LESSONS LEARNED FROM THE PIEDMONT HEALTHCARE HIPAA SECURITY AUDIT

Ken Schwartz, Vice President, Compliance
Piedmont Healthcare, Inc. Atlanta, GA

Nadia Fahim-Koster, MBA, CHPS, CISSP
Director, Information Security, Piedmont Healthcare, Inc. Atlanta, GA

Cliff Baker, Director, Health Information Technology, PricewaterhouseCoopers, Atlanta, GA

August 19, 2008

The Privacy Symposium
The Sixteenth National HIPAA Summit

Introduction

This presentation will provide an overview on the following topics:

- The OIG Security Audit of Piedmont
- Lessons learned from the OIG Security Audit of Piedmont
- The CMS Security Audits
- The key security and privacy challenges in Healthcare

OIG Security Audit of Piedmont

Piedmont Healthcare is a multi-facility healthcare system comprised of:

- 4 hospitals located in and around metro Atlanta: Piedmont Hospital, Piedmont Fayette, Piedmont Mountainside and Piedmont Newnan
- Piedmont Heart Institute (employed cardiology practices)
- Piedmont Medical Care Corporation (employed primary care and specialty practices)
- 8200+ employees
- 2 data centers
- Hybrid EMR and paper record systems covering inpatient and outpatient hospital and office/ambulatory services
- 250+ applications

OIG Security Audit of Piedmont

Key Process Points:

- OIG audited Piedmont beginning in March 2007, and concluding in June 2007
- HIPAA Security Rule is enforced by CMS, not OIG
- Rule provides CMS with broad discretion over enforcement decisions based on provider cooperation and commitment to information security
- Purpose of OIG audit was to assess CMS enforcement of the Security Rule by auditing provider compliance
- Several other OIG audits underway since ours
- We have had informal discussions with OIG regarding its findings, but OIG has not released final report as of July 21, 2008
- Final report will be issued to CMS and will likely not be public

OIG Security Audit of Piedmont

Key Observations:

- Overall tone of process has been cooperative with OIG
- We are unable to comment on specific findings (as of July 21, 2008)
- Focus on overall complexity of systems and consistent application of policy across complex systems
- Focus on reasonable internal processes and policies rather than use of specific technologies or tools
- Wireless, identity and access management, auditing
- Housing information security in compliance rather than information services

Lessons Learned

- Organizations should treat Information Security as a compliance issue first and a technical issue second (not the other way around)
- Use a program management approach to Information Security with clearly defined roles and responsibilities, charter and strategic plan
- Perform regular risk assessments, taking into consideration the size and complexity of your organization
- Document how risks are either accepted or addressed by your organization
- Perform third-party vulnerability assessments (penetration testing)
- Be in a perpetual state of audit readiness, the same way you would for Joint Commission

Lessons Learned

- Establish a close working relationship with your organization’s CIO and IT staff as well as Chief Compliance Officer, depending on where you report in the organization
- Use the published CMS list of items that could be requested during an audit as part of your baseline documentation
- Revisit your documentation and your program, make sure it aligns with the HIPAA Security regulations at minimum *(NIST SP800-53: An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Draft)).*
- Keep key business people continually engaged in your security program
- Understand and anticipate business and clinical needs of the organization
- Ensure that your organization invests appropriately and proportionally in the Information Security Program

CMS HIPAA Security Audits

- As with all HIPAA regulations, enforcement is complaint-driven, and focuses on voluntary compliance.
- CMS has the authority to conduct compliance reviews as deemed necessary.
- CMS also has the authority to invoke civil money penalties (CMPs) as defined in the enforcement rule.
- To date, CMS has followed policies and procedures for handling complaints based on voluntary compliance and collaboration with the entities against which a complaint has been filed.

CMS audit focus areas

- Provide summary of the complaint from the perspective of both the complainant and the covered entity
- On-site review of covered entity’s and/or business associates policies, procedures and systems based on compliance review plan
- Detailed report, including findings, recommendations for corrective action. Each review will also include an assessment of the strategies deployed by the covered entity as they apply to the HIPAA requirements
- Each review will include an analysis of the covered entities remote access policies and procedures, in accordance with the CMS Remote Security Guidance Document issued on December 18, 2006. Such analysis will take place regardless of the nature of the complaint

