Healthcare Security Professional Roundtable

John Parmigiani
National Practice Director
Regulatory and Compliance Services
CTG HealthCare Solutions, Inc.
(Moderator)

Panelists

- John Parmigiani (moderator)
- Ali Pabrai
- Ken Patterson
- Tom Walsh
- Drew Hunt
- Richard Marks

Agenda

- Individual Presentations on Key Topic Areas
- Familiarity with Polling Mechanism and Audience Views on Security Issues
- Questions and Answers

Presentation Topics

- Security Policies- John Parmigiani
- Risk Analysis- Ali Uday
- Password Authentication- Ken Patterson
- Audit Control- Tom Walsh
- Contingency Planning- Drew Hunt
- Legal Considerations for Enforcement- Richard Marks

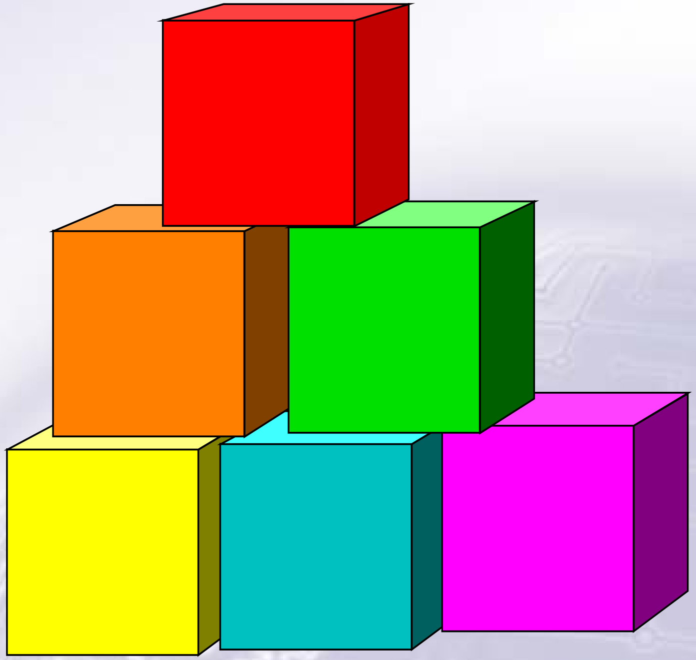
John Parmigiani

- CTGHS National Practice Director for Regulatory and Compliance Services
- CTGHS National Practice Director of HIPAA Compliance Services
- HCS Director of Compliance Programs
- HIPAA Security Standards Government Chair/ HIPAA Infrastructure Group
- Directed development and implementation of security initiatives for HCFA (now CMS)- Director of Enterprise Standards
  - Security architecture
  - Security awareness and training program
  - Systems security policies and procedures
  - E-commerce/Internet
- Directed development and implementation of agency-wide information systems policy and standards and information resources management
- AMC Workgroup on HIPAA Security and Privacy;Content Committee of CPRI-HOST/HIMSS Security and Privacy Toolkit; Editorial Advisory Boards of *HIPAA Compliance Alert's HIPAA Answer Book* and *HIPAA Training Line;* Chair,*HIPAA-Watch* Advisory Board; *Train for HIPAA* Advisory Board; HIMSS Privacy and Security Task Force

Security Goals

- Confidentiality
- Integrity
- Availability

of protected health information



Good Security Practices

- Access Controls- restrict user access to PHI based on need-to-know
- Authentication- verify identity and allow access to PHI by only authorized users
- Audit Controls- identify who did what and when relative to PHI

Symbiotic Relationship

- **Privacy + Security = Confidentiality (*the Present- HIPAA Compliance*)**

- **Electronic information security provides the necessary trusted environment for e-Health**

  (*the Future- total e-Health*)

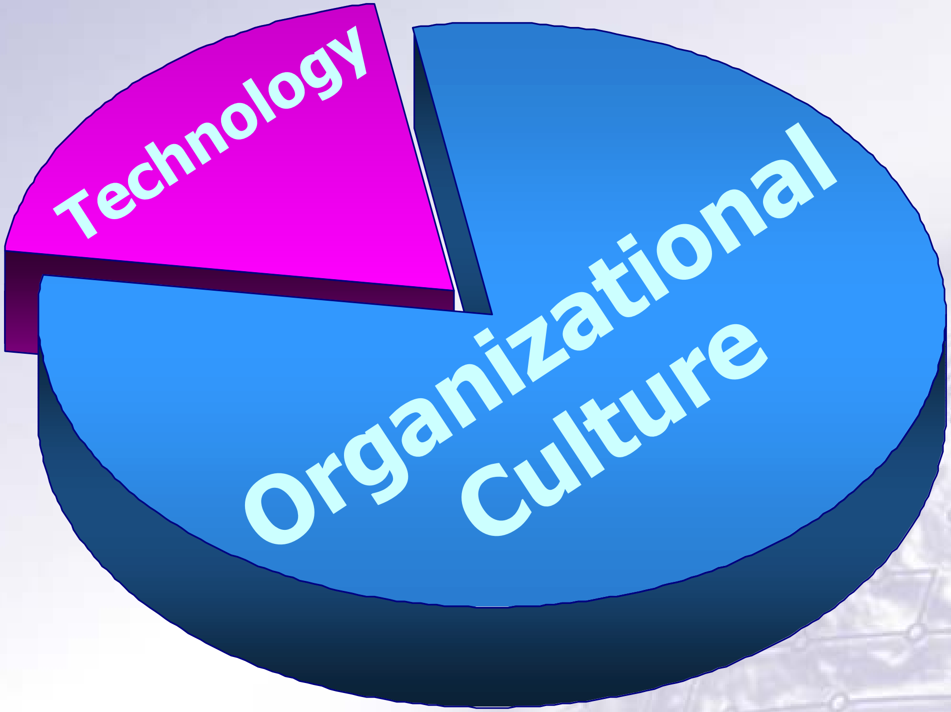
Immediate Steps

- Assign responsibility to *one* person-CSO and establish a compliance program
- Conduct a risk analysis
- Develop/update policies, procedures, and documentation as needed
- Deliver security training, education, and awareness in conjunction with privacy
- Review and modify access (authentication) and audit controls
- Establish security incident reporting and response procedures
- Develop business continuity procedures (contingency planning)
- Make sure your business associates and vendors help enable your compliance efforts

HIPAA = Culture Change

ctg HealthCare Solutions

Organizational culture will have a greater impact on security than technology.

