A SURVEY OF 10 HEALTH SYSTEMS' HIPAA COMPLIANCE STRATEGIES

Presented by:

Margret Amatayakul, RHIA, FHIMSS

Margret\A Consulting, LLC

Steven S. Lazarus, PhD, FHIMSS

Boundary Information Group

BOUNDARY INFORMATION GROUP

BIG
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

Workgroup on Electronic Data Interchange

- Nonprofit Trade Association, founded 1991
- 206 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) - www.wedi.org/snip
- WEDI Foundation formed in 2001
- Steven Lazarus, WEDI Chair

BIG HIPAA ASSESSMENT PROCESS

- **Interviews**
  - **Individuals & groups - all workforce members**
  - **Purpose:**
    - Ensure awareness
    - Respond to questions/concerns
    - Obtain information about current practices
    - Learn about future plans
- **Observations**
  - **Tour data center(s), file area(s), and key areas where transactions and individually identifiable health information used/disclosed**
  - **Purpose:**
    - Validate policy and procedure
    - Assess overall workflow
    - Establish context within which to make recommendations

BIG HIPAA ASSESSMENT PROCESS

- **Limited testing for privacy and security**
  - **Impersonation w/case studies to determine:**
    - Help desk response
    - Release of information response
  - **Shoulder surfing**
  - **Various logs and records reviewed**
  - **Key door locks tested**
  - **Check paper waste in trash bins**
  - **Third party authorization**
  - **Test workstations for:**
    - Location
    - Password
    - Virus protection
    - Internet use, screen savers, etc.

BIG HIPAA ASSESSMENT PROCESS

- Document review
  - Comprehensive review of policies, procedures, forms, agreements, etc.
    - Determine existence
    - Determine revision date
    - Determine internal consistency
    - Compare to HIPAA standards
- Comparison to industry practice
  - Results of readiness assessment are compared with findings from consultants' pool of other covered entities: 2000 - current

DISCLAIMER

- None of the findings described herein should be attributed to any one specific BIG client or to or all BIG clients.
- These findings are representative of those commonly found in 2000-2002.

TRANSACTIONS FINDINGS

- Significant reliance on and belief in vendor/clearinghouse to solve the problem.
- Focus primarily on 837 (claim) and 835 (remittance) to *preserve* cash flow
- Significantly less focus on other transactions that would *improve* cash flow; little C/B analysis
- Primary focus is IT and not applications:
  - Which are source for data content
  - Which will require significant work flow changes
- Some reluctance to file an extension; lack of understanding concerning DSMO modification delay impact

COMMON SECURITY FINDINGS

- Information Access Control (§142.308(a)(5))
- Technical Access Control (§142.308(c)(1) (i))
  - Who authorizes access to information?
  - How is access established?
  - When is access modified?
  - Is there emergency mode access?
  - On what is access based?
- Common Findings
  - IS assigns network access
  - Mix of formal (supervisor) authorization and less formal verification approaches used for applications
  - Access modification (when workforce members change jobs) often not performed
  - Minimal role-based access is most common; user-based for physicians (and no “break glass” access)

COMMON SECURITY FINDINGS

- **Entity Authentication (§142.308(c)(1) (v))**
  - **Is there automatic logoff?**
  - **Is there two-tiered authentication?**
- **Common Findings**
  - **Automatic logoff is generally in use, though often set for fairly long time in clinical areas**
  - **UserID and password most common**
    - Virtually no training on strong password selection
    - Multiple passwords for applications; virtually no single sign on
    - Often too frequent password change or no password change
    - Often weakest passwords and no change for network access

COMMON SECURITY FINDINGS

- **Security Incident Procedures (§142.308(a)(9))**
  - **Is there a central place to report security incidents?**
  - **Is it used?**
  - **Written policy, training?**
- **Common Findings**
  - **Several places to report** *information security* **incidents**
    - Help desk
    - Security Officer
    - Compliance Officer
    - Supervisor
    - (Often not risk management)
  - **No written policy**
  - **No training**
  - **No incident tracking, trending, or monitoring**

COMMON SECURITY FINDINGS

- Termination Procedures (§142.308 (a)(11))
  - How are workforce user accounts removed?
  - Is there continuity of confidentiality requirement?
- Common Findings
  - Employment Exit check lists often not used
  - No or ineffective communication between Human Resources and I.S.
  - Check list and notification process not automated
  - Best for involuntary terminations
  - Often months to remove voluntary and contractor terminations
  - Rarely exit interview includes:
    - Reaffirmation of confidentiality agreement
    - Solicitation of security issues