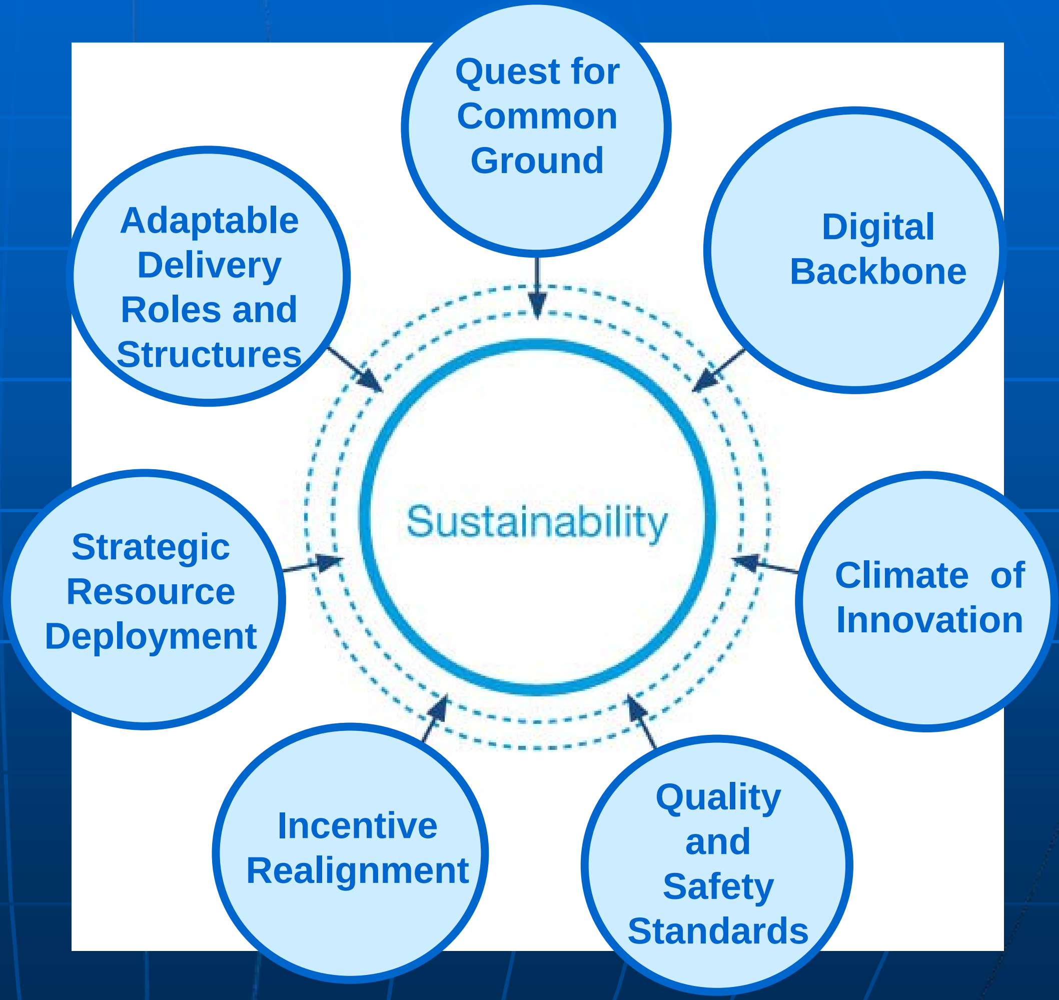
Trust is critical to a sustainable healthcare system

Trust Is at Stake. Privacy, security and information risk management have been elevated to key issues given the business impacts of failure – on both long-term relationships and value. The key elements of a sustainable healthcare system depend on trust:

•Trust must exist to establish a quest for common ground between trading partners.

•The strategic deployment of resources relies on a dependable and secure infrastructure for leveraging resources across traditional geographic and organizational boundaries

•Intellectual property must be protected in order to foster a climate of innovation



Quest for Common Ground
Adaptable Delivery Roles and Structures
Digital Backbone
Sustainability
Strategic Resource Deployment
Climate of Innovation
Incentive Realignment
Quality and Safety Standards

Security is critical to the delivery of quality care

Quality. Institute of Medicine's (IOM) 6 Aims. The IOM has recommended 6 aims for "Crossing the Quality Chasm."

