3.03 HIPAA Privacy: Practical Approaches and Experiences for Auditing for Privacy Compliance

Marcia Gonzales, JD

Compliance Officer & Privacy Officer

Indiana University School of Medicine

Office of Compliance Services

INDIANA
UNIVERSITY
SCHOOL OF
MEDICINE

- IUSM is the second largest medical school
- Only School of Medicine in Indiana with 9 sites
- Indianapolis is main campus
- MD students - 1,128
- Number of residents/fellows - 1,032
- Full-time faculty - 1,221
- Staff - 2,642
- 5 hospitals at Indianapolis campus

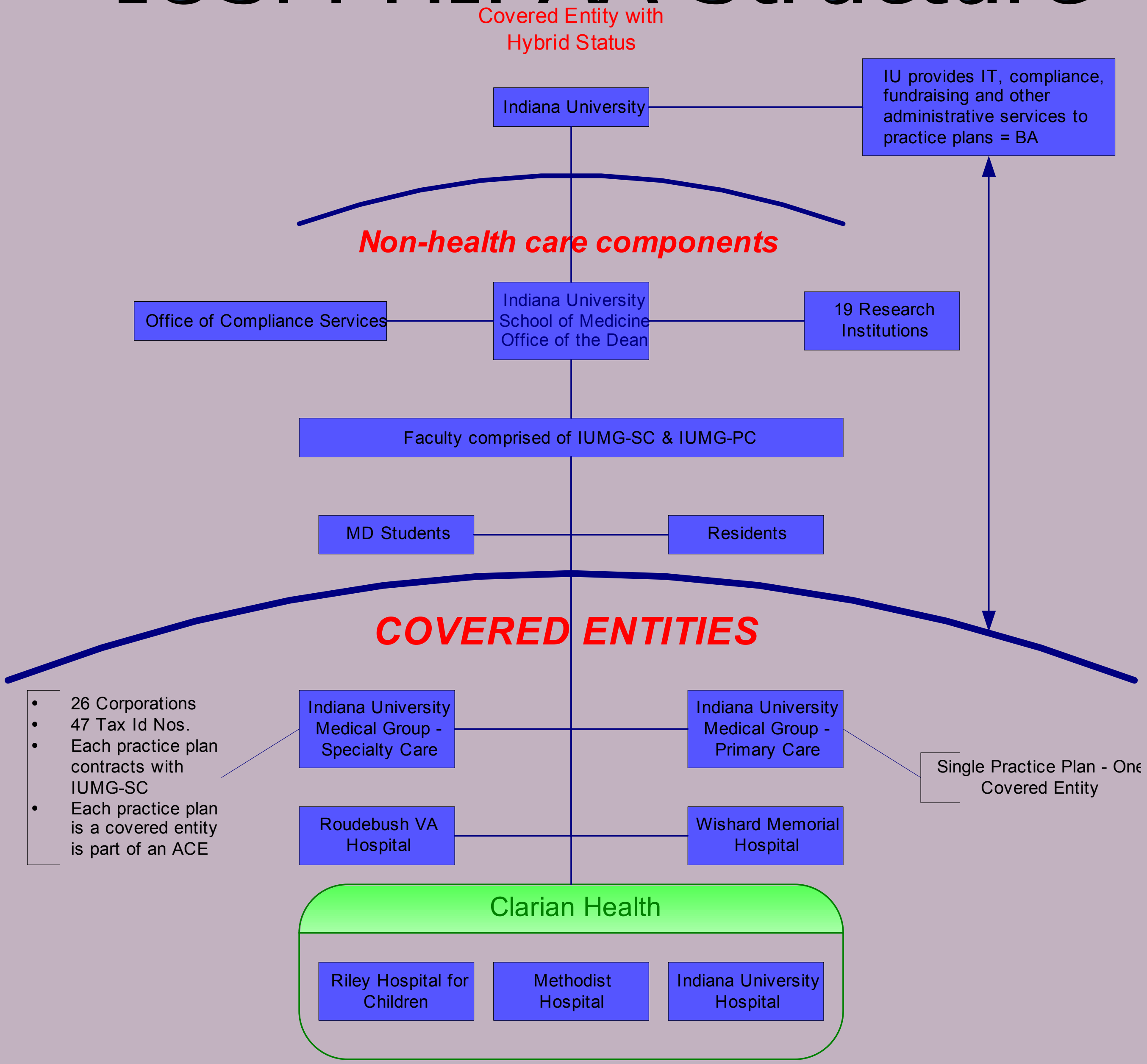
IUSM Research

- 19 Research Institutions
  - Some are not covered entities
- 5 IRBs through the Indiana University Purdue University Indianapolis (IUPUI) and Clarian federal wide assurance
- Fiscal Year 2002- 2003
  - Grants awarded - $186,974,090
  - Awarded research studies - 1,076

