MEDICAL GROUP MANAGEMENT ASSOCIATION — GOVERNMENT AFFAIRS

Medical Group Management Association
MGMA®

Leveraging HIPAA Security to Improve Your Medical Practice

CMS/NIST Security Workshop

Jan. 16, 2007

Robert M. Tennant, MA
Senior Policy Advisor
Medical Group Management Association

Government Affairs
Medical Group Management Association

Current Security Environment

- Practice use of electronic data increasing
- ID theft, security breeches a seemingly everyday occurrence
- Patients increasingly aware and concerned
- Practices VERY focused on HIPAA privacy…
- VERY unfocused on HIPAA security!

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

The two most important words in HIPAA security….

Medical Group Management Association
MGMA®

Why should you bother with HIPAA Security?

Government Affairs
Medical Group Management Association

What if your practice experienced a…

- Loss of financial data
- Temporary loss of medical records
- Permanent loss of confidential information
- Unauthorized access to confidential information
- Damage/loss of physical assets (i.e., computers, PDAs)
- Damage to clinic reputation, patient confidence
- Government enforcement action

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Potential Events

- Unauthorized access by employees
- Misuse of authorized access
- Physical disasters
- Server crashes
- Staff untrained on dealing with security issues
- Ineffective disposal of PHI

Threats

- Current employees (most common)
- Former employees
- Patients / visitors
- Vendors
- Equipment failures / weather
- Criminals

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Leveraging Security

- CMS has blessed us with…

  A Wonderful Final Rule!!!!

  – A clear blueprint for protecting your practice
  – A reminder of what you already should be doing
  – Gives you the flexibility to decide how to best protect your practice

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Security Rule—Key Concepts

- Provisions are either “Required” or “Addressable”
- Technology “neutral”
- Risk analysis/risk mitigation required
- Scalability: “flexibility of approach”
  - Size
  - Complexity
  - Capabilities
  - Technical Infrastructure
  - Cost of security measures
  - Potential security risks

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Implementing Security

- Where to begin?
  - Risk analysis
  - Gap analysis
    - Current state vs rule requirements
  - Start to develop policies and procedures (look for industry best practices)
  - Manage your risk
  - Documentation is critical
  - Start with physical security

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Security Compliance-Critical Questions

1. Do you know who has internal/external access to your systems?
2. Do you have software that tracks access to electronic patient information?
3. Does your information system have appropriate password and user identification protection in place?
4. Does it have event alarm software that can track unauthorized access?
5. Does your system have logon audit controls that identify who accessed particular information?
6. Do I have sufficient policies to handle PDA/laptops?
7. Do you have sufficient backup procedures/devices?

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Practical Issues—Security Compliance

- Larger clinics may wish to hire a consultant
- Difficult (but not impossible) for smaller clinics to organize compliance on their own
- Typical problems:
  - Training/education
  - Implementation planning
  - Policies, procedures and forms
  - How to decide what are the industry “best practices”?
- Look to industry groups/peers for assistance

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Final Thoughts

- Train your staff!
  - Utilize staff as mini security/privacy auditors
  - "HIPAA Hunt" with prizes?
  - Incorporate regular security/privacy reminders into staff training
  - "Real scenarios" effective learning tool
- Consider publicizing your commitment to security/privacy through posters/plaques etc
  - "*Patient Rights in Our Clinic*"

Medical Group Management Association MGMA®

Government Affairs
Medical Group Management Association

Resources

- Plenty of free or low cost resources to help you:
  - www.cms.hhs.gov (security series)
  - www.wedi.org
  - www.nist.gov

Medical Group Management Association MGMA®