Compliance With HIPAA Privacy Rule Before Security & Enforcement Rules are Final: Challenges in Practice

National Audioconference

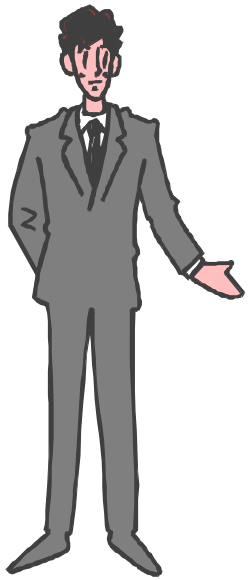
Sponsored by the HIPAA Summit

June 6, 2002

Chris Apgar, CISSP
Data Security & HIPAA Compliance Officer
Providence Health Plan

Presentation Overview

- HIPAA & Data Security
- Challenges & Deadlines
- Opportunities & Tactics
- Resources
- Contact Information



Data Security

Impact Overview

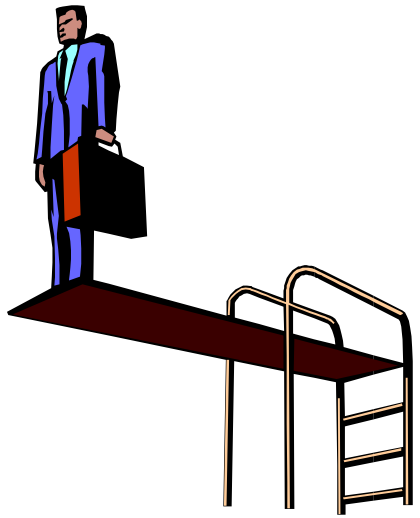
- Risk Assessment
- Policy & procedure development
- Training & awareness
- Contingency Plan
- Information access control (“need to know”)
- Audit & certification
- Documentation
- Record access (release management & file access)
- Personnel security & authentication
- Chain of Trust/Business Associate Agreement
- Security & privacy management
- Security incident response
- Physical security

Data Security

- **Rule likely not final no earlier than 3Q 2002**
- **Privacy Rule requires data security but regulatory definition not finalized**
- **In some cases court decisions have established draft rule as de facto standard**

Challenges & Deadlines

- Final privacy rule without security rule creates confusion and hampers compliance
- Coordination between plans, providers, business associates and regulators complicated
- Lack of industry scalable standards
- Lack of internal documentation & process
- Limited resources & time (Privacy Rule does require security)



Providence | Health Plans

Challenges & Deadlines

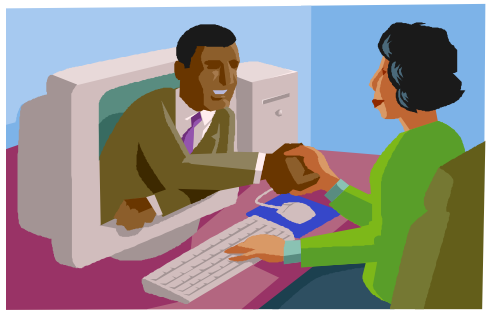
- Need to require security assurances from business associates but lack final standard
- “Just another IS project/regulatory requirement”
- No final rule increases the challenge of dedicating the resources
- Vendor reliance's – how do they spell security?
- Legal hindrances, contract changes & new litigation – courts & attorneys won’t go away

Challenges & Deadlines

- **Medicaid & Medicare: What standards will be applied?**
- **No published enforcement guidelines**
- **Political turf battles (federal/state/local) – the war to define security mandates**
- **Security certification not standard in healthcare & accreditation bodies want to get into the act**

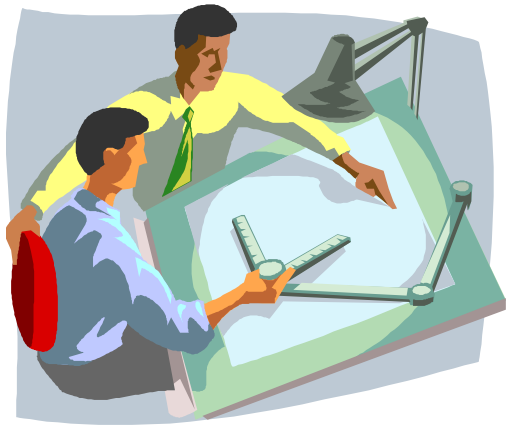
Opportunities & Tactics

- Privacy official & data security officer – grant authority and establish strong communication channels
- Complete risk assessment & gap analysis – point out costs of litigation and security failure
- Clearly and reasonably define what is needed when
- Senior management support required
- Apply appropriate project management methodology



Opportunities & Tactics

- **The better the documentation, the better the protection only if followed & current**
- **Standardize, simplify and enforce – cultural change required!**
- **Minimize exceptions to defined processes and boilerplate forms**



Opportunities & Tactics

- Education & training required
- Good security more process & culture than technology
- Review technical solutions & fit to organizational need
- Document protected health information storage, transmission, etc. process – how strong are your walls?

Providence | Health Plans

Opportunities & Tactics

- Develop contingency plan - what happens if the attorneys arrive or something goes wrong?
- Strengthen internal & external partnerships – participate in developing standards
- Keep current
- Remain flexible

Opportunities & Tactics

- Join industry/government HIPAA task force (local WEDI SNIP)
- Partner with state Medicaid agency
- If business associate, collaborate with other "business associates"
- Surf the web and network with colleagues & competitors
- Above all maintain a sense of humor!

Resources

- **HHS HIPAA Web Site: http://aspe.hhs.gov/admnsimp**
- **National Institute of Health (regulatory information): http://list.nih.gov**
- **HealthExec Online (HIPAA): http://www.healthexec.net/index.html**
- **SANS Institute: http://www.sans.org**

Resources

- **Workgroup for Electronic Data Interchange: http://www.wedi.org**
- **CPRI-Host Resource Center: http://www.cpri-host.org**
- **HIPAA Assessment: http://www.nchica.org/activities/EarlyView/nchicahipaa_earlyview_tool.htm**
- **Thomas Legislative Guide: http://thomas.loc.gov**

Resources

- American Association of Health Plans: http://www.aahp.org
- American Medical Association: http://www.ama-assn.org
- American Hospital Association: http://aha.org
- American Health information Management Association: http://www.ahima.org
- American Health Quality Association: http://www.ahqa.org

Question & Answer

Chris Apgar, CISSP
Data Security & HIPAA Compliance Officer
Providence Health Plan
(503) 574-7927 (voice)
(503) 574-8655 (fax)
apgarc@providence.org

Providence | Health Plans