Specific Areas to Consider

- Fundraising
  - Source of their potential or current donor lists
  - Relationships with health care providers
  - Specific guidelines developed
- Education
  - Type of access is provided for educational purposes ?(beyond usual education of Medical Students & Residents)
  - Who provides the access?

IUSM HIPAA Structure



Covered Entity with Hybrid Status

Indiana University

IU provides IT, compliance, fundraising and other administrative services to practice plans = BA

Non-health care components

Office of Compliance Services

Indiana University School of Medicine Office of the Dean

19 Research Institutions

Faculty comprised of IUMG-SC & IUMG-PC

MD Students

Residents

COVERED ENTITIES

- 26 Corporations
- 47 Tax Id Nos.
- Each practice plan contracts with IUMG-SC
- Each practice plan is a covered entity is part of an ACE

Indiana University Medical Group - Specialty Care

Indiana University Medical Group - Primary Care

Single Practice Plan - One Covered Entity

Roudebush VA Hospital

Wishard Memorial Hospital

Clarian Health

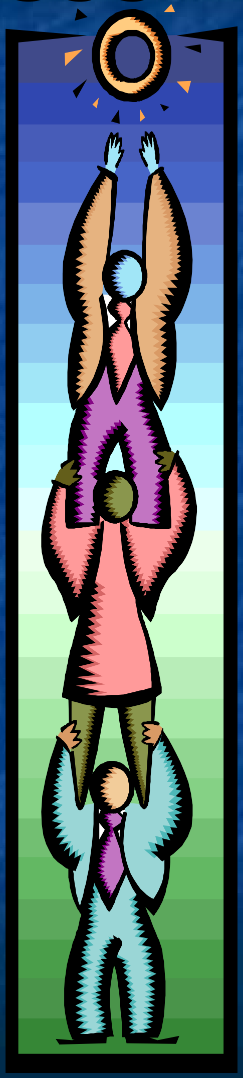
Riley Hospital for Children

Methodist Hospital

Indiana University Hospital

HIPAA Implementation Process

- IUSM HIPAA Compliance Plan
  - IUSM is not a health care component of Indiana University
  - Business associate to Physician Practices and Hospitals
  - Faculty - workforce members of several covered entities
- Access to education for faculty, residents, students and staff
- Physician Practice Plan Workplan
  - Step by step approach to implementation & tracking milestones
  - Met with Practice Plan administrators every 2 weeks for 6 months
  - Results of Workplan status reported to Deans



Practice Workplan

LEGEND:

IP - In Progress

C - Completed

O - Overdue

NS - Not Started

REFERENCE TOOLS:

