The Complexity of HIPAA Enforcement

The HIPAA Privacy, Security and Breach Notification Regulations are written and enforced by the Office for Civil Rights (OCR). This enforcement is within the general provisions of the HIPAA regulations (see 45 CFR §§ 160.300 – 316).

The HITECH Act of the American Recovery and Reinvestment Act of 2009 (ARRA) added several other types of enforcement.

Enforcement Types:

- **Regulatory** – civil enforcement
  - Complaint (see 45 CFR §160.306)
    - How to file http://www.hhs.gov/ocr/privacy/psa/complaint/index.html
  - Compliance Review (see 45 CFR §160.308)
  - Penalties
    - Violation, did not know, $100 -- $50,000, $1.5 M
    - Violation, reasonable cause, $1,000 -- $50,000, $1.5 M
    - Violation, willful neglect with correction, $10,000 -- $50,000, $1.5 M
    - Violation, willful neglect no correction, $50,000, $1.5 M
- **Regulatory** – OCR submits to the Department of Justice, criminal investigation and enforcement
  - Penalties:
    - $50,000 and/or up to 1 year imprisonment
    - $100,000 and/or up to 5 years imprisonment for false pretenses
    - $250,000 and/or up to 10 years imprisonment if commercial advantage, personal gain, or malicious harm
- **Regulatory** – Breach report to OCR
  - How to report a breachhttp://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
- **Regulatory** – Preemption (see 45 CFR §§ 160.201 – 205)
  - Contrary
  - More stringent
  - Omnibus Rule – GINA, underwriting
- **Statutory**
  - HITECH Act
    - State Attorneys General http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html
      - Civil penalties
      - Attorneys' fees
      - Perhaps some return to individual harmed
    - Proactive Audit Program http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html

Complaints, Compliance Reviews, and Audits have resulted in significant fines!