USING A PROJECT-BASED APPROACH TO ACHIEVE HIPAA PRIVACY AND SECURITY COMPLIANCE

Prepared for the Third HIPAA Summit
October 26, 2001

Presented by -

Harry E. Smith, CISSP
(Harry_Smith@TimberlineTechnologies.com)

TOPICS

- Why Projects Fail
- Understand Objectives
- Maximize Teamwork
- Avoid Pitfalls
- Monitor Progress

WHY PROJECTS FAIL

- Unclear Objectives
- Insufficient Coordination of Effort
- “Un-Ecological” Decisions
- Problems Not Detected Early

UNDERSTAND YOUR OBJECTIVES

What are the objectives of your HIPAA compliance project?

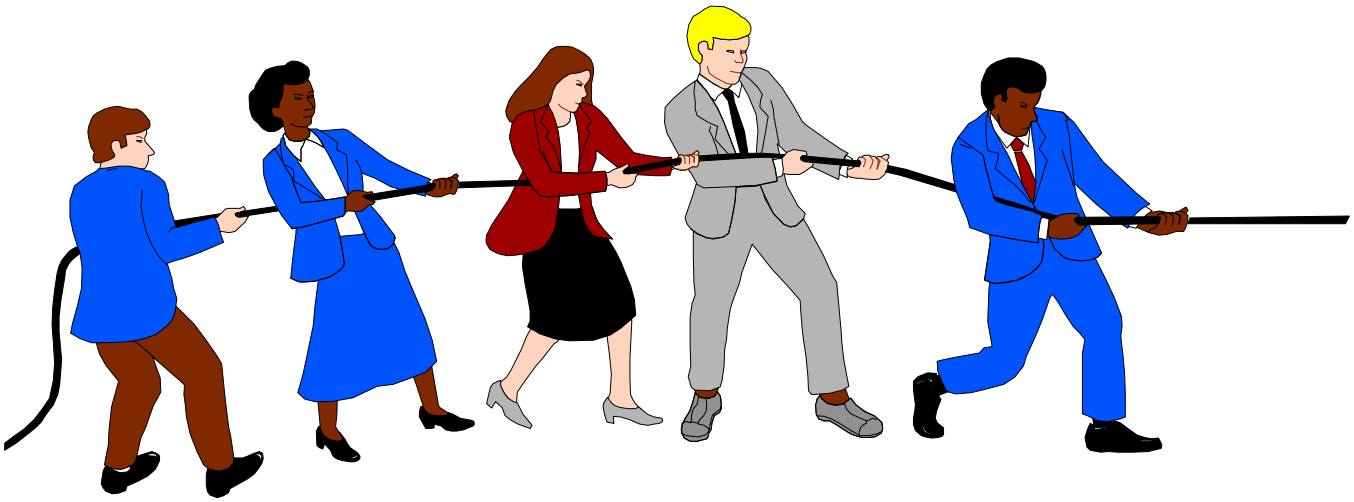
Protect sensitive patient information?

Meet all privacy and security requirements?

Pass a compliance review?

MAXIMIZE TEAMWORK

- Duplication of Effort
- Counterproductive Activities
- Dropped Requirements



AVOID PITFALLS

- Turf Battles
- Land Mines
- Sabotage
- Burned Bridges

"This is what the regulation requires and they are just going to have to accept it!"

MONITOR PROGRESS

- Schedule Slips
- Cost Overruns
- “Scope Creep”

COMPLIANCE CRITERIA

§164.520(c)(3)(iii): If the first service to an individual is delivered electronically, notice of information practices must be delivered contemporaneously in response to the request for service.

§164.520(c)(3)(iv): A covered entity must honor a request for a paper copy of the notice of information practices when the notice has previously been delivered electronically.

INSPECTION

Subject Individual's Right to Inspect and Copy Protected Health Information

§164.520(c)(3)(iv): A covered entity must disclose protected health information to the subject individual when requested to do so.

§164.524(a)(1): A covered entity must grant access to protected health information to the subject individual with certain exceptions (e.g. psychotherapy notes, trial evidence, etc.).

§164.524(c)(1): A covered entity must provide access to protected health information to the subject individual in designated record sets.

§164.524(c)(2)(i): A covered entity must provide access to protected health information to the subject individual in the form requested by the subject individual, if it is readily producible in such form.

