Sanctions for security breaches**

Training Delivery

Steps Toward Compliance…

ctg HealthCare Solutions

- Develop programs for Awareness, Education, and Training
  - Identify various audiences
  - Determine specific needs of each audience
  - Determine best mode of delivery
  - Establish a "certification" test for each aspect of the program (to ensure knowledge transfer and for proof of compliance)

How People Learn

- 10 % by Hearing
- 40% by Seeing
- 50% by Doing

"What I hear, I forget.
What I see, I remember.
What I do, I understand."
- Confucius 451 BC

Training Delivery Mechanisms

- Briefings
- Formal Classroom Training
- Video
- CBT
- WBT
- Conferences

Some Commonly Used Methods

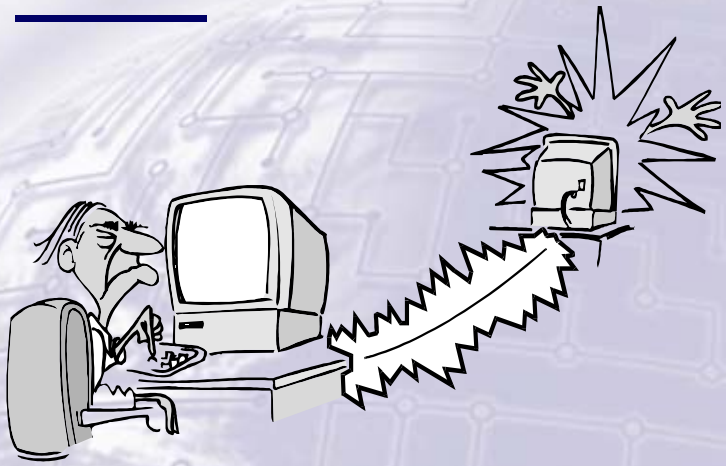
- Fliers or handouts
- Posters
- An *Intranet* web page
- Articles in company newsletters
- Promotional products

  EX: Mouse pads, rulers, stress balls, flowers, etc.
- Presentations at meetings
- "Munch-N-Learn"

  Bring snacks! ("If you feed them, they will come.")

Less Common Methods

- Host special events
- Integrate security into other training classes
- Use screen savers with awareness reminders
- Use network logon messages
- Look for "teachable moments"
- Develop security "champions"
- Leverage a "negative event"
- Use the "Grapevine"



Targeted Training

- **Board Members and Executives**
  - **Stress oversight role and consequences of non-compliance**
  - **How rest of industry is addressing compliance**
  - **Up-to-date awareness of guidance, rulemaking, and legislative changes**
- **Front-line Staff**
  - **Emphasize privacy and how it's protected by security**
  - **Describe penalties for rogue actions**
  - **Explain good security practices**

Targeted Training…

- Administrative Staff
  - Emphasize good security practices
  - Describe how access to PHI must be terminated when the employee leaves or is reassigned to a new function
- Technical Staff
  - Emphasize security mechanisms for protecting data at rest and in transit
  - How to implement authentication and access, disaster recovery, encryption, etc. requirements

Targeted Training…

- **Support Staff- cleaning, maintenance, business associates, etc.**
  - **What to do when they encounter PHI: any information seen on someone's desk or computer monitor is private and nothing is to be done to it**
  - **Any information, not their own, is not to be discussed even if accidentally viewed**

Preferred Delivery Modes

- New hires- Internet, Intranet, or multi-media computer training
  - Can be accessed at anytime
  - Same question can be repeated
  - Can be turned off when audience loses interest
  - Best as introduction

Preferred Delivery Modes…

- Clinicians, mid-level managers, and board members- Stand-up presentations
  - Can be customized
  - Speaker can respond to questions from the audience
- Departmental point people- train-the-trainer approach
  - Can relate to co-workers and provide relevant, pertinent lessons
  - Impact on each departmental function explained

Keep it simple!

"Our next speaker's remarks are encrypted.
Those of you with hand-helds may log on if you have the password."

Cartoon by Dave Harbaugh from hcPro's healthcare Humor

Thank You

Questions?

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