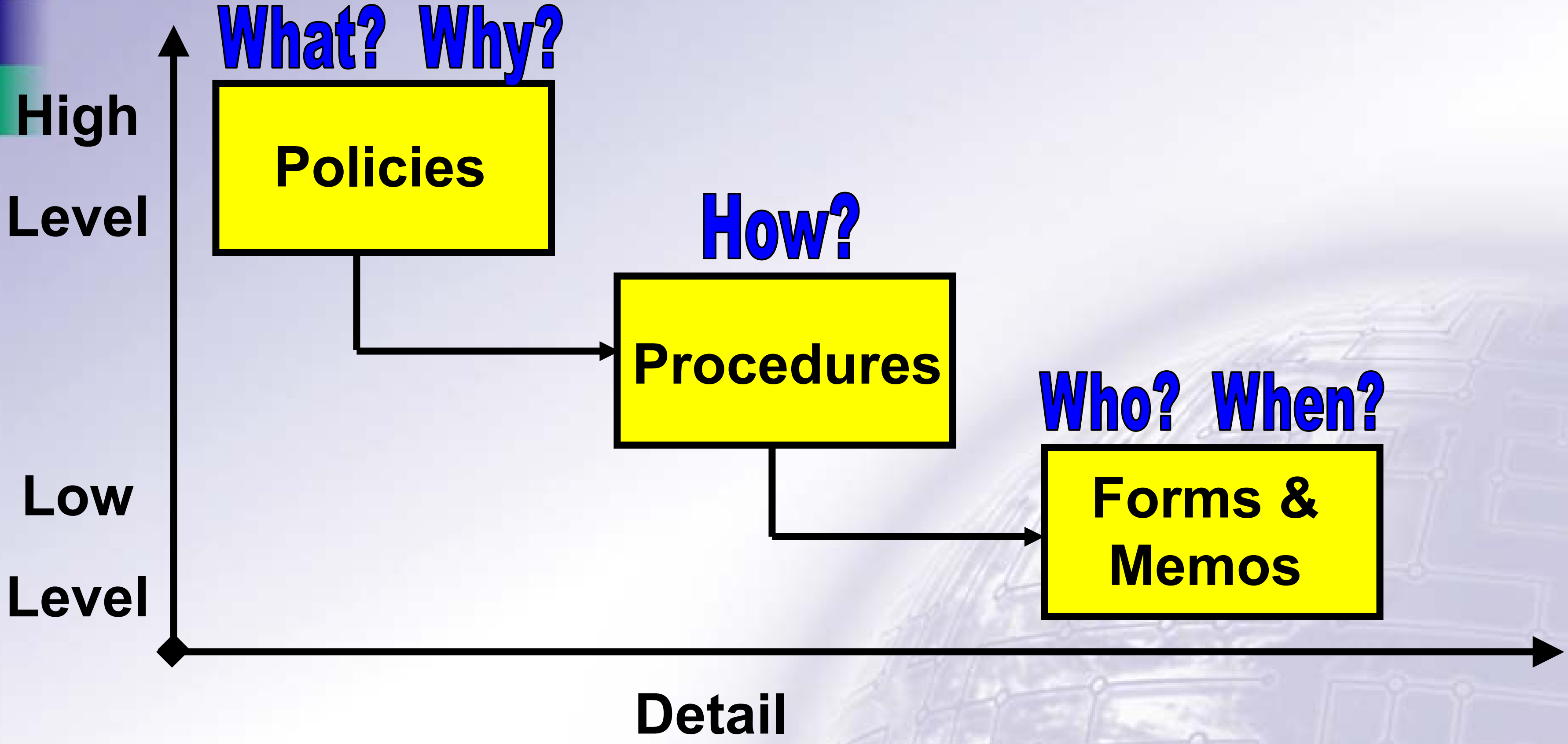


20% technical

80% policies & procedures !!!

Must have people optimally interacting with technology to provide the necessary security to protect patient privacy. Open, caring-is-sharing environment replaced by "need to know" to carry out healthcare functions.

Policies, Procedures & Documentation



Importance of Policies/Procedures

- State the organization’s intent relative to what it will do to protect patient-identifiable and sensitive health information
- Must be clear and concise and “actionable”
- Must be implemented and enforced
- Foundation piece for helping to prove “due diligence” along with other “documentation”

Privacy Policies and Procedures

- Corporate and department policies and procedures relating to: confidentiality, information security, information security incident reporting, disciplinary action and sanctions for security and confidentiality breaches, physical and technical security

- Confidentiality agreements-employees and vendors

Information Security Policy

ctg HealthCare Solutions

- The foundation for an Information Security Program
- Defines the expected state of security for the organization
- Defines the technical security controls for implementation
- Without policies, there is no plan for an organization to design and implement an effective security program
- Provides a basis for training
- Must be implemented and enforced or just "shelf ware"

Thank You!
Next Panelist- Ali