Connecting Healthcare®
Engaging Patients™

HIPAASuccess - Physician Education Series

HIPAA Audits and Enforcement

Your Faculty:
Susan A. Miller, JD

- Chief Operating Officer, and Privacy Officer, Connecting Healthcare
- Served as Advisor and Outside Attorney OCR, NIST and CMS
- Content drafter and manager NIST HIPAA Security Toolkit
- Served as Advisor and Outside Attorney NJ Medicaid Agency, GA Medicaid Agency
- Served as Director and Assistant Director on federal states HIPAA contract programs, MA and NJ
- Served as Advisor and Outside Attorney for covered entities, business associates, HIEs, and vendors
- Board Member, Southern Healthcare Administrative Regional Process (SHARP), a regional collaborative workgroup alliance of private and public health care organizations and HHS, HRSA and CMS
- Founding Security and Privacy Co-Chair for the Workgroup for Electronic Data Interchange (WEDi) Strategic National Implementation Process (SNIP)

Tag Line …

The ever changing roadmap of legal authority to use everyday and when the "%$+%" hits the fan!

AGENDA

- HIPAA Enforcement
  - OCR
    - Complaints, Investigations, + Audits
    - Guidance Documents + FAQs
- How does OIG fit in?
  - 2016 FY Hospitals' electronic health record system contingency plans
- What are the Cross-overs with Meaningful Use?
  - Encryption and Risk Analysis/Assessment
- What Other Federal Agencies?
- What is a Digital Copyright?
- State Laws and Regulations Impacts
  - Plus, State Insurance Commissioners
- Court Cases
- How to Protect Your Organization
- Cybersecurity Insurance

HIPAA Enforcement

- **The Office for Civil Rights [OCR]**
  - Writes HIPAA Security, Privacy and Breach Notification Regulations
  - Enforces HIPAA Security, Privacy and Breach Notification Regulations
  - Keeps the penalties and fines imposed
  - **Legal Authority**:
    - The laws: HIPAA, the HITECH Act
    - The related regulations
      - Notice of Proposed Rule Making [NPRM]
      - Final Rule [FR]
    - The regulations' preambles
    - OCR Guidance Documents
    - OCR FAQs

HIPAA Enforcement

Complaints to the Secretary: in the original1996 Law and related regulations

- 45 CFR 160.306
- http://www.hhs.gov/ocr/privacy/hipaa/complaints/

Complaint Requirements - Your complaint must:

- Be filed in writing, either electronically via the OCR Complaint Portal, or on paper by mail, fax, or e-mail;
- Name the covered entity or business associate involved and describe the acts or omissions you believe violated the requirements of the Privacy, Security, or Breach Notification Rules; and
- Be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause."

HIPAA Enforcement

Complaints to the Secretary

- **ANYONE CAN FILE!**
- **HIPAA PROHIBITS RETALIATION**
- **HOW TO SUBMIT YOUR COMPLAINT** - *To submit a complaint, please use one of the following methods.*
  - File your complaint electronically via the OCR Complaint Portal at https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf
  - File A Complaint Using Our Health Information Privacy Complaint Package at http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf
  - File A Complaint Without Using Our Health Information Privacy Complaint Package at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html#nopackage
  - File A Security Rule Complaint at https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf;jsessionid=E68436962D0B81F547503C5016113B55.ajp13w

HIPAA Enforcement

- **Investigations**: from the original 1996 HIPAA Law and related regulations
  - 45 CFR 160.306(c)
  - The Secretary will investigate any complaint when a preliminary review of the facts indicates a possible violation due to willful neglect
  - The Secretary may investigate any other complaint filed

