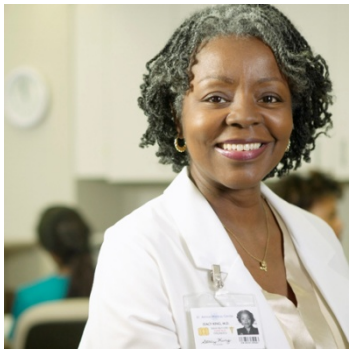

AMA Presentation at the CMS & NIST Workshop

Mari Savickis
Assistant Director, Division of Federal Affairs
American Medical Association
January 16, 2008

AMA
TOGETHER WE ARE STRONGER

HIPAA Security Rule Compliance for Physician practices

- The challenge: A significant number of physicians are in small and solo practices
- These practices typically lack IT resources, or time to understand HIPAA security and apply it
- These practices typically have limited IT knowledge (ie “what is a right click?”)

The challenges….

- Many practices believe that HIPAA is “privacy”
- Lack of understanding that HIPAA includes a separate Security rule
- Less outreach following transactions and code sets and privacy rules

The challenges…

- The terminology of the security rule is overwhelming and unfamiliar
  - For example the concept of a “risk analysis” is well understood by IT professionals but foreign to physicians and their staff
- Investment in HIPAA education competes with other priorities
  - Still viewed as an unfunded mandate

The challenge

- Many physician practices rely on their vendors for HIPAA security compliance
- Physicians trust their vendors when they tell them they are “HIPAA compliant”
- More and more physicians are using technology but some still perceive avoiding it will help limit privacy violations

Solutions?

- Great outreach and education is a must!
- The recent CMS guidance “Security Standards: Implementation for the small provider” is an good start
- Continuing education and awareness is required

Solutions---focus

- A number of security compliance areas continue to be prevalent:
  1. Lack of understanding and confusion over the requirement for a risk analysis
  2. Missing basic written policies and procedures
  3. Poor administrative policies-sharing of passwords or forgetting to do back ups

Solutions-focus

4. Failure to employ strong authentication
5. Failure to report and respond to security incidents
6. Failure to have a contingency plan
7. Training is non existent
8. Weak “perimeter control” in terms of physical security and technical security

Summary

The AMA strongly urges CMS to:

- Make HIPAA security an education / outreach priority
- Focus on helping physicians understand what is required of them in a way that they can digest, information that is practical, and tips on meeting compliance through the scalability and flexibility called for in the rule
- Continue to engage physicians especially smaller ones
- Place emphasis on giving physicians the tools they need to achieve compliance rather than any punitive efforts
- Engage the AMA's feedback – we welcome the opportunity!


AMA
AMERICAN
MEDICAL
ASSOCIATION