COMMON SECURITY FINDINGS

- Media Controls (§142.308(b)(2))
  - Are all systems backed up? Where are backups stored?
  - How is confidential paper handled? trash handled?
  - Is fax receipt verified?
- Common Findings
  - Often only some systems are backed up
  - Usually critical system backups are stored off site; some backups stored in (removable) fireproof box on site, or even “laying around” server
  - “Bee Alert” system in a few locations; most everyone has addressed white boards, marquees, and sign-ins
  - Very good PHI trash control in California, lax in other areas
  - Fax machine acknowledgement ■ recipient verification
  - One fax best practice: return cover sheet to acknowledge receipt

COMMON PRIVACY FINDINGS

- **Sanctions (§164.530(e)(1))**
  - **Are workforce sanctions for breaches applied fairly and consistently?**
  - **Are they documented?**
- **Common Findings**
  - **“Subject to disciplinary action, up to and including termination” standard statement**
  - **Escalation more common than zero tolerance**
    - Usually no specific escalation procedures documented
  - **In hospitals, sanctions process is different for physicians than for the rest of the workforce**
  - **Volunteers are usually subject to the same sanction as employees**

COMMON PRIVACY FINDINGS

- **Individual Rights (§164.520 - .528)**
  - **Are individual rights afforded today?**
  - **How are individuals informed of their rights?**
  - **Is there documentary evidence of due process?**
  - **What technical measures support privacy rights?**
- **Common Findings**
  - (.520) No one has instituted Notice of Privacy Practices (Patients Rights and Responsibilities Notice)
  - (.522(a)) Restrictions not well-accommodated in systems
  - (.522(b)) Confidential communications (not well understood) and not well-accommodated in systems
  - (.524) Access is most commonly granted right (although somewhat begrudgingly); but no policy on or due process for denial
  - (.526) Amendment is occasionally granted; but no policy on or due process for denial
  - (.528) Accounting for disclosure is least common

COMMON PRIVACY FINDINGS

- Consent (§164.506)
- Authorization (§164.508)
- Opportunity to Agree/Object (§164.510)
- Uses & Disclosures Not Requiring (§164.512)
  - Are these documents consistent with HIPAA?
  - Do individuals understand these documents?
- Common Findings
  - Virtually everyone has a consent, though generally for release of information for payment
  - Virtually everyone has authorization forms and policies/procedures when authorization is not required
  - Virtually no one gives patients opportunity to object

COMMON PRIVACY FINDINGS

- Minimum Necessary (§164.502(b))
  - Is PHI limited to intended purpose?
- Common Findings
  - Most still are confused as to what this pertains to
  - Few understand how they will carry out minimum necessary

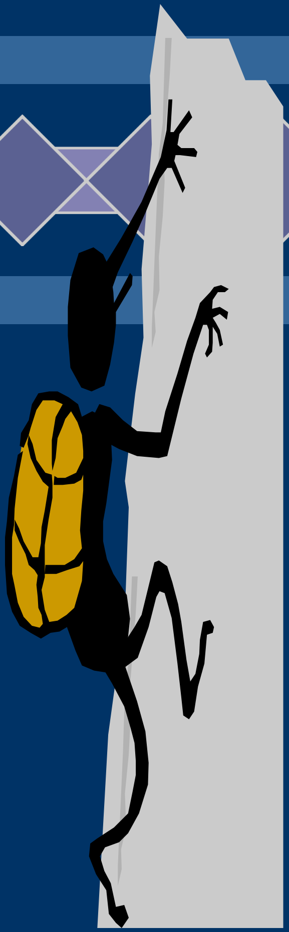
COMMON PRIVACY FINDINGS

- Organizational Relationships (§164.504)
  - Are organizational relationships clear?
  - Are they documented?
- Common Findings
  - Most providers understand they are covered entities
  - Many organizations are confused concerning relationships to other organizations *vis-à-vie* business associates, especially affiliated physician groups

COMMON SECURITY/PRIVACY ADMINISTRATIVE FINDINGS

- Information Security Responsibility (§142.308(b)(1))
- Information Privacy Official (§164.530)
  - Have these been appointed?
  - To whom do they report?
  - Do all members of workforce know who they are?
- Common Findings
  - Appointment and reporting relationship varies
  - Many seem to think they know who they are!
- Training and Awareness
  - Little *information* security training or awareness
  - Good *information privacy* awareness; less training

HIPAA READINESS



Steve Lazarus
sslazarus@aol.com
303-488-9911

Margret Amatayakul
margretcpr@aol.com
847-895-3386