A Practical Risk-Based Approach
April 23, 2003
Today’s Speakers

• Ken DeJarnette
• Jody Noon
• Rena Mears
• Brian Geffert
Today’s Agenda

• Polling Questions <not available in printed document>
• Final Rule Overview
• Applicability
• Common Language
• Key Points
• An Approach to HIPAA Security
• Enterprise Security Program
• Lessons Learned
• Interactive Questions & Answers
Final Rule Overview

- Administrative, Physical, Technical Safeguards
- Adds Required Specification
  - Safeguards that must be implemented
- Adds Addressable Specification
  - Assess whether an implementation specification is a reasonable and appropriate safeguard in its environment
- More flexible and less prescriptive than the draft security rules
- Requires organizations to document the decision process (e.g. framework) used to determine how to implement the required and addressable specifications
- Removes Electronic Signature Standard
- Compliance date is April 21, 2005
“Enterprise Security needs to take into account both Security and Privacy”
### Privacy

- Privacy Official
- Privacy Notice
- Privacy Policies & Procedures
- Employee Education
- Complaint
- Monitoring
- Corrective Action

### Security

- Security Official
- Policies & Procedures
- Employee Education
- Incident Procedures
- Evaluation
- Corrective Action

### Administrative Requirements

#### Access, Use & Disclosure of PHI (Including EPHI)

- Authorizations
- Minimum Necessary Access
- Treatment-Payment-Operation (TPO)
- “Public Good” Exceptions

#### Individual Rights

- Access to Records
- Request for Restrictions
- Disclosure Accounting
- Amendment of Records

#### Business Associates

- Identification
- Written Agreement
- Non-compliance Process
- Due Diligence
Key Points

“Not a New Approach”

- Security Standards are not novel or exhaustive (i.e. ISO 17799, Common Criteria, etc.)
- Risk-based Approach is similar to what is happening in other industries (i.e. GLBA in Financial Services)
Key Points

“Flexibility is Opportunity”

• Less prescriptive means organizations have more choices to address implementation specifications based on the risks faced by their organization

• Allows organizations to balance their risks against the costs of implementing safeguards
“Do not start with a Gap Analysis”
An Approach to HIPAA Security

“How do you implement and manage HIPAA security for your organization?”

BOTTOM LINE:
A Security Decision Framework is needed to effectively and efficiently address all the implementation specifications.
An Approach to HIPAA Security

“Establishing a Security Decision Framework”

<table>
<thead>
<tr>
<th>FRAMEWORK STEPS</th>
<th>KEY ACTIVITIES</th>
<th>KEY ISSUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSINESS REQUIREMENTS DEFINITION</td>
<td>Security Standards, Privacy Considerations</td>
<td>Develop Reasonable and Practical Interpretations of HIPAA Security Rules</td>
</tr>
<tr>
<td>BUSINESS IMPACT ANALYSIS</td>
<td>Document Current Environment, Perform Risk &amp; Safeguard Analysis</td>
<td>Complexity, Environment, Risk, Cost</td>
</tr>
<tr>
<td>SOLUTION IMPLEMENTATION</td>
<td>Compliance with Strategy, Define Initiatives, Define Program Management Structure, Plan Projects</td>
<td>Develop Actionable Projects Mapped to Requirements</td>
</tr>
<tr>
<td>COMPLIANCE MONITORING</td>
<td>Define Monitoring &amp; Progress Reporting, Develop Compliance Plan &amp; Develop Management Reporting Process</td>
<td>Place Projects into Overall Plan to Report Progress and Compliance</td>
</tr>
</tbody>
</table>

“Starting Point for an Enterprise Security Program Requirement and Implementation Process”
An Approach to HIPAA Security

“Alignment with Enterprise Security Program (ESP) while maintaining linkage to the individual regulations”
“Incorporating HIPAA Security into a Holistic and Process-Oriented Approach to Manage Enterprise Security”
“Everyone is on the same page through a common risk language”
“Core security program and standards established”
“Evolutionary integration and consistent execution of security across the enterprise”
“End-to-end transaction integrity achieved”
Security Effectiveness

“Is everything ok?”

Strategic Alignment
- Strategic Business Drivers
- IT Strategies
- Legal/Regulatory Requirements
- Desired Risk Profile
- Security Strategy & Policy

Business Enablement
- Perimeter Network
- Internal Network
- Applications
- Facilities
- Specialized Architectures

Process Enhancement
- System Development Lifecycle
- Project Management
- Change Control
- Production Readiness
- Architecture Standards
- Help Desk
- Incident Response
- Compliance

Tailored Best Practices
- ISO/IEC 17799
- Industry & Business Standards

Security Foundation
- Privacy Blueprint
- Identity Management Blueprint
- Application Integrity Blueprint
- Logging, Monitoring & Reporting
- Systems & Network Infrastructure
- Physical & Environmental
- Information & Asset Baseline
- Infrastructure Blueprint
- Business Continuity Management Blueprint
- Management Blueprint

HIPAA Security: A Practical Risk-Based Approach
Enterprise Security Program

- **Strategic Alignment**: Everyone is on the same page through a common risk language
- **Security Foundation**: Core security program and standards established
- **Process Enhancement**: Evolutionary integration and consistent execution of security across the enterprise
- **Business Enablement**: End-to-end transaction integrity achieved
- **Security Effectiveness**: Is everything ok?