Safety

- Information for clinical decisions is accurate

Efficiency

- Physicians get access to the information that they need when they need it

Patient-centeredness

- Patient's provide information when they trust that their privacy is maintained

Effectiveness

- Unintended changes are minimized

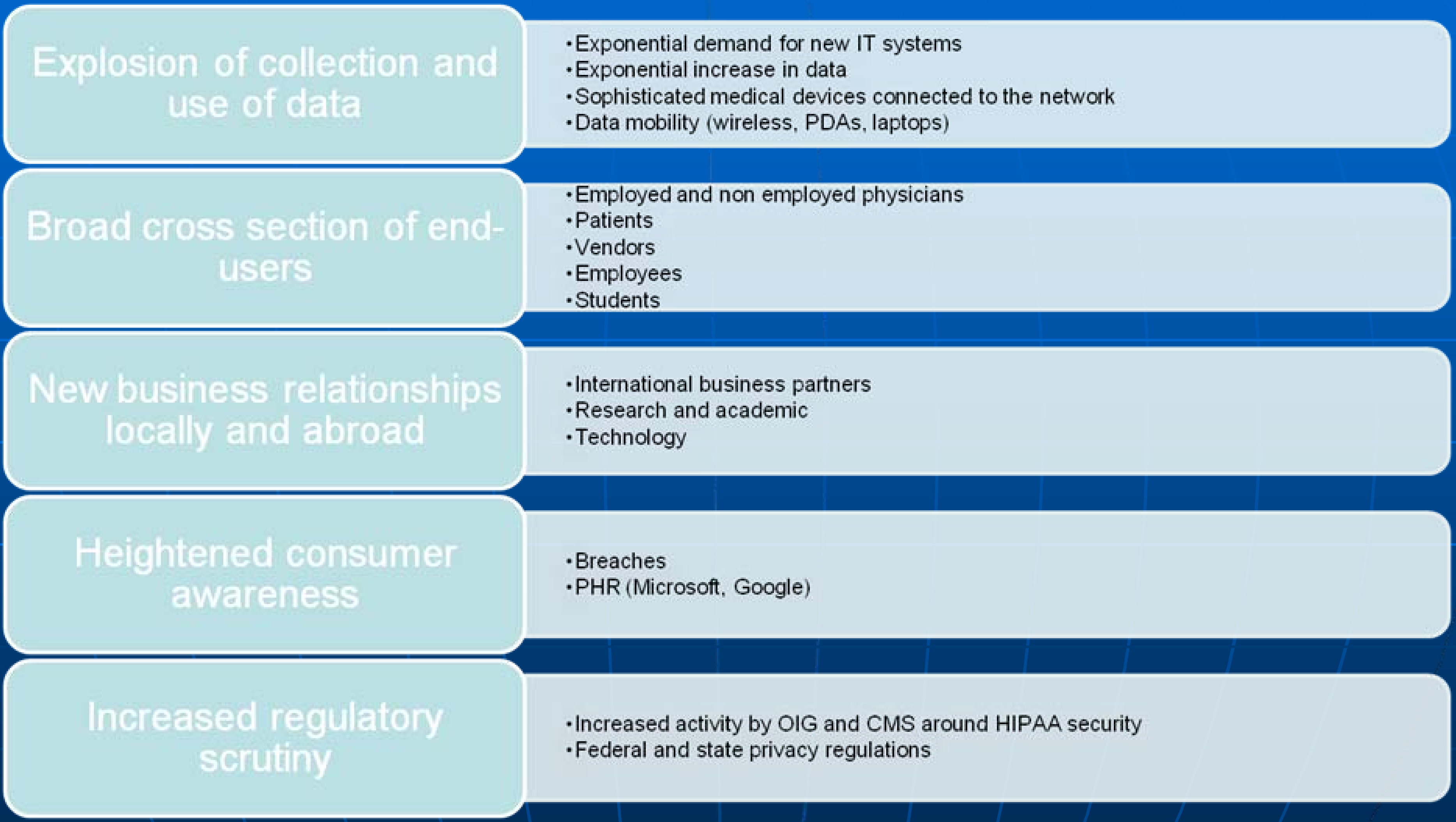
Timeliness

- Clinical information is availability in a timely manner

Equity

- Bias is not instituted due to inappropriate sharing of information

Key Security and Privacy Challenges in Healthcare



Explosion of collection and use of data

- Exponential demand for new IT systems
- Exponential increase in data
- Sophisticated medical devices connected to the network
- Data mobility (wireless, PDAs, laptops)

Broad cross section of end-users

- Employed and non employed physicians
- Patients
- Vendors
- Employees
- Students

New business relationships locally and abroad

- International business partners
- Research and academic
- Technology

Heightened consumer awareness

- Breaches
- PHR (Microsoft, Google)

