Roundtable Discussion of Healthcare IT Security Strategies

Sandra G. Behrens, ***Carnegie Mellon***

L. Arnold Johnson, ***NIST***

William R. Wilson, ***Carnegie Mellon***

Walter Wright, ***FBI***

Richard D. Marks, ***Davis Wright Tremaine LLP***

Hypothetical Case Study

- Major Academic Medical Center
  - 250,000 patient records on file electronically
- Hacker downloads 5,000 complete patient records & posts them to the Internet
- Hacker may still be probing
  - Using trail of computers to conceal identity
  - Where is hacker located?
- Medical Center CEO (with IS director) calls general counsel - what to do?
- General Counsel calls outside counsel

Hypothetical Case Study

- What advice do you have?
- What advice would you have given if you had gotten this call four months before the hacking started?
- What is the prevailing standard of care in the information security industry for dealing with this kind of problem?
- How does the HIPAA statute affect your advice?

HIPAA Statute

"Each person … who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards --

(A) to *ensure* the *integrity and confidentiality* of the information; and

(B) to protect against *any* reasonably anticipated

(i) threats or hazards to the *security or integrity* of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) *otherwise to ensure* compliance with this part by the officers and employees of such person."

(42 USC §1320d-2(d)(2); in effect now - does not require final security rules to become effective)

HIPAA Statute

- ✓ Civil penalties (42 USC §1320d-5) - HHS/ OCR
  - $100 each violation (transaction costs)
  - $25,000 annual limit for violating each "identical requirement or prohibition" - could be a big number
- ✓ Criminal penalties (42 USC §1320d-6) - DOJ/ U.S. Attorney
  - Knowingly - 1 year/ $50,000
  - False pretenses - 5 years/ $100,000
  - Malice, commercial advantage, personal gain - 10 years, $250,000

HIPAA Civil Suits

Private law suits by patients

- Easier because standard of care is so much higher
- Statute trumps the regs: "*any* reasonably anticipated," "ensure"
- Best practices - what is "any reasonable"? Are the references to security processes and technology in the security industry?