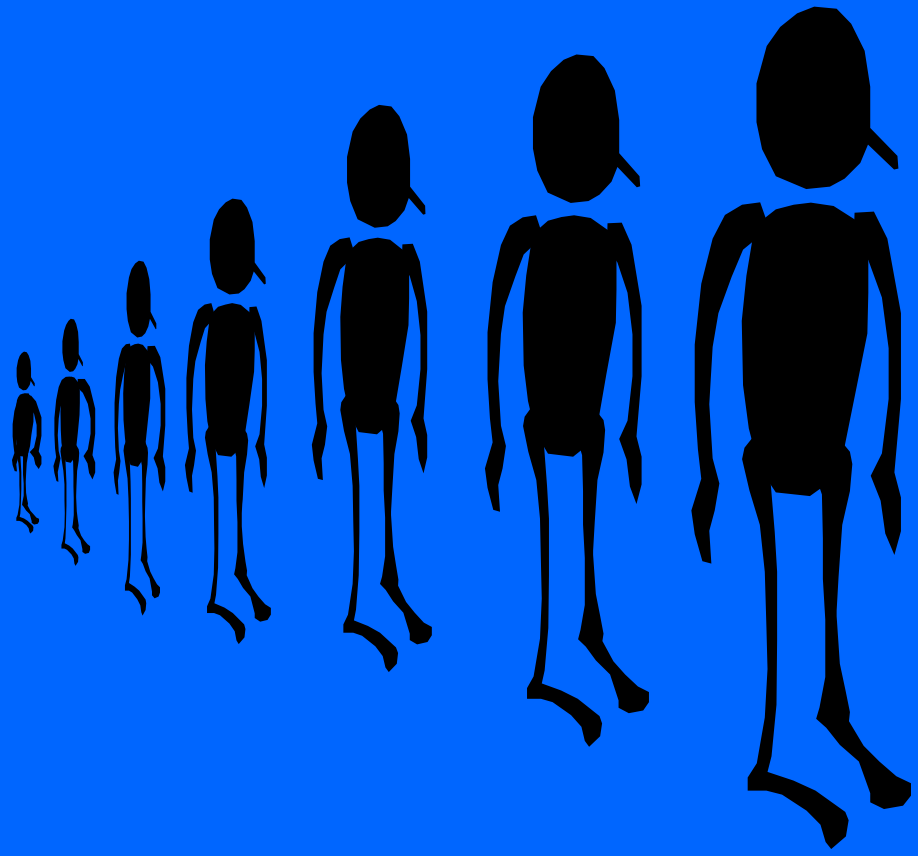
Complying with the Ongoing HIPAA Workforce Training Requirement

