Privacy and Security in the Roman Empire:

One Hospital's Experience with a "Do It Yourself" HIPAA Plan

Melissa Cornwell
HIPAA Coordinator/Privacy Officer
Floyd Medical Center
Rome, Georgia

What is the Roman Empire?

- Rome, Georgia
- 65 Miles NW of Atlanta, GA
- 65 Miles SW of Chattanooga, TN
- 135 Miles E of Birmingham, AL

What is the Roman Empire?

- Rome is the county seat of Floyd County, GA
- Rome's Land Area = 22 Square Miles
- Rome's Population = 34,980
- Floyd County Population = 90,565

THE FORUM

A Civic Center Complex

Rome's Health Care Assets

- Rated #1 in health care out of 193 small cities in the United States, Rome is home to more physicians per capita than any other city in Georgia. We serve as a health care center for a regional population of over 500,000 people (17 North Georgia counties).

Rome's Health Care Assets

Two Hospitals:

- Floyd Medical Center
  - 304-Bed, Acute Care Hospital
  - Sole Inpatient Provider of Women's and Children's Services in Floyd County (maternity, NICU, newborn nursery, & pediatrics)
  - Emergency Services
  - Designated Trauma/Intensive Care/Coronary Care
  - Full Medical/Surgical Services
  - Inpatient Rehabilitation Unit
- 201-Bed Acute Care Facility (HCA-owned)
  - General Acute and Intensive Care Services
  - Open Heart Surgery Referrals for NW GA

FMC as a “Covered Entity”

- Floyd Medical Center
- Floyd Home Health Agency
- Community HospiceCare
- Centrex Primary Care Network (19 Primary Care & 4 Urgent Care Offices)
- Floyd Outpatient Rehabilitation Center
- Health@work Occupational Health Services
- Windwood Psychiatric Hospital
- Floyd Health Care Foundation
- FMC’s Self-Insured Employee Health Plan

FMC's "First Steps for HIPAA"

- Prior to the summer of 2001, two groups within our organization led efforts toward HIPAA compliance:
  - Following a JCAHO survey in November 2000, the Accreditation Compliance Committee met semi-monthly to discuss privacy-related issues in preparation for a coordinated HIPAA compliance effort
  - Nursing Informatics led a separate effort toward compliance for the Security Rule and Transactions and Code Sets (TCS) Rule

HIPAA Project Management Office

- **Project Manager:**
  - Thirty-year veteran of our workforce
  - Past Director of Medical Records, past Director of Human Resources, and most recently, Senior Director, Case Management/Quality, and Healthcare Consultant
- **Project Coordinator/Privacy Officer**
  - Previous experience with federal regulations (i.e., HCFA, CARF, Corporate Compliance); policy and procedure development, medical office operations

- **Started with 1 FTE in November 2001; increased to 1.5 FTE's in June this year**

First Tasks

- Read the Regulations
  - http://aspe.os.dhhs.gov/admnsimp/
  - Downloaded regs in HTML format
  - Copied and pasted into MS Word documents
  - Searchable; original formatting preserved
- Subscribed to HIPAA-REGS list for updates
- Identified appropriate and legitimate HIPAA conferences, seminars, and web resources
- Participated in VHA Georgia Compliance/ HIPAA Council meetings

Identifying Resources

BEWARE OF INFORMATION GLUT

FMC's Top Web Resources

- www.hipaadvisory.com
  - Phoenix Health (VHA) site
- www.cpri-host.org/resource/toolkit/toolkit.html
  - Computer-based Patient Record Institute
- http://www.healthlinknm.org/nmchili/
  - New Mexico Coalition for Healthcare Information Leadership Initiatives
- www.clients1.kslaw.com
  - King & Spalding subscription website (Offers Georgia pre-emption information)
- For more information than you will ever need, go to:
  http://pweb.netcom.com/~ottx4/HIPAA.htm

7 Steps to HIPAA Compliance*

1. Project preparation
2. Develop educational processes:
   - General workforce training
   - Education re: HIPAA-compliant P&P's
   - Job-specific training
3. Assess current practices & subsequent gap analysis
4. Identification of Business Associates; contract revision/creation
5. Identification of legal issues and solutions
6. Development of ongoing monitoring/auditing tools
7. Gap closure/implementation

*Adapted from "Hands-On HIPAA: Developing Your HIPAA Implementation Plan" audio conference, copyright Phoenix Healthcare, 2001