HIPAA Security: A Practical Risk-Based Approach
Lessons Learned

• Involve the Business and key stakeholders
  – Risk tolerance is a key component in determining information security end state during HIPAA Assessment
  – Maintain a tight linkage between the regulatory requirements, business requirements and proposed information security processes and solutions

• Use an Enterprise Security Framework
  – Facilitate a common method for evaluating security requirements and deploying security solutions across the organization
  – Providing for consistent security decisions, planning and investments

• Develop reasonable and practical interpretations of the HIPAA Security Regulations
  – HIPAA tells you “what to do”, but gives latitude on “how to do it”
Lessons Learned

• An organizational Risk Management and Planning process is essential
  – Gain consensus around threats, risks and defining acceptable risk
  – Develop repeatable, traceable Risk Management process

• Develop actionable projects that tie back to the original requirements and address the identified security gaps
  – Aggregate and prioritize projects into an overall program plan
  – Develop strong, sustainable linkages that can trace project justification to original gaps/findings

• Privacy is a key element to process
  – Privacy stakeholders and subject matter experts need to be actively involved in the process
Interactive Q&A

Ken DeJarnette

Jody Noon

Rena Mears

Brian Geffert

Thank you for participating! For more information, please contact the team by calling (800) 877-1298 or sending an email to HIPAAHC@deloitte.com. You can also access all of our HIPAA materials at www.deloitte.com/us/healthcare.
Ken DeJarnette, Principal, Deloitte & Touche, Privacy Practice
(415) 783-4316 or kdejarnette@deloitte.com

• Mr. DeJarnette is a Principal in Deloitte & Touche, specializing in the areas of security and privacy. In addition to practicing law for several years, Ken has over ten years experience in product development and management, and security and privacy consulting. Ken has lead security and privacy projects in regulated industries, including the development of enterprise security programs, the development of security risk frameworks for analyzing processes, systems and applications, the development of security polices and procedures, and the design and implementation of secure infrastructures. Ken is also a member of several ABA committees, including the Information Security Committee (where he is listed as a contributor to the development of the PKI Assessment Guidelines), and the Privacy and Computer Crimes Committee (where he is the co-chair for the Corporate Privacy Handbook). He is also a member of the International Privacy Officers Association and speaks frequently on the topic of information security programs and data protection in financial institutions.
Speakers’ Bios

Jody Noon, <Title>
(503) 727-5207 or jodynoon@deloitte.com

- <Insert Bio here>
Rena Mears, Partner, Deloitte & Touche, Privacy Practice
(415) 783-5662 or renamears@deloitte.com

• Rena Mears is a partner in Deloitte’s privacy practice. She has more than fifteen years experience in management consulting, with an emphasis on the design and implementation of privacy architectures. For our clients, Rena has been the partner-in-charge of significant privacy projects involving privacy assessments, the design of methodologies for surveying and inventorying personally identifiable information across large entities, the development of privacy risk frameworks for analyzing businesses and processes, and the design and implementation of secure infrastructures. In addition, she has advised her clients on issues involving the European Union Data Protection Directive, Safe Harbor, Gramm-Leach-Bliley, and HIPAA. Rena regularly presents at conferences and workshops, speaking on subjects related to Data Privacy, Privacy Architecture and Public Key Infrastructure Implementation. Rena is a member of the American Bar Association Information Security Committee, the American Institute of Certified Public Accountants Information Technology Committee, and the IBM Privacy Management Council (Founding Member).
Brian Geffert, Senior Manager, Deloitte & Touche, Security Services
(415) 783-4162 or bgeffert@deloitte.com

- Mr. Geffert specializes in health care information systems controls and technology risk assessments. Mr. Geffert has worked on the development of HIPAA assessment tools and services for health care industry clients to determine the level of readiness with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. In addition, Mr. Geffert conducts HIPAA awareness training related to the security and privacy requirements for health care organizations. Finally, Mr. Geffert has developed plans and implemented solutions to address health care clients HIPAA security requirements.

- Mr. Geffert has presented and participated in panel discussions on HIPAA at health care industry conferences and meetings. Also, Mr. Geffert has served as a member of the executive committee of the HIPAA Security Summit, which is an industry lead group, to develop the implementation guides for the HIPAA security standards. Mr. Geffert has served a member of the steering committee for the Strategic National Implementation Process (SNIP), sponsored by WEDI, which is addressing implementation related issues surrounding the HIPAA regulations. Finally, Mr. Geffert is the co-author of “HIPAA 201: A Framework Approach to HIPAA Security Readiness”.

- Mr. Geffert is a member of the Information Systems Audit & Control Association (ISACA) and a Certified Information Systems Auditor (CISA). In addition, Mr. Geffert is a Certified Information Systems Security Professional (CISSP). Finally, he is a member of the Health Information Systems Security Association (ISSA).