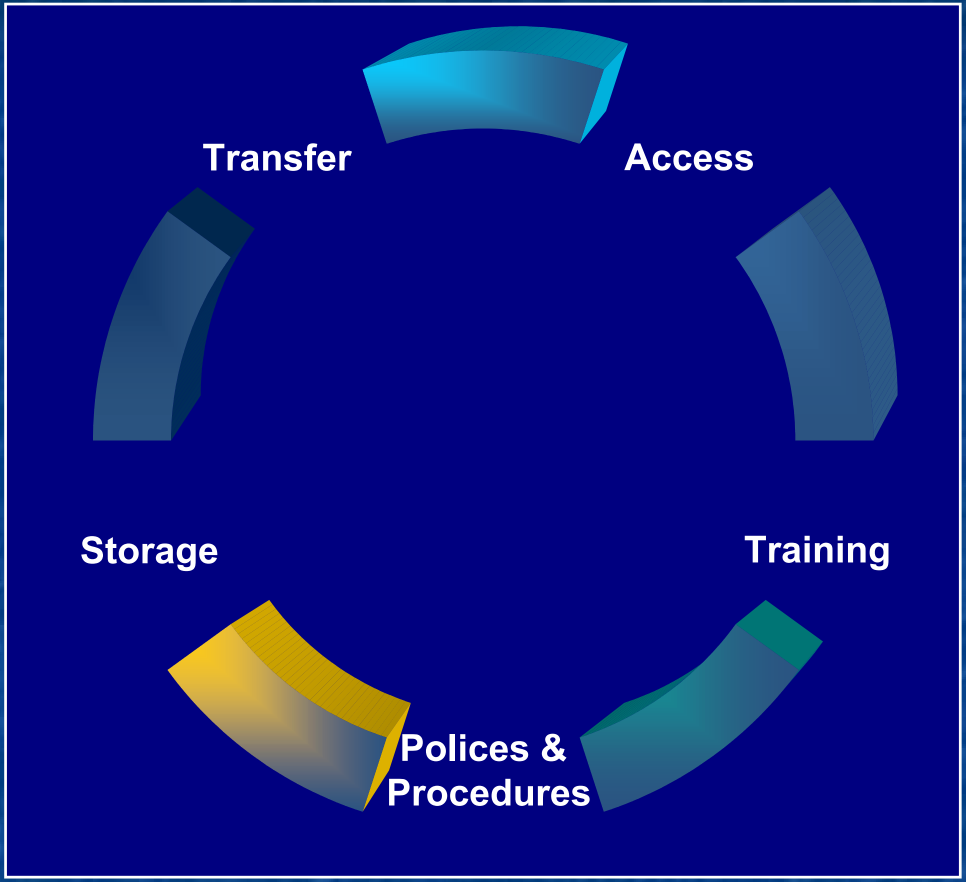
Attachment B - HIPAA Roles & Responsibilities - ***Approved by Compliance Committee, and provided by IUSM Office of Compliance Services (OCS)***

Attachment D - HIPAA Key Terms

Attachment J - Policies and Procedures Resource Documents

Tasks	Position Responsible	Status	Start Date	Due Date	Completion Date	Issues / Barriers
Conduct Assessment	*PPHL*					
Evaluate how your organization measures up to HIPAA regulations using the selected assessment tool (Answer and document responses to each survey question or criteria in the selected tool or check list)	*PPHL*					
Document privacy and security gaps in compliance and the areas that need to be addressed to comply with HIPAA	*PPHL*					
Evaluate level of non-compliance, sensitivity and risk of each compliance gap	*PPHL*					

Measuring Compliance



Transfer

Access

Storage

Training

Polices &
Procedures

Did we do what we said we were going to do?

Measuring Compliance -STAT

- **Storage**
  - Where is PHI stored? For what purpose?
  - Is PHI sufficiently safeguarded?
- **Transfer**
  - When is PHI being sent electronically?
  - Is the transfer reasonably safeguarded?
- **Access**
  - How is this determined?
  - Is legitimate access being denied?
- **Training**
  - Have employees been trained?
  - What process is in place to train new employees or to communicate changes in policy?