Step 1: Project Preparation

- Met with FMC “Sponsors”
  - Senior Vice President
  - Vice President, Corporate Compliance
  - Vice President, Finance
- Selected Privacy Officer
- Selected Security Officer
- Developed Organizational Chart
- Selected HIPAA Compliance Task Force
- Developed Board Resolution

Step 1: Project Preparation

- Selection of Privacy Officer
  - Initially, our Director of HIM bore this role; upon her departure, HIPAA Coordinator became her successor
- Selection of Security Officer
  - Director of Information Systems/Networking
- Job Descriptions: Duties of Privacy Officer and Security Officer were integrated into existing job descriptions

Step 1: Project Preparation

- Identification of Workgroups
  - Privacy (Chaired by Privacy Officer)
  - Security (Chaired by Security Officer)
  - Transactions & Code Sets (Chaired by Director of Patient Financial Services, with strong workgroup representation from Information Systems/Data Processing)
  - Education Workgroup (Chaired by Director of Corporate Education)

Step 1: Project Preparation

- Appointed a Steering Committee, to include:
  - Sponsors
  - HIPAA Project Management Office
  - Privacy Officer
  - Security Officer
  - Vice Presidents for Nursing, Corporate Operations
  - Human Resources Manager
  - Director of Patient Financial Services
  - Director of Corporate Education

Organizational Structure: HIPAA Compliance Team

Corporate Compliance Committee

HIPAA Sponsors
Sonny Rigas, Sr. V.P.
Mary Johnson, V.P.
Rick Sheerin, V.P.

Legal Counsel

HIPAA Steering Committee
Mary Johnson, Diane Davis, Sonny Rigas, Rick Sheerin, Greg Polley, Robbie Lane, Brian Barnette, Deborah Robitaille, Donna Casey, Linda Wilhelm, Valerie Cloud, Melissa Cornwell

Project Management Office
Robbie Lane, Manager
Melissa Cornwell, Coordinator

Transactions/Code Sets/ Identifiers Workgroup
Donna Casey, Chair

- Rick Sheerin, VP/Designee
- Greg Polley, VP/Designee
- IS Shirley Stafford
- IS Leonard Culberson
- IS Louise McKinney
- IS Renee Brooks
- HIM Deborah Robitaille
- Centrex Anita Borders
- Home Care Carol McBurnett
- Hospice Carol McBurnett
- WW Tara Sherman

Privacy Workgroup
Melissa Cornwell, Privacy Officer
Chair

- Diane Davis, VP/Designee
- IS Renee Brooks
- HR Valerie Cloud
- RM Jackie Newby
- PI Debbie Smith
- Accred Winnie Chesley
- Customer Rel. Denise Martin
- Centrex Al Davis, Liz Beacham
- Home Care Deborah Parker
- Hospice Janet Elrod
- FP Vicki Wiles
- WW Janette Barker
- HIM Shelley Anderson

