How to Perform a Large Scale HIPAA Security Gap Analysis as a Means of Performance Improvement

Roy G. Clay III, BSCS, CDP

HIPAA Security Project Coordinator

Louisiana State University Health Sciences Center

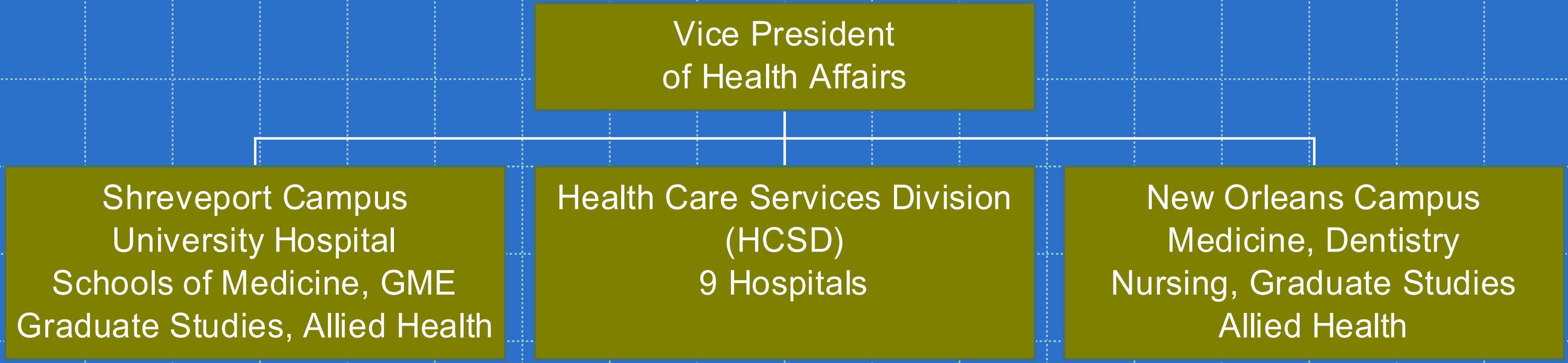
New Orleans, LA

rclay1@lsuhsc.edu

Louisiana State University A Hybrid Entity

- Covered Component
  - Health Sciences Center
  - Pennington Biomedical Research Center
  - Definity Health Plan
- Non-Covered Component
  - Agricultural & Mechanical College
  - Law School
  - Agricultural Center
  - LSU at Eunice
  - LSU at Alexandria
  - LSU at Shreveport
  - University of New Orleans

LSU Health Sciences Center



Vice President
of Health Affairs

Shreveport Campus
University Hospital
Schools of Medicine, GME
Graduate Studies, Allied Health

Health Care Services Division
(HCSD)
9 Hospitals

New Orleans Campus
Medicine, Dentistry
Nursing, Graduate Studies
Allied Health

Health Care Services Division (Large Scale)

- 5000+ Inpatient Admissions/mo.
- 30000+ Outpatient visits/mo.
- 600+ Deliveries/mo.
- 1,000,000 Lab tests/mo.
- 14,000 Prescriptions filled/mo.
- 3000+ Surgical Procedures/mo.
- 28000 ED visits/mo.
- 32,000+ Diagnostic Radiology procedures/mo.
- 2000+ Medical Staff members
- 10000+ Employees

Challenges

- Large multi-entity organization.
- Distributed authority.
- Heterogeneous infrastructure.
- Budget. (What budget?)
- Poor organizational communication.
- Lack of computer literacy.
- Good practices in some areas but other areas overlooked.
- Little (if any) documentation.

Gap Analysis Process

- Appoint Security Officer and Give Him the Authority to Perform the Gap Analysis.
- Iterative Discovery Process.
- Compile Results and Make Recommendations.

Educate Your New Security Officer

- Security NPRM - http://aspe.hhs.gov/admnsimp/bannerps.htm#security
- AAMC Guidelines - http://www.aamc.org/members/gir/gasp/hipaaresources.htm
- WEDI SNIP Whitepapers - http://snip.wedi.org/public/articles/index.cfm?Cat=17