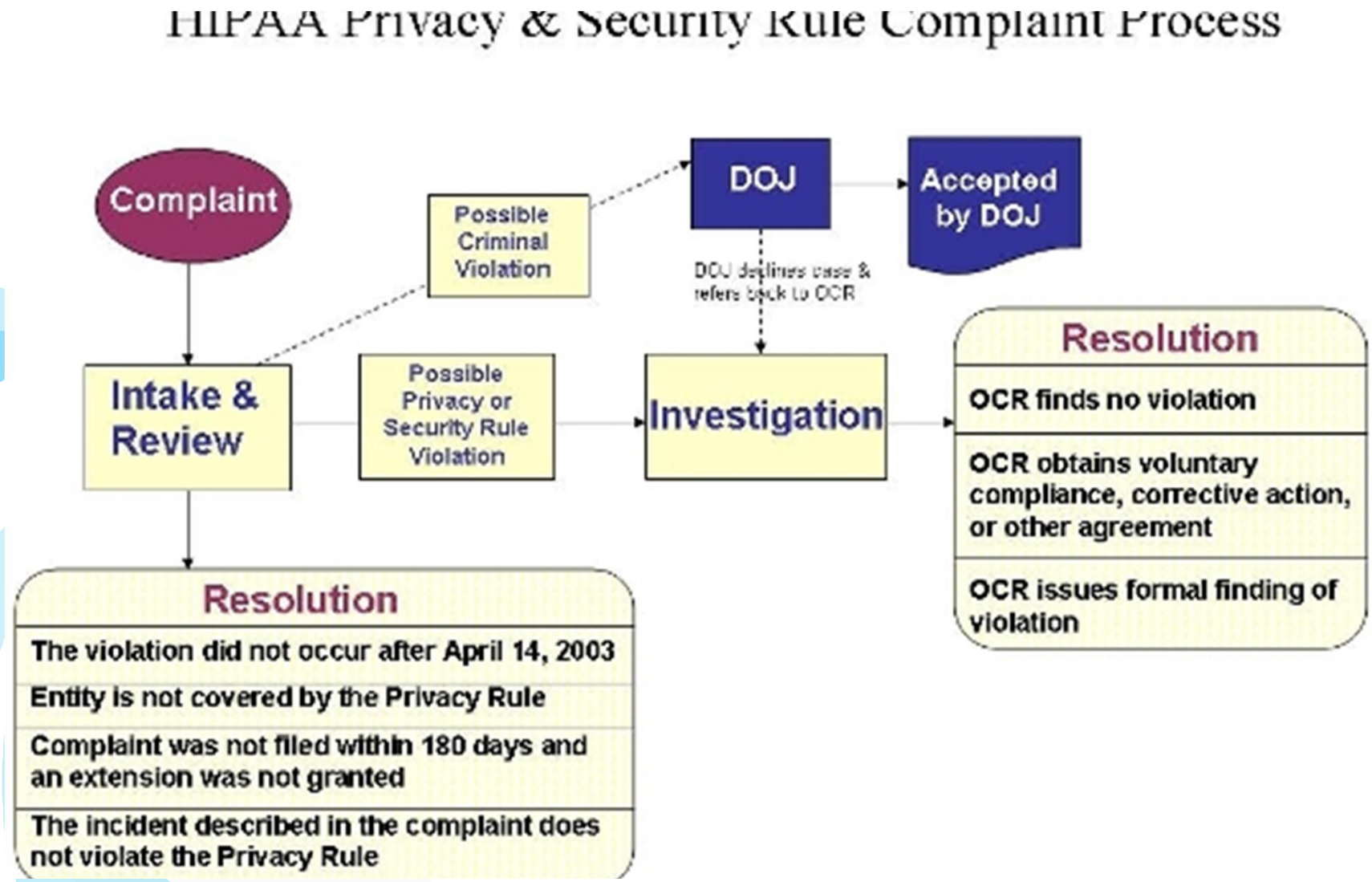
- **Results in**:
  - Resolution Agreements
  - Corrective Action Plans
  - Penalties and Fines

HIPAA Enforcement

Penalties and Fines

Violations	Amount per Violation	Violations of an identical provision in a calendar year
Did not know	$100 - $50,000	$1,500,000
Reasonable cause	$1000 - $50,000	$1,500,000
Willful neglect - corrected	$10,000 - $50,000	$1,500,000
Willful neglect – not corrected	$50,000	$1,500,000

HIPAA Criminal Enforcement



HIPAA Enforcement

Guidance: Significant Aspects of the Privacy Rule

- Introduction
- General Overview
- Incidental Uses and Disclosures
- Minimum Necessary
- Personal Representatives
- Business Associates
- Uses and Disclosures for Treatment, Payment, and Health Care Operations
- Marketing
- Public Health
- Research
- Workers' Compensation Laws
- Notice
- Government Access
- Decedents
- Student Immunization
- Marketing: Refill Reminders

HIPAA Enforcement

Special Topics at
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/index.html

- Public Health
- Research
- Emergency Situations: Preparedness, Planning, and Response
- Health Information Technology
- Genetic Information
- Information is Powerful Medicine: HIV and HIPAA
- HIPAA Privacy Rule and the National Instant Criminal Background Check System (NICS)
- HHS Strengthens Patients' Right to Access Lab Test Reports
- HIPAA and Same-sex Marriage: Understanding Spouse, Family Member, and Marriage in the Privacy Rule
- OCR Invites Developers to Ask Questions about HIPAA Privacy and Security

HIPAA Enforcement

Security Rule Guidance http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

- Security 101 for Covered Entities
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational, Policies and Procedures and Documentation Requirements
- Basics of Risk Analysis and Risk Management
- Security Standards: Implementation for the Small Provider

Plus: Risk Analysis, and Remote Use

HIPAA FAQs at http://www.hhs.gov/hipaa/for-professionals/faq

Preambles – in both NPRMs and FRs

HIPAA Enforcement

- **Audits**: in the HITECH Act and *does not have any regulations* at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html
  - Phase 3 to begin 1Q2016
  - New/updated protocols to be posed by 12/31/2105 at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Can grow into an investigation, and
  - Result in:
    - Resolution Agreements
    - Corrective Action Plans
    - Penalties and Fines

OCR + ?