Security Workgroup
Brian Barnette, Security Officer
Chair

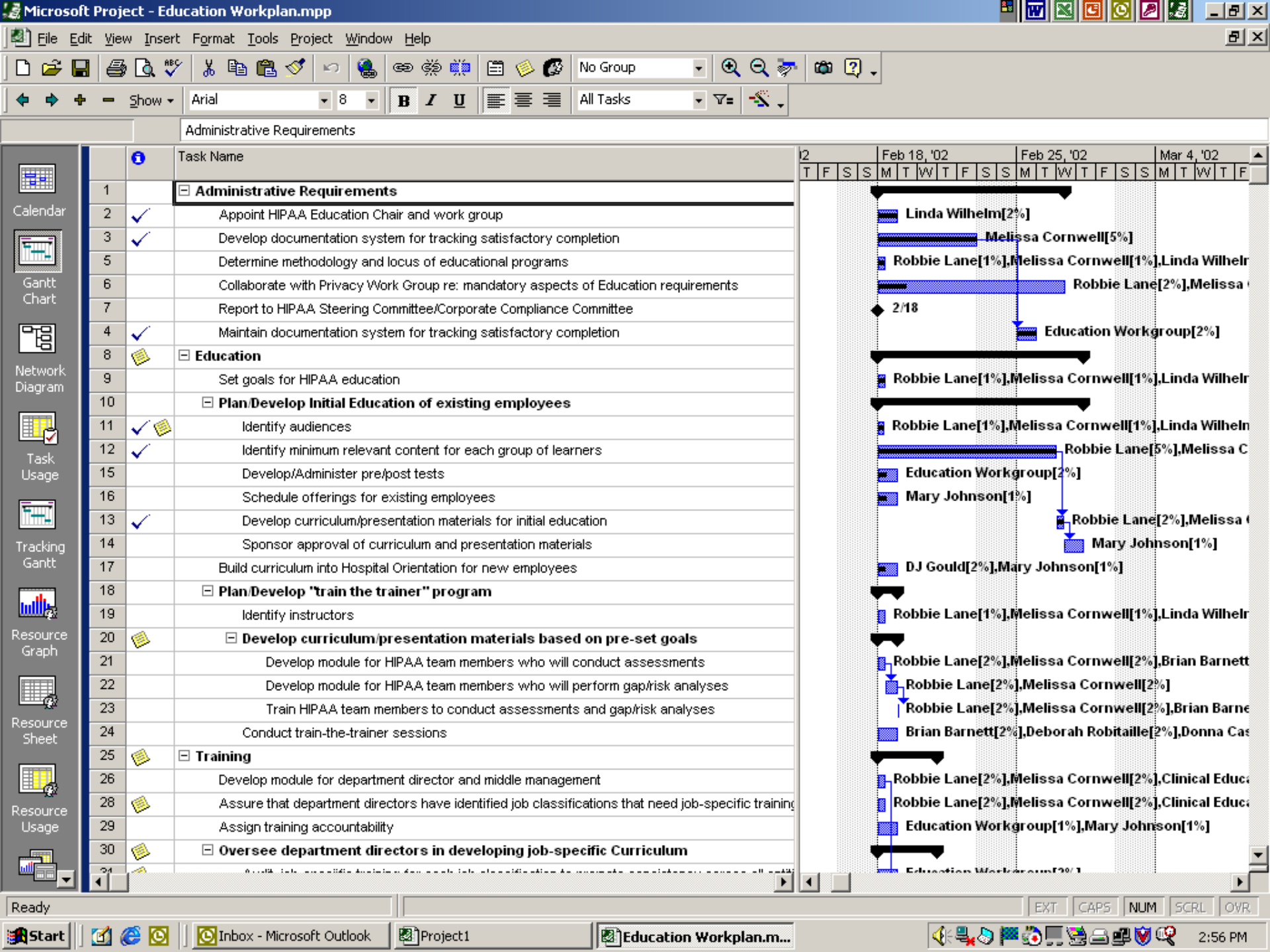
- IS Stacey Cline
- IS Scotty Harper
- Health Plan Rick Tew
- WW John Minshew
- RM Jackie Newby
- PF Dennis Newby
- Sec Richard Bryant
- Centrex - Al Davis

Education Workgroup
Linda Wilhelm, Chair

- Departmental Educators TBD
- Ed Sherry Payne
- PM Haley Crider
- Additional Members TBD

Step 1: Project Preparation

- Concurrent with development of our organizational chart, we planned project oversight using Microsoft Project™
  - Developed an overall HIPAA compliance work plan based on our “7 Steps”
  - Developed separate work plans for each work group
  - Privacy, Security, TCS, and Education work plans were presented only as a suggested framework. Each workgroup is encouraged to use its expertise to mold and perfect the proposed work plan


Microsoft Project - Education Workplan.mpp
File Edit View Insert Format Tools Project Window Help
No Group
Show Arial 8 All Tasks
Administrative Requirements
Calendar
Gantt Chart
Network Diagram
Task Usage
Tracking Gantt
Resource Graph
Resource Sheet
Resource Usage
Task Name
1 Administrative Requirements
2 Appoint HIPAA Education Chair and work group
3 Develop documentation system for tracking satisfactory completion
5 Determine methodology and locus of educational programs
6 Collaborate with Privacy Work Group re: mandatory aspects of Education requirements
7 Report to HIPAA Steering Committee/Corporate Compliance Committee
4 Maintain documentation system for tracking satisfactory completion
8 Education
9 Set goals for HIPAA education
10 Plan/Develop Initial Education of existing employees
11 Identify audiences
12 Identify minimum relevant content for each group of learners
15 Develop/Administer pre/post tests
16 Schedule offerings for existing employees
13 Develop curriculum/presentation materials for initial education
14 Sponsor approval of curriculum and presentation materials
17 Build curriculum into Hospital Orientation for new employees
18 Plan/Develop "train the trainer" program
19 Identify instructors
20 Develop curriculum/presentation materials based on pre-set goals
21 Develop module for HIPAA team members who will conduct assessments
22 Develop module for HIPAA team members who will perform gap/risk analyses
23 Train HIPAA team members to conduct assessments and gap/risk analyses
24 Conduct train-the-trainer sessions
25 Training
26 Develop module for department director and middle management
28 Assure that department directors have identified job classifications that need job-specific training
29 Assign training accountability
30 Oversee department directors in developing job-specific Curriculum
Feb 18, '02
Feb 25, '02
Mar 4, '02
T F S S M T W T F S S M T W T F S S M T W T F
Linda Wilhelm[2%]
Melissa Cornwell[5%]
Robbie Lane[1%],Melissa Cornwell[1%],Linda Wilhelr
Robbie Lane[2%],Melissa
2/18
Education Workgroup[2%]
Robbie Lane[1%],Melissa Cornwell[1%],Linda Wilhelr
Robbie Lane[1%],Melissa Cornwell[1%],Linda Wilhelm
Robbie Lane[5%],Melissa C
Education Workgroup[2%]
Mary Johnson[1%]
Robbie Lane[2%],Melissa
Mary Johnson[1%]
DJ Gould[2%],Mary Johnson[1%]
Robbie Lane[1%],Melissa Cornwell[1%],Linda Wilhelr
Robbie Lane[2%],Melissa Cornwell[2%],Brian Barnett
Robbie Lane[2%],Melissa Cornwell[2%]
Robbie Lane[2%],Melissa Cornwell[2%],Brian Barne
Brian Barnett[2%],Deborah Robitaille[2%],Donna Cas
Robbie Lane[2%],Melissa Cornwell[2%],Clinical Educa
Robbie Lane[2%],Melissa Cornwell[2%],Clinical Educa
Education Workgroup[1%],Mary Johnson[1%]
Ready
EXT CAPS NUM SCRL OVR
Start
Inbox - Microsoft Outlook
Project1
Education Workplan.m...
2:56 PM