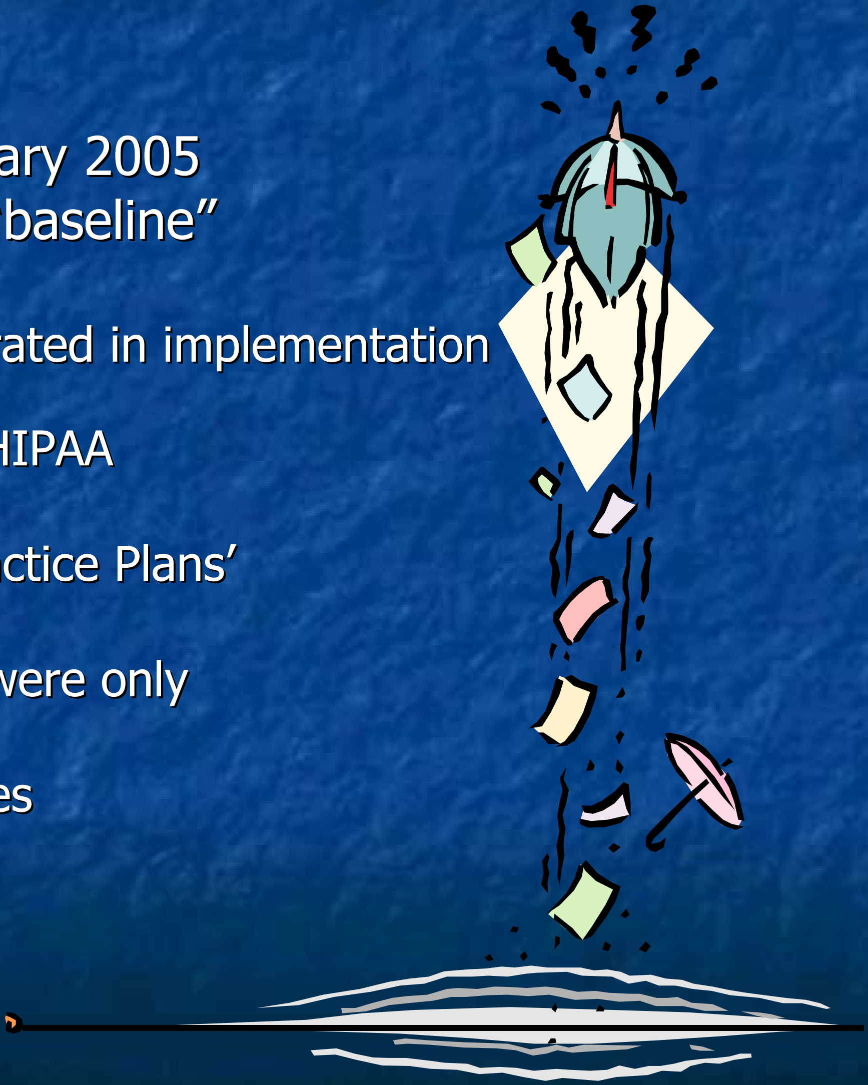
Polices & Procedures

- Uses and disclosures of Protected Health Information (PHI)
- Minimum Necessary
- Decedents
- Fundraising
- Marketing
- Authorizations
- Patient Rights
- Personal Representatives and Others involved in a Patient’s Care

- Verifying the Identity and Authority of a Person requesting PHI
- De-Identified Data
- Limited Data Sets
- Business Associates
- Complaints
- HIPAA Documentation
- Training
- Safeguards
- Notice of Privacy Practices
- Changes in Law

IUSM Privacy Audit Strategy

- Will begin Privacy Audits in January 2005
- Initial audit will be treated as a "baseline"
- General Purpose
  - Compliance with HIPAA incorporated in implementation documents
  - Test the effectiveness of IUSM HIPAA Compliance Plan
  - Test the effectiveness of the Practice Plans' HIPAA Compliance Plan
  - Determine if the Practice Plans were only "going through the motions", i.e., do the policies and processes address their specific issues.



Privacy Audit Strategy

- Initially, will audit all departments
  - 12 month process
  - Prior Written notice of the Audit will be provided to the practice plans/departments
  - Will ask each department to submit copy of Policies & Procedures prior to audit
  - Will use developed checklists
- Subsequent audits will be determined on a risk basis or done randomly.

Item	IUSM HIPAA Policy #	Requirement	Interview Question	Risk Value	Compliant	Needs Improvement	Non-Compliant
Part 164, Subpart E - Privacy of Individually Identifiable Information							
§164.502		***Uses and disclosures of protected health information: general rules***					
1	IUSM - HIPAA Privacy 1.0	**Permitted uses and disclosures - §164.502(a)(1) and 164.506.** A Covered Entity may not use and disclose except as permitted or required. Covered entities may use and disclose PHI for treatment, payment and healthcare operations.	Do you have a documented policy and procedure that explains the uses and disclosures of PHI permitted under HIPAA?	1			
2	IUSM - HIPAA Privacy 16.0	**Incidental Disclosures - §164.502(a)(1)(iii)** Incidental disclosures permitted as long as the Covered Entity has complied with Minimum Necessary and used reasonable safeguards.	Do you have a documented policy and procedure regarding Incidental Disclosures that are permitted under HIPAA? Do Associates understand the difference between an "incidental" disclosure and those that are not permitted?	1			
3	IUSM - HIPAA Privacy 2.0	**Minimum Necessary - §164.502(b) and 164.514(d)** Limit the amount of data to the minimum needed for a particular purpose	Do you have documented policies and procedures that address the minimum amount of PHI needed for routine and recurring uses and disclosures: (NOTE: The practice plan should have procedures that explain the amount of PHI needed for common operational and payment processes - e.g. patient registration, handling requests for information/records, billing, etc.) - Have you identified routine and recurring uses and disclosures of PHI? - Have you defined the minimum amount of PHI needed for these routine and recurring uses and disclosures? - Have you trained Associates on these policies and procedures as it relates to their job functions - i.e. operational-level training? NOTE: General awareness training does not provide sufficient detail for explaining the amount of PHI that is appropriate for a worker to perform their job.	3			