How Does OIG Fit In?

- **HHS Office of Inspector General's mission**
  - "to protect the integrity of Department of Health & Human Services (HHS) programs as well as the health and welfare of program beneficiaries. Office of Inspector General's (OIG) mission is to protect the integrity of Department of Health & Human Services (HHS) programs as well as the health and welfare of program beneficiaries"
- **OIG FY 2016 Work Plan**
  - Scrutinize federal regulators' oversight of security controls
    - OCR delays in launching a permanent HIPAA audit program
    - FDA medical device cybersecurity

What Are the Cross-overs with Meaningful Use

- **Stages 1, 2 and 3** have hooked the Meaningful Use requirements to the HIPAA security rule requirements
  - Administrative Safeguard:
    - Risk Analysis/Assessment
  - Technical Safeguards
    - Access Control + Transmission Security:
      - Encryption

What Federal Agencies

The 4 Federal Agencies all claim part of HIPAA Privacy and Security

- **OCR** (Office for Civil Rights) writes and enforces the HIPAA security, privacy and breach notification regulations
- **NIST** (National Institute of Standards and Technology) writes guidance documents and developed the NIST HIPAA Security Toolkit
- **FDA** (Federal Drug Administration) regulates medical devices
- **FTC** (Federal Trade Commission) protects consumers privacy; current focus includes, and has included, the privacy promises made on the Internet websites

What Is a Digital Copyright?

- **Protecting intellectual property on the Internet**

- **Librarian of Congress** final rule http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf

State Laws and Regulations Impact

Federal Identity Theft Law? Not yet!

- **Almost all States and Territories have Identity Theft Laws**
  - Many of them include medical/healthcare information
- **Some States have laws and regulations very much like the HIPAA Breach Rule**
  - California
  - Massachusetts

Court Cases

Federal Court

- Many of the cases filed in Federal Courts are class action suits. Most class actions suites fail due to having no standing; in other words you do not have the right to file the suit
- There is a Supreme Court case that states to have standing there must be "actual or imminent injury"
- On the other side of the coin, there is a case that originated in a Florida District Court [February 2014] that permitted a $3 million settlement for a certified class despite no injuries in fact

States Court

- The standing limitations found in Federal Court does NOT apply in state courts
- Some state courts have permitted individuals to circumvent the lack of an individual private right of action in HIPAA by claiming that the HIPAA privacy and security regulations are a standard of care in state law negligence claims
- The standard of care is the degree of prudence and caution required of an individual or entity to provide and use. The requirements of the standard are often dependent on specific circumstances and facts of a case

How to Protect Your Organization

- **Organization Protections**
  - Yearly Risk Analysis/Assessment + Remediation
  - Yearly Review HIPAA Policies and Procedures and all other documentation
  - ***Encryption, encryption, encryption***
  - ***Cybersecurity Insurance***

- **Patient/Member**
  - Help with Credit Reporting Services is OK, but
  - Practical Outline of the impact much more important
    - See FTC https://www.identitytheft.gov

Cybersecurity Insurance

- **Cybersecurity insurance** transfers some of the financial risk of a security breach to the insurer
  - It is only a risk management strategy
  - It is not a security breach solution
  - Clear working is essential
  - It may not include coverage for privacy breaches
  - It is different from liability insurance

Free Tools

- **NIST HIPAA Security Toolkit** at *http://scap.nist.gov/hipaa/*
- **ONC Risk Assessment Toolkit** at *http://www.healthit.gov/providers-professionals/security-risk-assessment*
- **NIST National Cybersecurity Center of Excellence (NCCoE)** at https://nccoe.nist.gov

Takeaways

1. **Do an honest Risk Analysis/Assessment Yearly**
   - **Include all new technologies + services**
2. **Plan and implement your Risk Management**
   - **From your risk analysis report**
3. **HIPAA Audit: Review/update/modify all your HIPAA documentation yearly, and**
4. **Encrypt everything you reasonably can**
5. **Consider Cybersecurity Insurance**

Questions

Thank You

Please contact:

- **Susan A. Miller, JD**
- **COO, CPO, Connecting Healthcare**
- **O = (978) 369-2092**
- Susan.Miller@ConnectingHealthcare.com