Step 2: Develop Educational Processes

- Privacy Rule: § 164.530: “A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.”
- Training must be completed by April 14, 2003
- Training must be job specific
- Must train new employees
- Must tailor training as privacy rules change or are updated

Step 2: Develop Educational Processes

- We developed one master set of “HIPAA Basic Training” slides as an early view of the regulations
- Tailored this set for several specific groups:
  - Board of Directors
  - Operations Council (Leaders with Departmental Budget Responsibilities)
  - Leadership Committee (All Managers and Supervisors)
  - Employees: this version was included as a 15-minute video segment in our annual Corporate Compliance presentation

Step 2: Develop Educational Processes

- The Education Workgroup has designed and implemented general workforce privacy and security training for:
  - New employee orientation
  - Annual employee update
    - Implemented August, 2002
- The Privacy Workgroup is determining job-specific training and training related to unit-specific privacy issues, including oral communications and visitation
    - To be implemented approximately January, 2003

Step 2: Develop Educational Processes

- Key points for general employee education:
  - Why does HIPAA make a difference?
  - The Minimum Necessary Requirement
  - Oral Communications
  - Patient Rights
  - Corporate Policies and Procedures re: privacy and security
  - General Security Issues: Workstation, E-Mail, FAX

Step 3: Assessment and Gap Analysis

- This is where the fun begins!
- How to assess?
- What to assess?
- Who to assess?
- How to document assessments?
- How to standardize results?
- How to measure gaps?

Step 3: Assessment and Gap Analysis

- Jonathan Tomes, JD: *Compliance Guide to HIPAA and the HHS Regulations*
- Provides a comprehensive list of questions for a HIPAA Privacy Assessment
  - Turns the privacy regs into question format
- We expanded upon that idea and framed three master assessments:
  - Privacy
  - Security (based on an AHIMA Model)
  - EDI (based on the regulation text)

Step 3: Assessment and Gap Analysis

- In addition to these rule-specific assessments, we needed an assessment tool that would provide a practical view of current privacy and security practices throughout our organization.

Step 3: Assessment and Gap Analysis

- What do we need to know about our current privacy and security practices that will help us understand our level of compliance with the proposed regulations?
  - Where is protected health information (PHI) entering our systems?
  - Where is PHI exiting our systems?
  - How do our employees use and disclose PHI in their day-to-day work flow?
  - Where is PHI stored?
  - Is stored PHI adequately protected?
  - Who will do the assessments?

