SIEMENS

HIPAA Security Summit

How Did We Get Here

What Were We Going to Accomplish?

Where Are We Now?

What's Next?

Roger May
HIPAA Program Manager
Siemens Health Services

Siemens medical
Solutions that help

SIEMENS

Agenda

- Challenges & Stimuli
- Summit Processes
- Summit Assets
- Participant Analysis
- Post-Summit Activities
- Current Status
- Go-Forward Plans
- Mini-Case Study
- Other Related Activities

SIEMENS

HIPAA Security

- Structured and Thorough
- Goal-Oriented
- Technology Agnostic
- Built to Cover the Issues
  - Not Defined for Specific Implementations
- Non-prescriptive
  - Requires Judgement
  - Subject to Interpretation
- But….. We will Need to Be Certified
  - Need Guidance!!!

SIEMENS

What Kind of Guidance?

- Reasonable
  - Can you live with it? Does it protect enough?
- “Implementable”
  - Can you put it into operation? Keep it there?
- Scalable
  - Dentists to Delivery Networks
- Business Oriented
  - How Do I fit it within my Business Processes?
- Where to Start???

SIEMENS

Use What's Available

- CPRI
- D.O.D. Rainbow Series
- ASC X12N
- Consulting and Technology Firms
  - Best Practices
  - Other Industries
- Business Continuity Firms / Experts

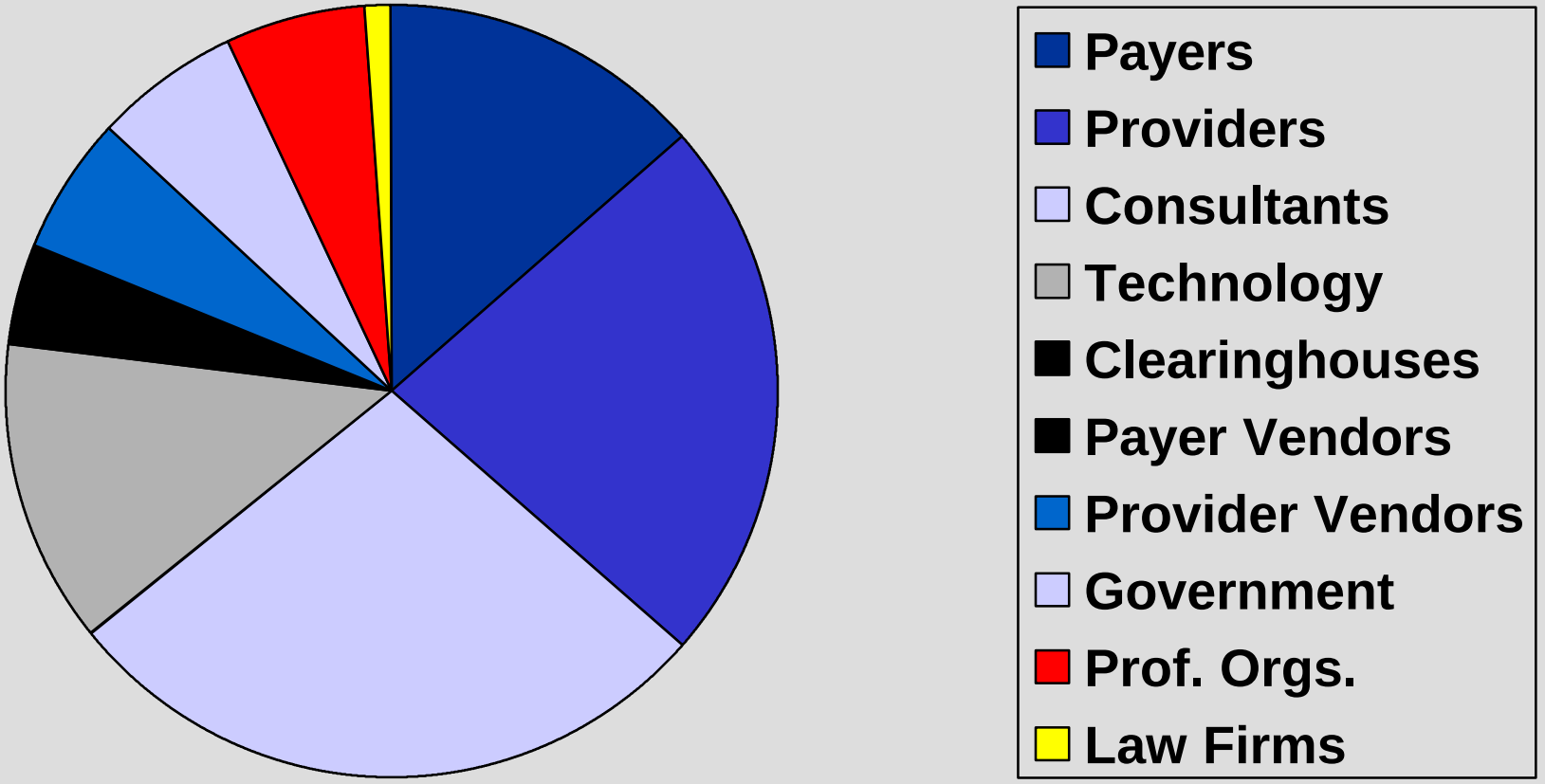
SIEMENS

Initial Event - October 1999

- Overview of HIPAA & Security Drill Down
- Reviewed Goals, Objectives, Methodology
  - Gathered Issues/ Concerns to Address
  - What are you worried about?
- Broke Into Tracks
    - Business Impact Analysis, Solution Design, Implementations, Monitoring and Reporting
    - Led by “Volunteers”
    - “Vendor-isms” were discouraged
- Report Back Progress
  - Ask, Refine, Encourage, Torture, Other
- Repeat Steps Above
- Close and Go to Next Phase

SIEMENS

Cross Industry Contribution



SIEMENS

So, Where Are We Now?