Increased regulatory scrutiny

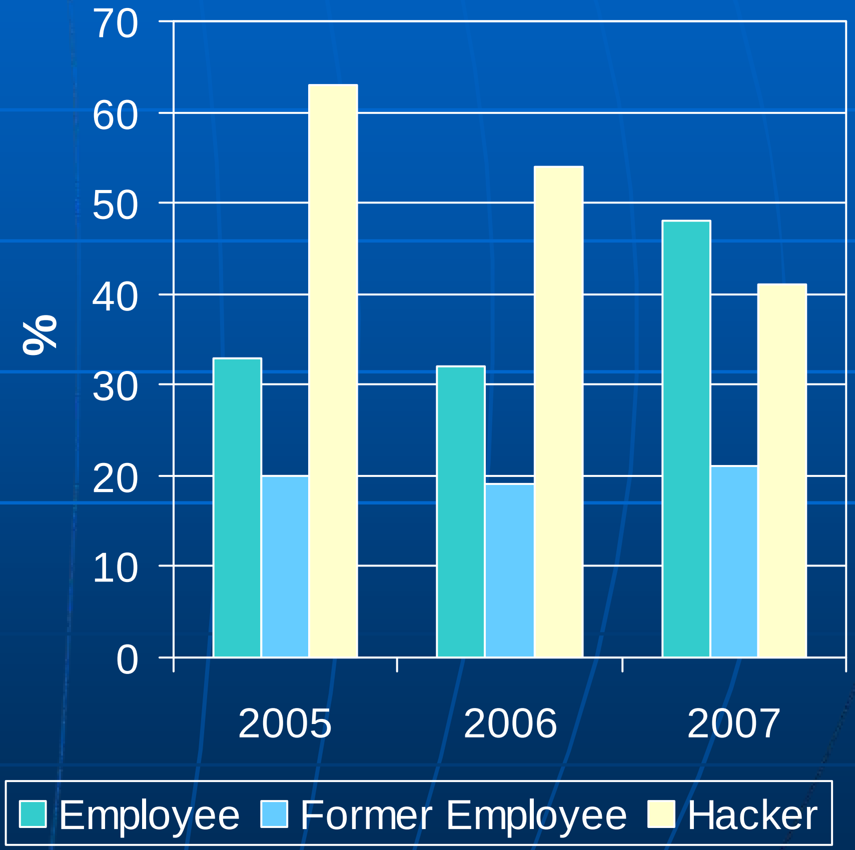
- Increased activity by OIG and CMS around HIPAA security
- Federal and state privacy regulations

Globally, Privacy Officers Are Increasingly Dealing with Identity Theft and the Risk of the Knowledgeable Insider

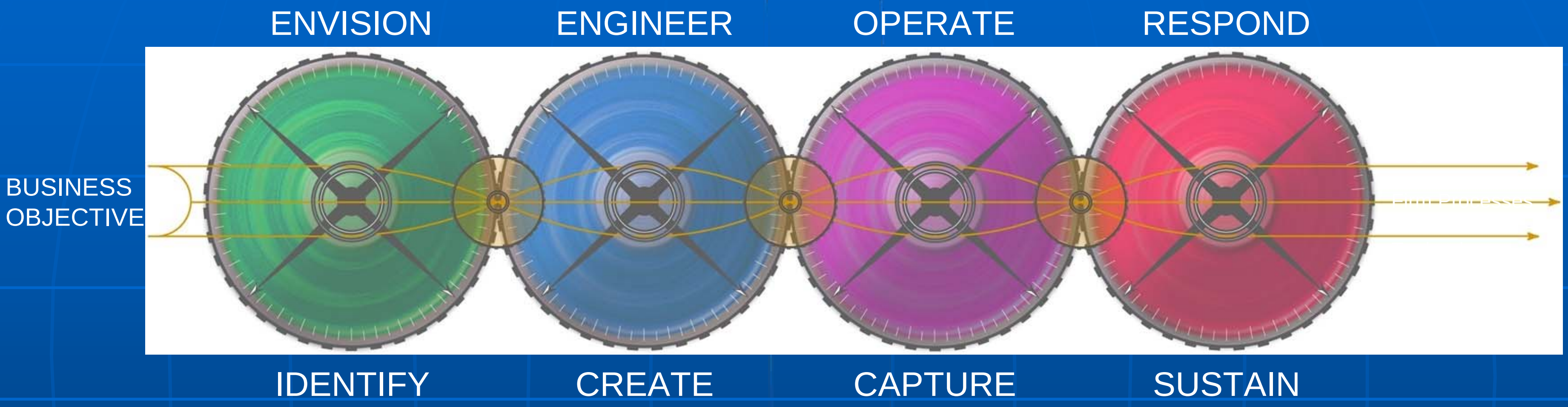
Insider threat is on the rise…

This year employees took over the number one spot as the most likely source of an information security event.