Step 3: Assessment and Gap Analysis

- Who will do the assessments?
  - Compliance Team Workgroup members divided into 15 teams of two members each
  - We identified 75 departments requiring assessments
  - Each team was assigned 5 assessments

Step 3: Assessment and Gap Analysis

- Assessment Tool #1 helped us determine:
  - Where is PHI entering our systems?
  - Where is PHI exiting our systems?
  - PHI Mapping Tool

Step 3: Assessment and Gap Analysis

- Assessment Tool #2 provided an answer to the question:
  - What are our current privacy and security practices?
  - Departmental Assessment
  - Results:
    - Any question with an aggregate score of less than 90% was considered an educational opportunity
    - 50% of questions fell into this range
    - Folks know the right answers – they “talk the talk,” but don’t always “walk the walk”

Step 3: Assessment and Gap Analysis

- Filling out Assessment Tool #3 was conditional upon answering the last question on the Departmental Assessment, which was, “Do any members of your department store protected health information in any non-clinical programs, or store any paperwork containing PHI?” (Examples: MS Word, Access, Excel, Outlook, 3M, hard copies of patient charts, charge or encounter forms)
- PHI INVENTORY

Step 3: Assessment and Gap Analysis

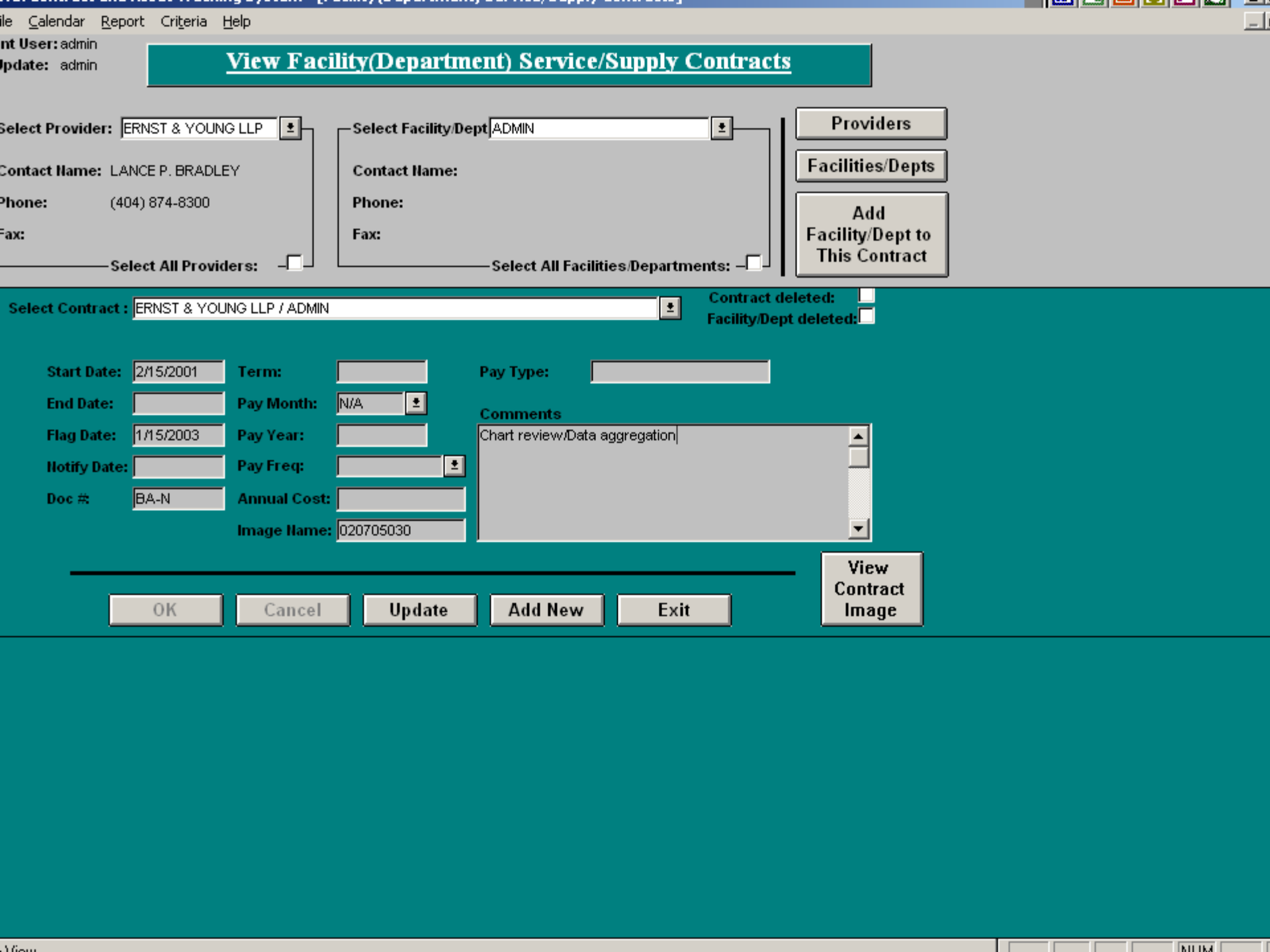
- Following compilation of departmental assessment results, the Privacy and Security Workgroups are completing “master” assessments
- Those results are being used to complete gap analysis tools

