

# MARTI ARVIN

University of Louisville  

---

Privacy Officer

Phone: 502-852-3803

Fax: 502-852-3855

Email: [marti.arvin@louisville.edu](mailto:marti.arvin@louisville.edu)



# HIPAA Compliance

---

The continuing challenges



# AGENDA

---

- ❑ The HIPAA enforcement rule and what it could mean to physician practices
- ❑ How to conduct an ongoing risk assessment as required by the security rule
- ❑ How to handle a HIPAA complaint in your practice?
- ❑ Q & A



# The HIPAA enforcement rule

---

- The HIPAA enforcement rule was finalized March 16, 2006
- The good news
  - OCR will continue to resolve issues informally if possible
  - Sanctions may not be imposed under certain circumstances
    - If the Secretary is satisfied that the person committing the violation did not know and with the exercise of reasonable diligence could not have known it was a violation
    - If the failure to comply was due to reasonable cause and not willful neglect
    - The violation would be a criminal violation
  - Sanctions may be reduced or entirely waived “to the extent that the payment of such penalty would be excessive relative to the compliance failure involved”



# The HIPAA enforcement rule

---

- The bad news
  - Once the enforcement process is started it will be difficult to get out of the process
  - The definition of a violation
  - You would not want to admit criminal liability to avoid civil fines



# The HIPAA enforcement rule

---

- A single act can constitute multiple violations
- Example:
  - The practice donates a computer to the local elementary school. The computer was not properly scrubbed and the information of 100 patients was compromised.
  - Violations
    - Security rule – improper technique for equipment disposal
    - Security rule – safeguard requirements
    - Security rule – information access management
    - Privacy rule – improper disclosure
  - Potential fines
    - Each standard that was violated carries a \$100 fine per standard.
    - There are three security rule violations and one privacy rule violation
    - The first two security rule violations may only count as one violation each
    - The last security rule violation and the privacy rule violation will likely count as one violation per patient
    - The minimum potential fine would be \$20,200
    - Change the fact to 1000 patients and the potential fine becomes \$50,200



# The HIPAA enforcement rule

---

- ❑ Failure to engage in a single act that is required by the rule can result in multiple violations.
  - Example
    - ❑ Your practice entered into a business relationship on December 12, 2005. This relationship requires a business associate agreement but one was not executed
    - ❑ Each day that a BAA is not in place is a violation
    - ❑ Potential fine \$26,900 (the BAA was not in place for 295 days but the maximum fine per standard is \$25000 per calendar year so \$1900 for 2005 and \$25000 for 2006)



# The HIPAA enforcement rule

---

- Example

- Your practice entered into five business relationships in 2005. These relationships require a business associate agreement. BAA terms were included but not all the required terms under the privacy and security rule were included
- The BAA are missing 3 of the required Privacy Rule terms and two of the required Security Rule terms
- Potential fine: \$2500 (3 privacy rule violation plus two security rule violations times 5 contracts times \$100 for each violation)



# The HIPAA enforcement rule

---

- The process outlined in the rule
  - OCR and/or CMS will try to resolve informally
  - If not resolved informally, letter will be sent to the CE
    - CE has 30 days to submit written evidence of mitigating factors or affirmative defenses

# The HIPAA enforcement rule

---

- Process continued
  - If OCR and/or CMS does not agree that affirmative defenses or other reasons not to impose a penalty apply the CE will:
    - Receive a notice of proposed determination
    - CE has 90 days to request a hearing before an ALJ
    - Once hearing is held, CE may appeal an unfavorable finding to the HHS Departmental Appeals Board
    - Next stop federal court



# The Risk Assessment Process

---

- ❑ You did your risk assessment when you implemented your HIPAA security compliance plan
- ❑ What have you done since?
- ❑ How often have you done it?
- ❑ What should you be looking at?
- ❑ Is it documented?



# The Ongoing Risk Assessment

---

- The Security Rule requires that you perform a risk assessment on an ongoing basis, what does this mean?
  - You should have some periodic process for evaluating risk
  - You should also have events that trigger a review of your prior risk assessment
  - Your actions related to compliance reviews of your security rule compliance should be modified accordingly



# The Ongoing Risk Assessment

---

- What should you look for in the ongoing risk assessment?
  - What were the high risk areas in your last assessment?
  - What has been done to mitigate or eliminate those risk?



# Ongoing Risk Assessment

---

- What should you be looking for in an ongoing risk assessment?
  - Have there been changes in the industry or at your organization that change the risk structure?
    - New anti-virus technology
    - Implementation of a new EMR
  - What have your compliance audits revealed?
    - Was something a higher/lower risk that you realized in the prior risk assessment?
    - Did you impose corrective action that needs to be reviewed or did it sufficiently mitigate the risk?



# Ongoing Risk Assessment

---

- ❑ This risk assessment may be part of a large risk assessment for the entire organization's compliance efforts
- ❑ The results should be the driver for your compliance reviews/audits for the coming review/audit period
- ❑ All of your efforts should be documented to demonstrate compliance with the Security Rule



# Handling HIPAA Complaints

---

- ❑ How does your privacy officer know there has been a HIPAA complaint?
- ❑ Who is tasked with handling complaints?
- ❑ Is the complaint documented?
- ❑ Is the process for resolving the complaint documented?



# HIPAA Complaints

---

- Some suggestions
  - Make sure you have a process to get the complaint to the Privacy Officer
  - If possible, make sure the complaint is investigated by someone that is independent and objective
  - Document the complaint, the investigation and the resolution
  - **DO NOT IGNORE COMPLAINTS**



# HIPAA Complaints

---

- ❑ Make sure someone acknowledges the complaint
- ❑ Be particularly conscientious if the complaint deals with information that has heightened protection
- ❑ Operate on a need to know regarding sharing information with others
- ❑ Depending on the nature of the complaint you may consider asking the complainant if he/she has talked with an attorney.



# HIPAA Complaints

---

- Document all conversations
  - The complainant.
  - Staff and others
- Document your resolution if you discover a violation has occurred.
  - Corrective action plan
  - Discipline if applicable and in general terms



# HIPAA Complaints

---

- ❑ If you discover no HIPAA violation has occurred inform the patient.
- ❑ Try to use lay person terminology
- ❑ Cite OCR FAQs if applicable
- ❑ If the complainant is still not satisfied offer them the number of OCR.

# QUESTIONS

---