- Compiled information and Available on
  www.smed.com/hipaa

  www.wedi.org/htdocs/resource/archive.htm
- Held Series of Conference Call and Face-to-Face Validation Sessions
- Rolled into WEDI SNIP Efforts on Security
  - Following Final Rules - Conduct Review Session and Update Findings

SIEMENS

What Were Some of the Issues

- Auditing - What, When, Who and For How Long
  - Audit User Activity - Intention is to track Fraud and Abuse
  - Log-on/Log-off & Function Level - Not at the detail level
  - Keep for Reasonable Time - Up to Organization to Determine
  - Who to Conduct Review? Frequency?

SIEMENS

What Were Some of the Issues

- Access Control
  - Policy
    - Do you have policies in place?
    - What does it cover?
    - Who manages it?
    - What happens when someone quits or is fired?
  - Technology - What does your system provide?
    - Role, User, Context
    - Single Sign-on, Biometric

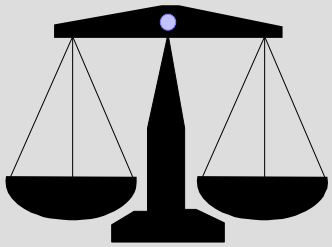
An Example

SIEMENS

Universal Health Services, Inc.

HIPAA,

A Healthcare Operational View



Siemens medical Solutions that help

SIEMENS

An Operational Approach

Identify Operational Task Forces

- Senior Management Leadership
- Information Technology / MIS
- Physical Plant / Facilities Mgmt.
- Health Information Management / MR
- Patient Accounting / Bus. Office
- Admissions / Reg / Scheduling
- Clinicians /Ancillary Services
- Legal/Risk Management
- Public Relations/ Marketing
- Compliance Office
- Human Resources
- Internal Audit

"Users are experts in their own areas - not HIPAA. You can teach HIPAA."

SIEMENS

An Operational Approach

- Incorporate Involvement from Different Levels (Department Head to Clerk / Staff)
- Involve Multiple Facilities (if applicable)
- Establish HIPAA Educational Program
  - Determine Organizational View of Compliance
  - Identify Areas of Impact / Significance
  - Provide Facility Specific Examples
  - Keep it Simple and Accessible
  - Initial and On-Going Education

SIEMENS

An Operational Approach

- Task Forces Review Areas and Document
  - Day to Day Operations
  - Areas of Exposure / Potential Exposure
  - Existing Policies & Procedures w/Recommended Changes
  - New Recommendations
  - Solutions Designed for Efficiency

Note - Compare Task Force Functions to Avoid Overlap (For Example - Which area should own insurance pre-verification - Business Office or Admissions?)

SIEMENS

An Operational Approach

- Task Force Recommendations to Central Oversight Committee for Review and Approval
  - Include Initial Compliance Approach
  - Document On-Going Monitoring Recommendations
  - Educational Programs
- Senior Management Review as Appropriate
- Communication to Other Facilities for Review and Comment (if applicable)
  - Drives Individual Ownership - Make it Theirs

SIEMENS

An Operational Approach

- Implement Changes in an On-Going Manner
  - No Need to Wait for “All”

    (For example - Volunteers need to sign confidentiality agreement.)
  - Keep it Simple
- Create Centralized Mechanism for Managing Comprehensive Documentation (Groupware)
- Incorporate w/Existing Compliance Initiatives

SIEMENS

Managing Challenges

Siemens medical
Solutions that help

SIEMENS

Managing Challenges

- Senior Management Education
  - Provide HIPAA Education with Real Examples of Compliance Exposure
  - Reference Business / Operational Impact - This is Not an IS Only Initiative
  - Identify Key Senior Management Sponsor to be on Corporate Oversight Committee
- Identify Potential Financial Expenditures
  - And Opportunities for ROI
- Incorporate Legal and Risk Management on Central Oversight Committee

SIEMENS

Managing Challenges

- Task Force Education Regarding HIPAA Requirements
- Organization's Specific Definition of What Represents Being Compliant
- Manage Transition with Business Associates
- Communicate with Personnel at All Levels
  - Anxiety Around HIPAA Required Changes
    - What is the impact on me and my department?
    - What additional work will I be required?
    - What liabilities exist?

SIEMENS

Miscellaneous Tips

Siemens medical
Solutions that help

SIEMENS

Miscellaneous Tips

- Read the Federal Register...
- Utilize Associated Industry Material as Reference
- Partner with Vendors
  - Create Ability to Influence Vendor Decisions

SIEMENS

Miscellaneous Tips - Go Through Systems Inventory

- Identify / Brainstorm Issues Based Upon ‘Type’ of Application
  - Medical Records - Known dependence on physicians = ease of access requirements, quick security process
  - Medical Records - Frequently shared outside hospital:

    chart copies, birth records = potential exposure
- Identify Any Issues Based Upon Vendor
  - Vendor HIPAA communication
  - Known issues with previous regulatory compliance efforts
  - Vendor longevity / stability
- Streamline and Standardize

SIEMENS

Summary

- It is Coming
- Word on the Street on Rules
  - No Big Surprises
- Tools are Available
  - Refinements Coming
- Practical Experiences are Underway
  - Stay Tuned for Case Studies
- Let us Know if We Can Help

Other Resources

- WEDI SNIP Security & Privacy White Papers - www.wedi.org/snip
  - Regional SNIP
- EarlyView - www.nchica.org
- CPRI-HOST Toolkit - Security Assistant
- Education via HIPAA University
- Countdown to Compliance - Transcripts & Audio

  www.smed.com/hipaa

Questions?