Step 3: Assessment and Gap Analysis

- Gaps are identified by green, yellow and red priorities
  - Green = compliant; little or no risk
  - Yellow = partially compliant; moderate risk
  - Red = non-compliant, high-risk
- Privacy Gap Assessment

Step 4: Identification of Business Associates and Contract Development

- As with most organizations, just about every department at FMC “owns” contracts.
- In order to review all existing contracts to analyze the need for Business Associate Agreements, our HIPAA Steering Committee approved the purchase of contract management software which tracks:
  - Vendors & contact information
  - Start, end, and notification dates
- The software flags contracts due for review and/or renegotiation
- Allows us to track BA Agreements


ile Calendar Report Criteria Help
nt User: admin
Update: admin
View Facility(Department) Service/Supply Contracts
Select Provider: ERNST & YOUNG LLP
Contact Name: LANCE P. BRADLEY
Phone: (404) 874-8300
Fax:
Select All Providers:
Select Facility/Dept ADMIN
Contact Name:
Phone:
Fax:
Select All Facilities/Departments:
Providers
Facilities/Depts
Add Facility/Dept to This Contract
Select Contract : ERNST & YOUNG LLP / ADMIN
Contract deleted:
Facility/Dept deleted:
Start Date: 2/15/2001
End Date:
Flag Date: 1/15/2003
Notify Date:
Doc #: BA-N
Term:
Pay Month: N/A
Pay Year:
Pay Freq:
Annual Cost:
Image Name: 020705030
Pay Type:
Comments
Chart review/Data aggregation
OK
Cancel
Update
Add New
Exit
View Contract Image

ile Calendar Report Criteria Help

t Date:

Current User: admin

Date: 8/27/2002

Flagged Contracts Alarm

Number of Flagged Contracts for Physician-Facility/Dpt : 1

Press <Process> to process this category of contracts now.

Press <Next> to go to the next category of contracts.

Press <Exit> to return to the Main Menu.

Process Next Exit

Step 4: Identification of Business Associates and Contract Development

- Our legal counsel has prepared a standard Business Associate Addendum which includes required verbiage not only for HIPAA, but JCAHO and OIG requirements.
- The HIPAA PMO designed a form letter to be included with Business Associate Agreements to introduce the concept to those vendors not aware of the new requirements.
- The letter extends an offer to Business Associates to negotiate certain provisions, but does not guarantee our accommodation

Step 5: Identification of Legal Issues and Solutions

- What is our status as a “Covered Entity”?
  - Single Covered Entity
  - Hybrid Entity
  - Affiliated Covered Entity
- Review of required documents:
  - Business Associate Agreements
  - Trading Partner Agreements
  - Limited Data Set Agreements
  - Required forms (authorizations, consents)
  - Policies and Procedures

Step 5: Identification of Legal Issues and Solutions

- How will we establish our Organized Health Care Arrangement?
  - Revision of Medical Staff Bylaws/Rules and Regulations
  - Creation of OHCA partnerships with other covered entities with whom we share PHI (MRI facility, angioplasty, etc.)

Step 5: Identification of Legal Issues and Solutions

- Issues for consideration for an OHCA*:
  - Amend staff bylaws to make participation in the OHCA an essential requirement to join or stay on the medical staff
  - Each medical staff member formally agrees to abide by the terms of the notice "with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement." [164.520(d)(1)]

* Issues are adapted from a list compiled by David Hainlain, Citrus Memorial Hospital, and posted in Phoenix Healthcare's HIPAA electronic mail exchange, "HIPAAlive"

Step 5: Identification of Legal Issues and Solutions

- The OHCA adopts a single NPP to cover use and disclosure of PHI obtained during the course of treatment while a patient is treated on the premises of the hospital or on material sent for analysis at the hospital's lab.
- Patient treatment outside of the hospital's premises and not utilizing hospital services, such as a follow-up visit with the surgeon after discharge, is outside the context of the arrangement.

Step 5: Identification of Legal Issues and Solutions

- The NPP notifies patients that the hospital routinely shares PHI with the medical staff to facilitate treatment by the medical staff to patients and payment to the medical staff for services rendered to the patient in connection to services given to the patient by the hospital.