Privacy Audit Strategy

- Walk through audit
    - What would a patient or visitor see or hear?
- Evaluation of written policies and current processes
    - Compliance with IUSM policies
    - Compliance with core requirements
        - Notice of Privacy Practices (NPP)
        - Authorizations
        - Disclosures
        - Accounting for Disclosures
        - Complaint Process
- Employee Interviews
    - Was the employee trained?
    - What is the employee's understanding of HIPAA?
    - Does the employee understand his/her responsibilities?
    - Does the employee know how to report any concerns involving privacy breaches?

IUSM Privacy Audit Strategy – Who's on First?

- Factors to consider:
  - Size of department
    - number of employees
    - Number of practice sites
  - Department location – open or shared areas vs. private or more secure locations
  - Sensitivity of PHI typically handled, i.e., psychotherapy notes, communicable diseases etc.

- Prior Training
- Availability of internal resources
- Existence of any prior complaints
- Compliance with HIPAA Privacy Workplan initiatives
- Human Subject Research
  - Number of studies
  - Type of studies
  - Number of databases kept

Research Audit Game Plan

IUPUI Research & Sponsored Programs will audit compliance with

- Research SOPs developed to address HIPAA Privacy
- Informed Consent and Authorization requirements
- Data Use Agreements
- Recruitment Strategies – compliance with recruitment checklists
- Representation made in
  - IRB applications
  - Summary Safeguards

Item	SOP Section	Requirement	Interview Question	Risk Value	Compliant	Needs Improvement	Non-Compliant
1	SOP - 5.5	**§164.514 Use of de-identified data for research**	Do the reviewed studies involve de-identified health information? If so, which de-identification method was used - Safe Harbor or statistical? - If Safe Harbor, were all 18 identifiers removed? *(See 5.5.2 in the SOP for details.)* - If Statistical, did someone with statistical expertise made this determination? Who? What methodology was used (e.g. what confidence interval) and was this documented? Are re-identification codes used? If so, how are they protected? Are re-identification codes ever stored with the de-identified data or given to a third party?	3			
2	SOP - 5.6	**§164.514(e) Research using limited data sets for research**	Do any of the sampled studies involve a Limited Data Set? If so, was a Data Use Agreement obtained with the recipient? Review sample of data and determine whether all direct identifiers were removed. *(See Section 5.6.1 in the SOP for details.)*	3			
3	SOP - 5.7	**§164.512(i) Authorizations**	How/when do you obtain an authorization from a subject? (Have PI describe at what point they obtain an individual's authorization for the studies you are reviewing.) Has a subject ever refused to sign or asked you to change the authorization? How do you handle these situations? Has a subject ever revoked an authorization? If so, how did you handle and document the request? How/where are authorizations stored? Auditor Notes: Review the Summary Safeguard Statement and recruitment checklist to determine whether an authorization is required for recruitment and enrollment into the study. Does the authorization contain all the required elements? *(See Section 5.7.1 of the SOP for details.*)	3			

Audit Expectations

- Mutual educational opportunity
- Initial Goals
  - Identify areas of vulnerability
  - Determine where areas of assistance are most needed, if additional education is required
  - Provide a forum and opportunity for departments/practices to clarify issues
  - Identify specific areas where targeted training is needed
  - Determine if there are any systemic issues across all practice plans
  - Prepare report for each department and for the IUSM
  - Review findings against Risk Assessment done for Security