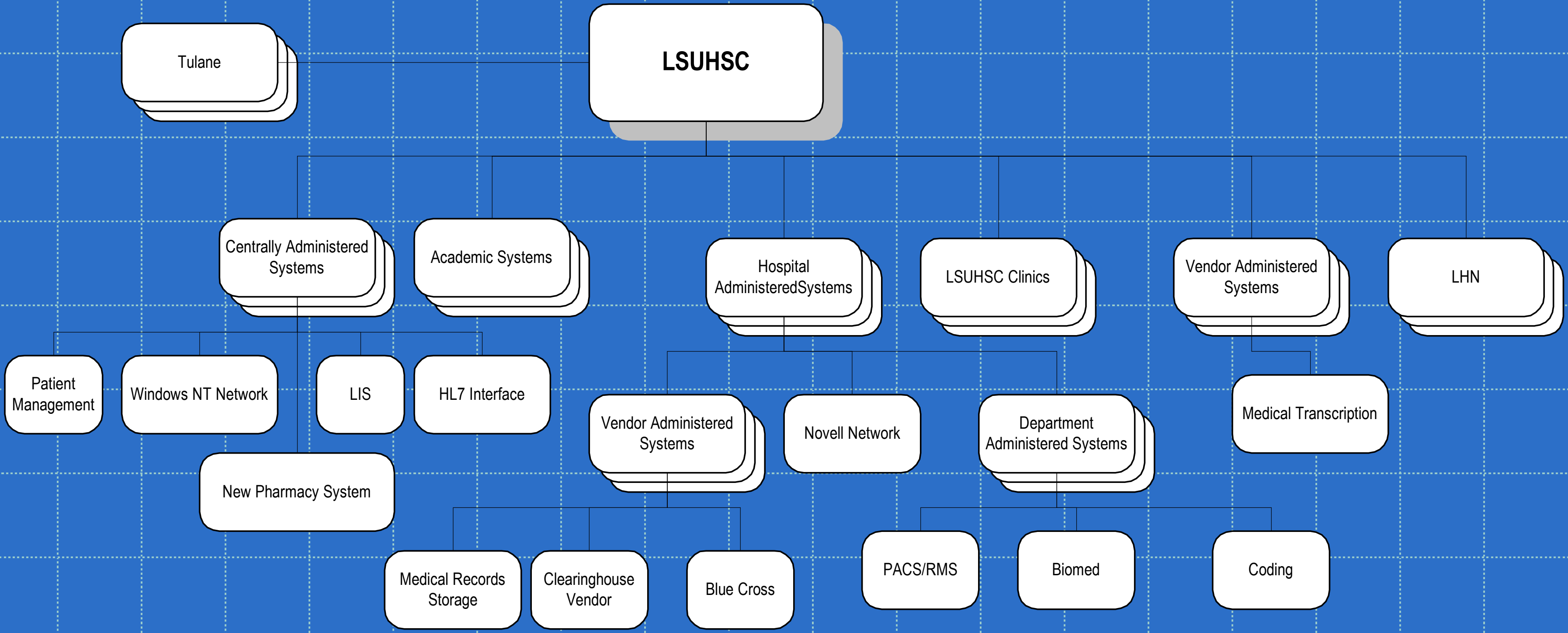
Iterative Discovery Process

- Where is the data?
- Surveys.
- Interviews.

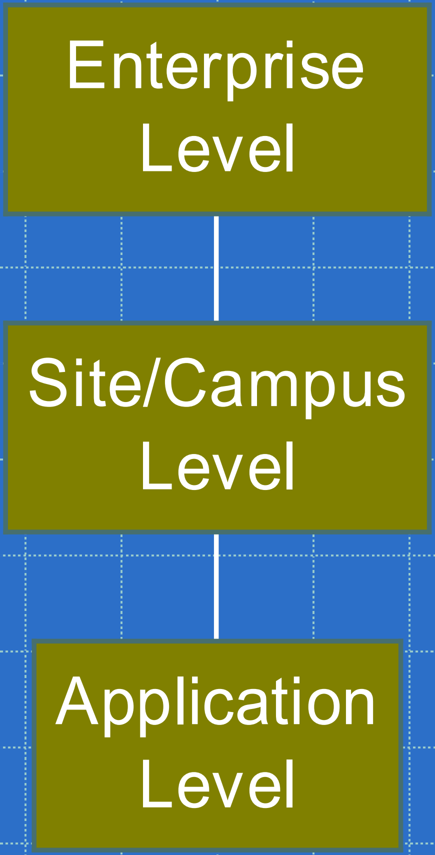
Where is the Data?

LSUHSC HCSD HIPAA Gap Analysis Project

Application Administration
August 8, 2001



Top Down Surveys



Enterprise Level

Site/Campus Level

Application Level

Interviews

- Five Targeted Groups
  - Executive Staff (Including Medical)
  - Human Resources
  - Training
  - Information Technology
  - System Users
- Use responses from surveys to guide your interviews.

Results and Recommendations

- Don’t wait to complete your surveys and interviews to begin compiling recommendations.
- Provide management with alternatives wherever possible.
- Make sure your recommendations are supported by your results.

Remember

- Be prepared to go over things again and again.
- Plan for items to be late.
- Know how to escalate.
- Make every step educate as well as collect information.

Caveat Emptor!

- “20% of HIPAA attorneys are passing incorrect information to their clients.” – *Alan Mertz, Executive Vice-President, Healthcare Leadership Council*
- HIPAA is new. Most of the consultants got to be experts on HIPAA by reading about it.
- Vendors probably know less about HIPAA Security than you do.

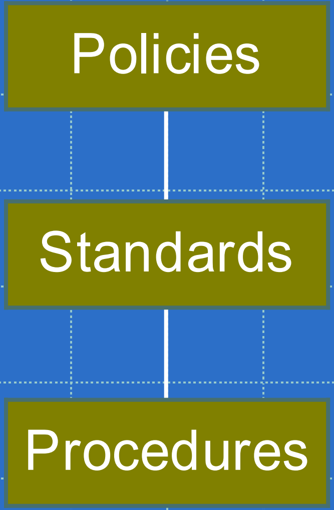
Performance Improvement

- Security Management Process
- Policies, Standards, and Procedures (PSP Not P&P)
- Change Management
- Measurements

Security Management Process

- Include other areas essential to the security process. (Facilities, Hospital Police, etc.)
- This group is the primary security policy making body.
- Recommends security projects to be included in overall project list.

Policies, Standards, and Procedures



Policies

Standards

Procedures

Policies, Standards, and Procedures

- Policies are developed from the security management process.
- Policies should be simple and concise.
- Standards are set and revised by the appropriate group (usually IT) as specified in the policy.
- Procedures are developed to meet the requirements of policies and standards as needed.
- http://www.iso-17799.com/iso.htm

Standards

- As few as possible but sufficient to cover all situations.
- Must be written.
- All projects, grants, construction, etc. must be checked for adherence to standards.

Change Management

- Communications Tool.
- Automate workstation patches.
- Keep logbooks on servers.
- Use request form to initiate and track changes.

Measurements

- Identify and track critical statistics.
- Make sure your measurements make sense from the users’ perspective.
- Scan your network.

Finally

- Gap analysis provides a database than can be mined for performance improvement.