Step 5: Identification of Legal Issues and Solutions

- The OHCA agreement itself must describe:
  - Service delivery sites
  - That members of the OHCA will share PHI for purposes of treatment, payment, and healthcare operations
  - **To all members of the OHCA that, except for the joint notice, each entity under the OHCA is still a separate entity and responsible for their own HIPAA compliance efforts (transactions, security & privacy).**

Step 6: Ongoing Monitoring and Auditing

- Development of policies and procedures which require periodic assessment of privacy practices
- Documentation of privacy and security training
- Inclusion of privacy and security issues in quality review activities
- Built-in monitoring as required by the Security Rule

Step 7: Gap Closure & Implementation

- The previous slides I've reviewed with you cover our HIPAA-related efforts over the course of the first eight months of our HIPAA implementation project.
- Except for the completion of our departmental assessments and general workforce education, our first eight months of work were spent planning, organizing, and developing appropriate tools to measure and document our progress.

FMC's "HIPAA HIERARCHY"

- Corporate Level: Gap Closure completed by Administration or the HIPAA PMO:
  - Set up PMO & Establish Implementation Task Force & Structure
  - Status as a CE
  - Establish OHCA
  - Develop Overall Project Plan
  - Establish Contract Review Processes; Construct BA Agreements

FMC's "HIPAA HIERARCHY"

- Management Level: Gap Closure completed by Directors, Managers, and the HIPAA Task Force:
  - Establish Organization-Wide Education (New Employee Orientation; Annual Updates)
  - Identify Job-Specific Training Needs
  - Assessment and Gap Analysis
  - Assist With Business Associate Agreement Negotiations
  - Review, revise, and/or create required and optional forms (consents/authorizations)
  - Evaluate Security/Technical Upgrades
  - Develop System-Wide Notice of Privacy Practices

FMC's "HIPAA HIERARCHY"

- Staff Level: Gap Closure completed by Front Line Staff Members:
  - "Where the Rubber Meets the Road"
  - Review, revise, and/or create privacy and security policies and procedures
  - Disseminate new policies and procedures
  - Coordinate efforts with Education Workgroup to deploy job-specific education programs
  - Identify Unit/Department-Specific Privacy and Security Issues & Recommend Remediation

The Privacy Puzzle/Eating the Elephant

- The Privacy Rule (annotated Word document with August 2002 modifications highlighted) is 134 pages long
- FMC's Privacy Workgroup has 14 members
- It became evident very early that we would need to enlist ad hoc members to complete specific tasks and to provide the third level of our "HIPAA Hierarchy"
- Using our Privacy Assessment document as a guide, we split specific tasks into 6 general categories and assigned Privacy Workgroup members to each category

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams:
  1. Business Associates Team
     - Original objective was to identify BA's and ensure that contracts were completed
     - Once we purchased contracting software, this burden switched to the HIPAA PMO
     - We have unofficially renamed this team the Policy and Procedure Review Team
       - They will review all new and/or revised policies and procedures, ensuring that P&P's are consistent across our different entities and avoiding duplication

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams (con't):
  2. Notice of Privacy Practices Team
     - Write the document!
     - Considerations:
       - Make it work across our entities – joint notice
       - Had to wait for amended rule to be written to know whether to include consent language
       - Modified rule recommends layered notice – nice, but more work for the team
       - Lots of simple samples were published…AFTER the team completed their first, six-page draft!

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams (con't):
  3. HIM/Patient Rights
     - Made up of members from Health Information Management/Medical Records Administration
     - Tasks include:
       - Accounting for disclosures
       - Authorizations
       - Disclosures without authorization
       - Patient Rights
         - Amendments/Corrections
         - Restrictions
         - Access/Denial of Access

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams (con't):
  4. Personnel Requirements/Self-Insured Group Health Plan
     - Personnel-related tasks
       - Sanctions
       - Background Checks
     - SIGHP tasks:
       - Amend plan documents
       - Ensure Privacy Rule compliance
       - Partner with TPA re: Transactions and Code Sets
       - Partner with TPA to file TCS Extension

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams (con't):
  5. The "Miscellaneous Leftovers" Team
     - Marketing
     - Fundraising
     - Consent (if mandated by amended rule)
     - Research
     - Retention of Designated Medical Record Sets

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams (con't):
  6. "Best Practices"/Educational Liaison Team
     - Most Challenging; Most Fun
     - Dealing with Cultural Change
     - Oral Communications
     - Minimum Necessary Requirement
     - Privacy and Security P&P Review
     - Identify job-specific training needs
     - Advise Education Workgroup on the need and/or recommended teaching method for facility-wide education
     - Research and adopt privacy & security "Best Practices"

