




# **Analysis of the Final HIPAA Security Rule**



**Sponsored by: HIPAA Summit  
February 18, 2003**



**Chris Apgar, CISSP  
HIPAA Compliance Officer  
Providence Health Plans**

# Key Points

- Where to start
- Objective steps
- Good news
- Resources



# Where To Start

- Data security as a strategic versus tactical objective
- Overcoming the belief that security is another IT initiative
- Problem generally not getting to the top but keeping top management engaged



# Where to Start

- Focus on culture, business process versus technology – change the belief “this is only an IT issue”
- Partner with regulatory, compliance, clinical – generally deep concern felt for privacy of patient/member
- Patience & a sense of humor a must!



# Objective Steps

- Define business objectives & constraints
  - Road map required or “how does security impact me?”
  - Business objectives, constraints helps define required security infrastructure
- Determine Security Scope
  - Due diligence => much broader than HIPAA
- Project management required – success requires proper planning, resources, measurable results, etc.



# Objective Steps

- Beyond the risk assessment
  - Risk assessment/gap analysis paints the picture
  - Business decisions required – not all risks will be mitigated
  - Results will define required scope, plan and resources
- It needs to be sustainable following implementation (and there's a cost)



# Object Steps

- You need to be able to see it
  - On the organizational chart and in knowledgeable staff
  - Simple & current policies & procedures
  - Risk assessment repetition and integration
  - Technology needs to protect, remain flexible
  - In operation security stretches beyond organizational borders



# Objective Steps

- Simple walkabout test
  - What is in plain sight?
  - Passwords on post its under keyboards?
  - Logged in and unattended computers?
  - Easy access to secure areas like the data center?
  - What's in the dumpster?



# Good News

- Often Little/no technology required
- Relatively low budget – high priced consultants not necessarily required
- Rule not proscriptive – security program requirements flexible
- Most “bang for the buck” - can get great results through strong workforce education programs



# 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>
- **Tunitas Group:** <http://www.tunitas.com>



# 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](http://www.nchica.org/activities/EarlyView/nchicahipaa_earlyview_tool.htm)
- **Thomas Legislative Guide:**  
<http://thomas.loc.gov>

# Question & Answer

**Chris Apgar, CISSP**  
**HIPAA Compliance Officer**  
**Providence Health Plan**  
**3601 SW Murray Blvd., Suite 10**  
**Beaverton, OR 97005**  
**(503) 574-7927 (voice)**  
**(503) 574-8655 (fax)**  
**[chris.apgar@providence.org](mailto:chris.apgar@providence.org)**