Kate Borten, CISSP, CISM
President, The Marblehead Group

Training Checkup

- Agenda
  - Who
  - What
  - (Where)
  - When
  - Why
  - ... and How

WHO



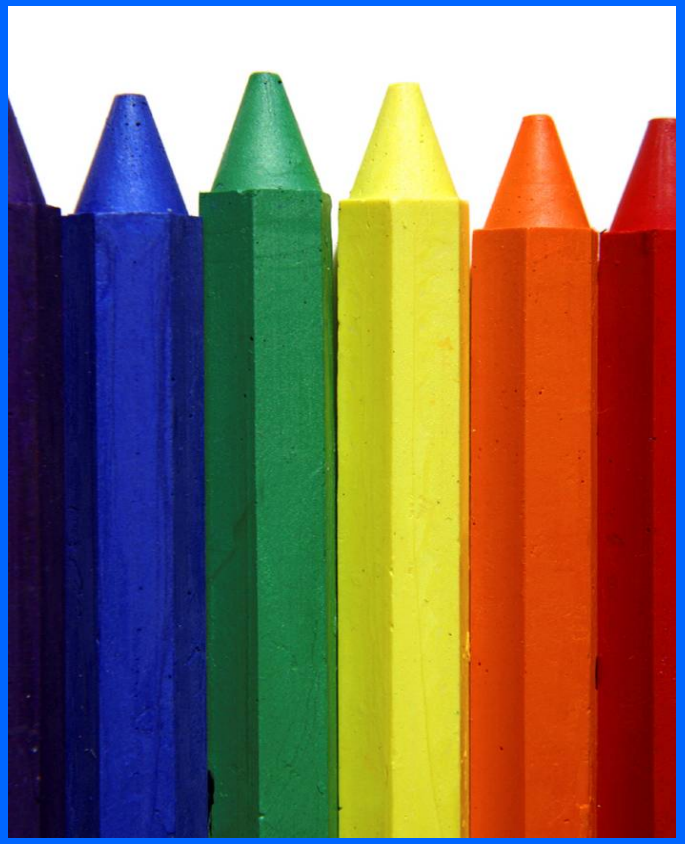
Who Needs Privacy & Security Training

- Full "workforce"
  - Including management
  - Including trainees, students, volunteers, certain contractors
- Not required, but consider
  - Temp agencies with relationship (share or review program, materials, 'certification')
  - BAs who may not have resources, insight (share program, materials)

NIST Special Publication 800-16 Rev1 (adapted)

- Geared to federal agencies, but good guidance for all *(csrc.nist.gov)*
  - Expose all users to privacy & security awareness materials
  - Provide additional training with specific materials to certain groups such as
    - Executives
    - Managers
    - CIO, system/network/application administrators, and operations personnel
    - Auditors
  - Provide role-specific training to users with significant information security responsibilities

WHAT



Content Scope

- Full scope should include
  - Privacy *and* security
  - … of PHI in all forms
  - And (beyond HIPAA, but good practice) for any other information resources needing protection such as
    - Payroll, HR
    - Confidential business strategies, plans
    - Legal matters

Privacy and Security Basics

- Privacy
  - What does it mean
  - What are standard “fair information practices”
- Security
  - What does it mean (CIA defined)
  - Security program = administrative, physical, and technical (examples)
- Key principles
  - Minimum necessary; need to know

What's Being Protected Here

- Define PHI (examples)
- Identify other information to be kept confidential

Describe Threats to Privacy & Security

- Internal and external
- Examples of natural, environmental, and human threats
- Social engineering - examples and tips
- Spyware
- Phishing
- Scams and spam
- Identity theft

Common Privacy Topics

- Privacy notice content summary (if a CE)
- PHI uses and disclosures only when part of one's duties (and minimum necessary)
- Specialized topics for appropriate audiences
  - Use/disclosure of PHI for involvement in care
  - Facility directory
  - Authorizations
  - Responding to patient rights requests
  - Fundraising, marketing, research
  - Etc.

Common Security Topics

- HIPAA security rule: login monitoring (A), protection from malware (A)
- Password management
- Acceptable use of organization computers, network
- Physical security (e.g., conversations in public, badges, clean desk, screen angle, locked areas)
- Disposal (e.g., shredding paper, clearing e-data)
- Email; faxing

Common Security Topics (cont'd)

- Encryption
- Portable devices and media
- Working offsite and remote access
  - Including anti-malware protections, personal firewalls
- Data backup (if users are responsible)
- Software/application updates (if users are responsible)

Privacy and Security Incidents: Violations and Breaches

- Examples
  - Privacy and security examples
  - From minor to moderately serious to very serious
  - (the more examples, the better the understanding and recognition by the workforce)

Consequences

- Harm to individuals (examples… make it personal)
- Plus
  - Legal consequences for the organization and individual who caused violation/breach
  - Cost to the organization
  - Reputational harm to the organization
  - Sanctions if caused by workforce member (reminder of **sanction policy**)