The Privacy Puzzle/Eating the Elephant

- Privacy Workgroup Teams:
  - The Rules:
    - Bring in any ad hoc members you like
    - Make sure members are “front lines” employees who are familiar with issues and logistics
    - Document all your decisions
    - Include relevant decisions in new policies and procedures
    - Bring all new/revised policies and procedures back to the full Privacy Workgroup for review and approval

Transactions and Codes Sets: Bridging the Gap

- Understand what standard transactions are
- Identify the software vendors involved in coding and billing
- Contact each vendor regarding compliance plans (list of standard questions)
- Identify costs associated with implementation
- Identify tasks associated with implementation
- Structure a time line
- File for the extension

Transactions and Codes Sets: Bridging the Gap

- Business Office Considerations:
  - Oral communications- Registration areas; Patient Financial Services
  - Registration issues: obtaining written acknowledgement of NPP or statement of good faith efforts if NPP not provided to patient
  - P&P and appropriate forms for the request and review of restrictions
  - Explanation of facility directory and opt-out
  - Introduction of new standard transactions
  - And training staff on the many technical upgrades in registration and billing software

Security Solutions

- We wish to extend our gratitude to DHHS for delaying publication of a final Security Rule!
- This has allowed us to concentrate on Privacy Rule implementation
- Nevertheless, we have to deal with that broadly worded little Privacy Rule phrase, “A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information” (§164.530)

Security Solutions

- Such safeguards will vary from covered entity to covered entity
  - Difference in organizational cultures
  - Budgetary constraints
  - Existing technologies
  - Feasibility
  - “Reasonableness”
- The newly amended Rule specifies the need for role-based access

Security Solutions

- We went back to the ever-present FMC Security Assessment
- Identified those security-related tasks in which we were:
  - Already compliant
  - Need to achieve compliance in order to comply with the Privacy Rule
  - Wait for final Security Rule before implementing

Security Solutions

- FMC's List of Privacy-Mandated Security Tasks includes:
  - Privacy "to-do" list

Cultural Change: The "Soft Side" of HIPAA

- "90% of security violations occur from within the walls of the organization and 90% of those violations occur from personnel who have been granted access to the information for legitimate purposes.

  Ergo – 90% of security lies between the ears – that is training, education, and cultural change management."

  -Tom Hanks, PricewaterhouseCoopers, LLP

Cultural Change: The "Soft Side" of HIPAA

- Cultural change may be the single biggest challenge for covered entities
- Our departmental assessments proved to us that our employees understand the importance of privacy and security in protecting PHI
- We believe that most breaches in confidentiality are incidental or unintentional
- Constant reinforcement will be required to assure maximum compliance

Cultural Change: The "Soft Side" of HIPAA

- How to strike a balance between customer service and protection of privacy?
- We base our customer service efforts on the premise that with each client encounter, we automatically think, "How may I help you?"
- If helping someone involves divulging PHI, how do we tactfully turn down such requests?

Cultural Change: The "Soft Side" of HIPAA

- "The Step Child of HIPAA Compliance: Culture Change" by D'Arcy Guerin Gue
  - "HIPAAtized" culture might be "where compliant attitudes, behaviors and sensitivity to patient privacy and confidentiality become second nature and assumed throughout the workforce."
  - Some believe in the "Field of Dreams" approach to HIPAA Implementation: "Build it and they will come."
    - (i.e., do the assessments, write the policies, institute new technologies, change the forms, schedule the training, and…Voila! The workforce will follow) …maybe

Cultural Change: The "Soft Side" of HIPAA

- Involve employees in the implementation process, especially policy and procedure development
- Use HIPAA implementation as a launching pad for privacy policies and procedures
  - Visitation
  - How to select a "family representative"
  - How to identify individuals who have a "right to know"
  - Chain of command for privacy and security related questions
  - Complaint process

Elements of a Successful HIPAA Compliance Program

- Achieve buy-in from the top executives of your organization to the clinical and support staff members
- Research, Research, Research
- Plan, Plan, Plan
- Document, Document, Document
- Make it REASONABLE and SCALABLE for your organization's culture, size, and resources

Elements of a Successful HIPAA Compliance Program

HIPAA compliance is an initiative whose ultimate success depends upon the behaviors of every member of the workforce - and no organization or individual wants to be the weakest link…

GOOD LUCK!
BON CHANCE!

…On behalf of the Roman Empire,

THANK YOU-

Melissa Cornwell
HIPAA Coordinator/Privacy Officer
Floyd Medical Center
304 Turner McCall Boulevard
Rome, Georgia 30165
Mecornwell@floydmed.org