Denial of a Subject Individual's Request for Access

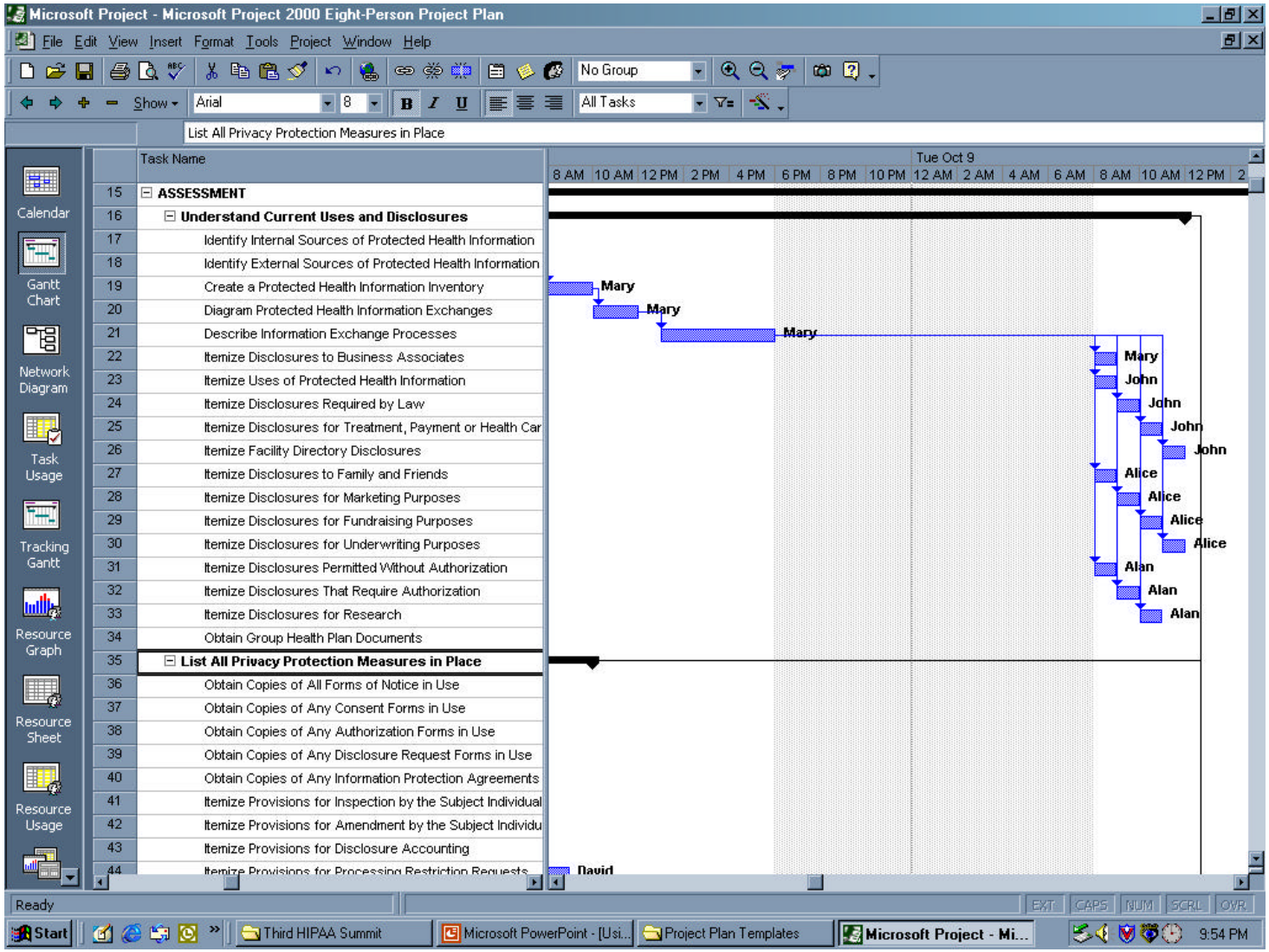
§164.524(d)(1): If a covered entity denies a subject individual's request to access certain protected health information, the covered entity must allow access to all information for which the reason for the rejection does not apply.

§164.524(d)(2): If a covered entity denies a subject individual's request to access certain protected health information, the denial must be in writing and must contain: the basis for the denial; a statement of the subject individual's

PROJECT PHASES

- Assess Current Procedures and Practices
- Perform a Gap Analysis Study
- Identify Compliance Options
- Implement Chosen Solutions
- Prepare for a Compliance Review

PROJECT MANAGEMENT



TIMBERLINE TECHNOLOGIES

http://www.TimberlineTechnologies.com

SUMMARY

- Spend time designing the plan.
- Get the buy-in of all people concerned.
- Measure progress to detect problems early.

REFERENCES

Cleland, David I. *Project Management: Strategic Design and Implementation.* (McGraw-Hill, 1994)

Kerzner, Harold P. *Project Management: A Systems Approach to Planning, Scheduling and Controlling.* (Van Nostrand Reinhold, 1995)

Project Management Institute Standards Committee. *A Guide to the Project Management Body of Knowledge.* (Project Management Institute, 1996)