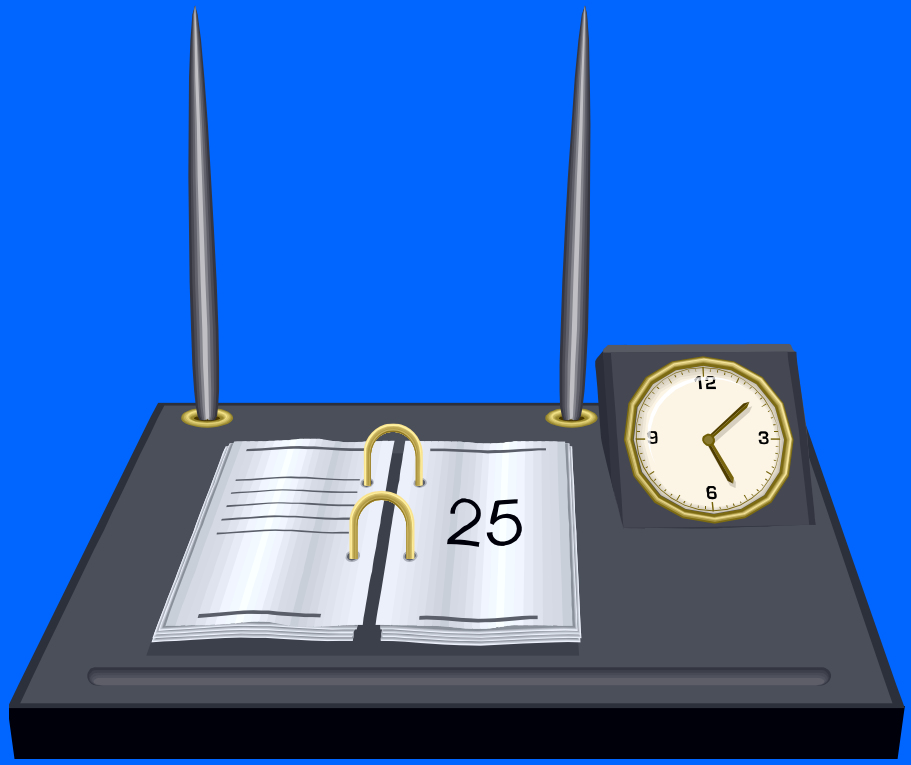
Reporting an Incident

- Individual's responsibility to report actual and suspected violations immediately
- Instructions (whom to call or email; KISS)
- Report immediately so that the team can begin response promptly... clock may be ticking (e.g., HITECH breach notification)
- No retaliation (reminder of policy)

Contact Info

- Who is the privacy official and how to contact
- Who is the information security official and how to contact
- Questions and suggestions encouraged

WHEN



HIPAA Rules & Timing

- Privacy rule somewhat vague
  - "To each new member of the workforce **within a reasonable period of time after the person joins the covered entity's workforce**; and
  - "To each member of the workforce whose functions are affected by a material change in the policies or procedures required by this rule, **within a reasonable period of time after the material change becomes effective**"
  - However, preamble sets expectation of some training even when someone is onsite (has PHI access) for only a few days

- Security rule also vague on timing
  - "Implement a security awareness and training program for all members of its workforce (including management)."
  - However, "program" => more than once, i.e., periodically and as needed when changes

NIST SP 800-16 Rev1 (adapted)

- Provide information security awareness and training to all new employees before allowing them access to systems
- Thereafter, at least annually
- Provide information security refresher training as frequently as appropriate, based on the sensitivity of the information that the employees use or process
- Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training

