Strategies to Comply with the HPAA Privacy Rule Before the HIPAA Security and Enforcement Rules are Final

Presented by:
Steven S. Lazarus, PhD, FHIMSS
Boundary Information Group
(303) 488-9911
sslazarus@aol.com

BOUNDARY INFORMATION GROUP

- Virtual Consortium of health care information systems consulting firms founded in 1995
- Internet-Based
  - Company website: www.boundary.net
  - BIG HIPAA Resources: www.hipaainfo.net
- Senior Consultants with HIPAA Leadership Experience Since 1992
- Clients include:
  - Hospitals and multi-hospital organizations
  - Medical groups
  - Health plans
  - Vendors
  - Third party administrators

Workgroup on Electronic Data Interchange

- Nonprofit Trade Association, founded 1991
- 203 organizational members
  - Consumers, Government, Mixed Payer/Providers, Payers, Providers, Standards Organizations, Vendors
- Named in 1996 HIPAA Legislation as an Advisor to the Secretary of DHHS
- Website: www.wedi.org
- Strategic National Implementation Process (SNIP) - snip.wedi.org
- WEDI Foundation formed in 2001
- Steven Lazarus, WEDI Chair (2001-2002)

1. Enforcement

- The Federal Government has the authority to enforce all laws and regulations
- Assume that there will be Federal enforcement on Privacy on April 14, 2003
- Privacy requires Security
- Many of the press accounts of privacy breeches have been security breeches that disclosed PHI

Privacy Rule, 45 CFR 164.530(c)

- Existing: "A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart."
- Proposed: "A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure

2. Security Strategy

- Prepare HIPAA Security policies and procedures to support the Privacy Compliance activity
- Prepare to train for both security and privacy

Security to Support the Privacy Requirement for Minimum Necessary

- Role-based or user-based access
- Access controls
  - – Unique identifier
  - – Password
  - – Password management
  - – Automatic log-off settings
- Link access authorization to job description
- Terminate access upon workforce termination or change in role

Security to Ensure that System Users are Properly Identified

- Use of strong passwords, biometrics, tokens or other forms of entity identification

Final Thoughts

- Privacy and security fit together. Covered Entities can not comply with privacy without security
- Apply security to all PHI, not just electronic data and its progeny