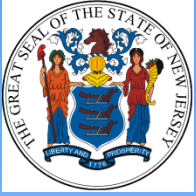# PREPARING for an OCR PRIVACY + SECURITY AUDIT

**Susan A. Miller, JD**

**HIPAA Summit West, October 2010**

# Agenda

- **What is an audit?**

- **Audit history**

- **What do you audit?**

- **Steps to take to protect your organization**

# What is an AUDIT?

- **An audit is an evaluation of your organization against specific requirements**
  - **HIPAA Privacy**
  - **HIPAA Security**
  - **HIPAA Breach and Breach Notification**
  - **HITECH Act updates**
  - **P+S within EHR Incentives Final Rule?**

# HIPAA Audit History

- **HIPAA Privacy + Security Rules**

- **OESS - Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews**

- **HITECH Act: Sec. 13411 AUDITS**
  - **periodic audits to ensure that covered entities and business associates to the requirements subparts C and E of part 164 of title 45, Code of Federal Regulations**

# What Do You AUDIT?

- **System, process, office or product ....your whole enterprise**
  - **Your EHR, your Internet connections, your servers, other electronic tools**
  - **Your Access databases, Excel spreadsheets**
  - **Your business processes, your workflow**
  - **Your connection to HIE/RHIO**
  - **Your physical security**

# Steps to Protect your Organization

- **Auditing and monitoring plan in place**
  - **Know your own organization, needs, and problems**
  - **OESS – Security Audit Checklist**
  - **42 questions form Piedmont**
  - **OCR compliance plans, examples, Providence Health System and CVS**

- **Easy way to report issues**

- **Test and role play**
  - **Update policies and procedures**
  - **Update training**

# OCR Enforcement Resources

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

- **Case Examples Organized by Covered Entity**
    - General Hospitals
    - Health Care Providers
    - Health Plans / HMOs
    - Outpatient Facilities
    - Pharmacies
    - Private Practices
- **Case Examples Organized by Issue**
    - Access
    - Authorizations
    - Business Associates
    - Conditioning Compliance with the Privacy Rule
    - Confidential Communications
    - Disclosures to Avert a Serious Threat to Health or Safety
    - Impermissible Uses and Disclosures
    - Minimum Necessary
    - Notice
    - Safeguards

# Contact Information

Sue Miller

TMSAM@aol.com