WHY

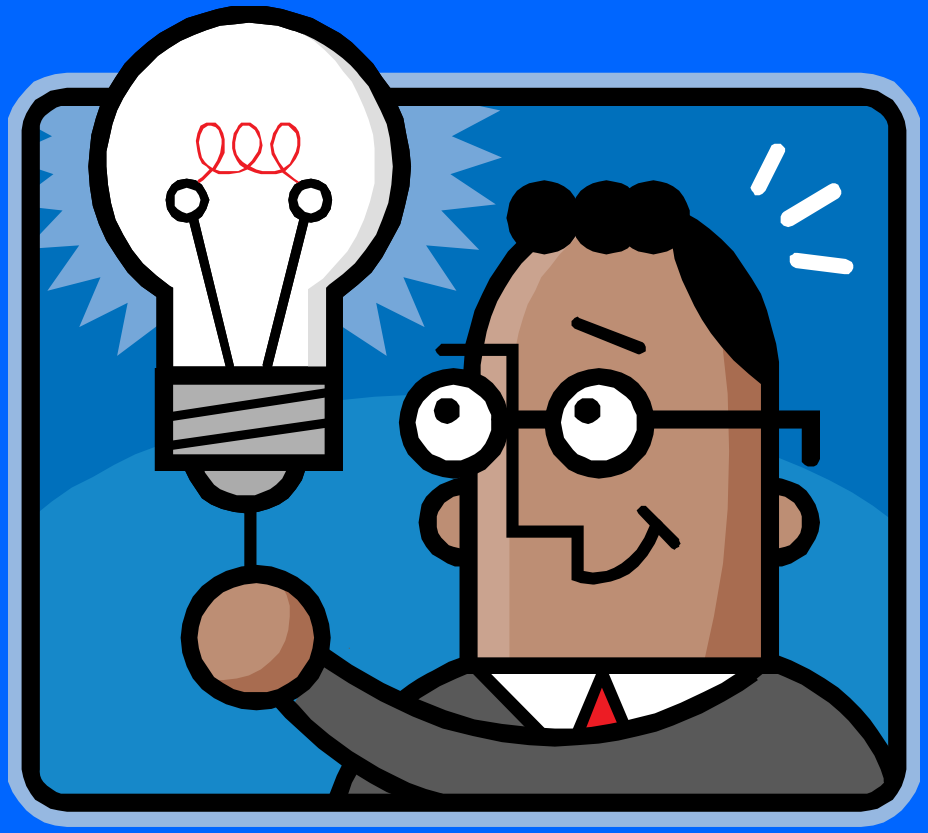
Why Train

- Yes, it's a legal requirement
- But also it's part of doing business. Makes sense to proactively protect an organization's information assets from loss of privacy, loss of data integrity, loss of availability since those losses would interfere with business... *and then some*

NIST SP 800-16 Rev1 (adapted)

- Fundamental value of information security (and privacy) awareness and training programs is that they change attitudes which should begin to change the organizational culture. “The cultural change sought is the realization that information security is critical because a security failure has potentially adverse consequences for everyone. Therefore, information security is everyone’s job.”

HOW



Training Techniques

- Privacy & security awareness and training
  - Classroom and/or computer-based instruction
  - Videos
  - Handouts (including customized to different levels of need)
  - Reminder messages (computer banner, email)
  - Staff meetings (agenda topic… “in the news”)
  - Newsletter articles (e.g., breaches in the news)
  - Posters
  - Trinkets (Post-it notes, pens, etc. with message)
  - Privacy & security day fair (vendors, give-aways)
  - Contests (prizes)
- Try to use multiple techniques to reinforce and to meet different learning styles
- Try to vary techniques and content to keep materials fresh

Customize for Audience

- Streamline for senior level (as appropriate if not accessing PHI, for example)
- Summarize and highlight main points for
  - Short-termer (e.g., visiting professional on site for two days)
  - New worker who won't get formal training for a week or more
- Etc.

Testing

- Not required, but good practice
- Options
  - Before-and-after quiz to show improvement
  - Quiz at end of presentation or online module to demonstrate comprehension
- Testing can also be used to demonstrate value of privacy/security program

Documentation

- Privacy rule requires documentation that training was provided; this is bare minimum
- Better to also take opportunity to get each person to sign (paper or online) training acknowledgement and agreement to follow privacy & security policies and procedures (signing should be a condition of employment)
- Consider coordinating with performance reviews

FINALLY …

- Monitor for compliance
  - Perform a review of the training program, checking the who, what, when, and how
  - Ensure new privacy/security requirements are added to training as appropriate
- Monitor for continuous improvement
  - Investigate and solicit creative ideas
- Revise training program as needed

Questions?

Kate Borten, CISSP, CISM
President, The Marblehead Group
1 Martin Terrace
Marblehead, MA 01945
781-639-0532
kborten@marbleheadgroup.com