- In 2007, 48% of respondents pointed to employees vs. 41% to hackers.
- But in 2005 only 33% of respondents sighted employees as the most likely source vs. 63% for hackers.



The Enterprise Security Business Model™
The Security Value Chain

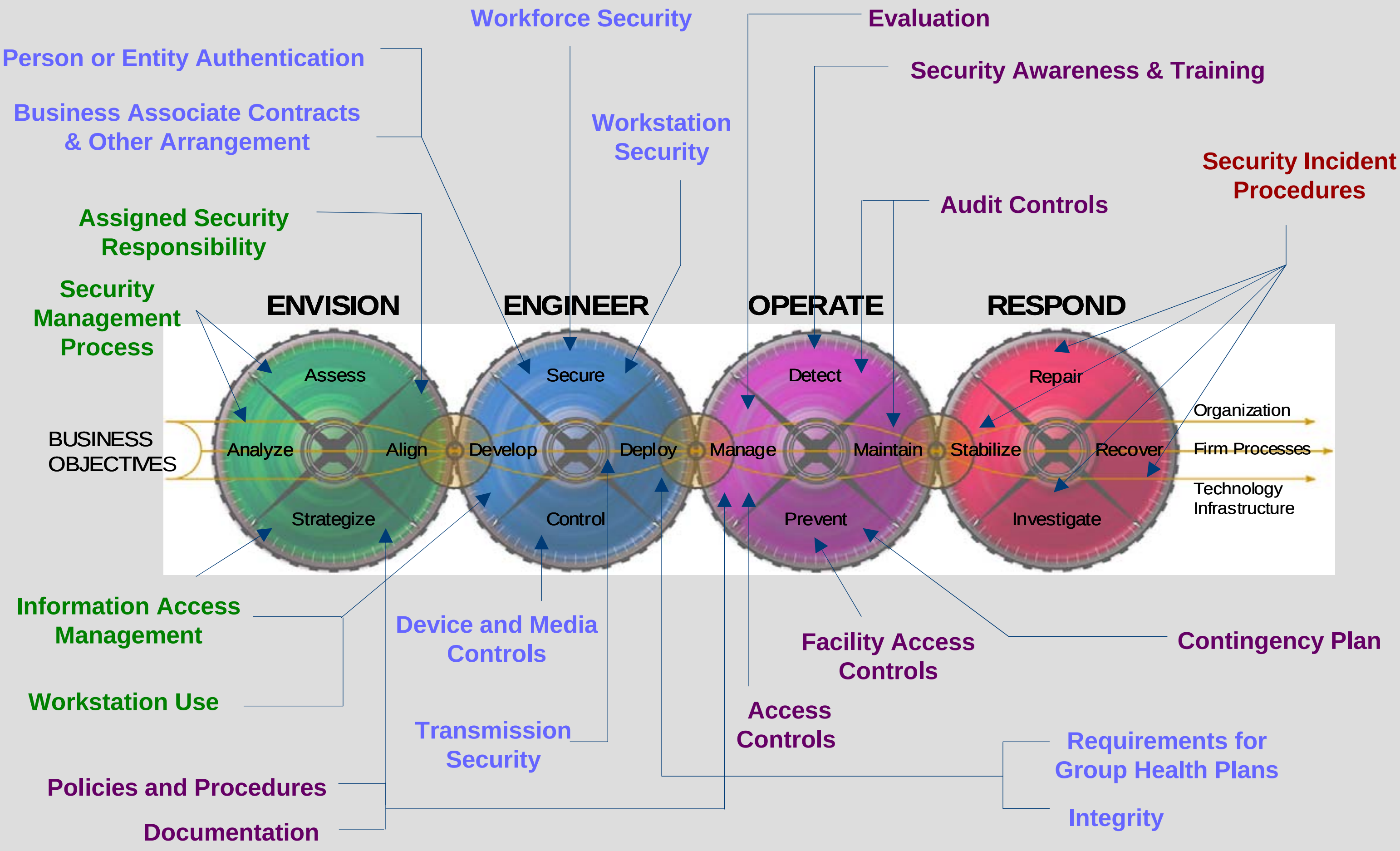


Model for adding value to the business via security

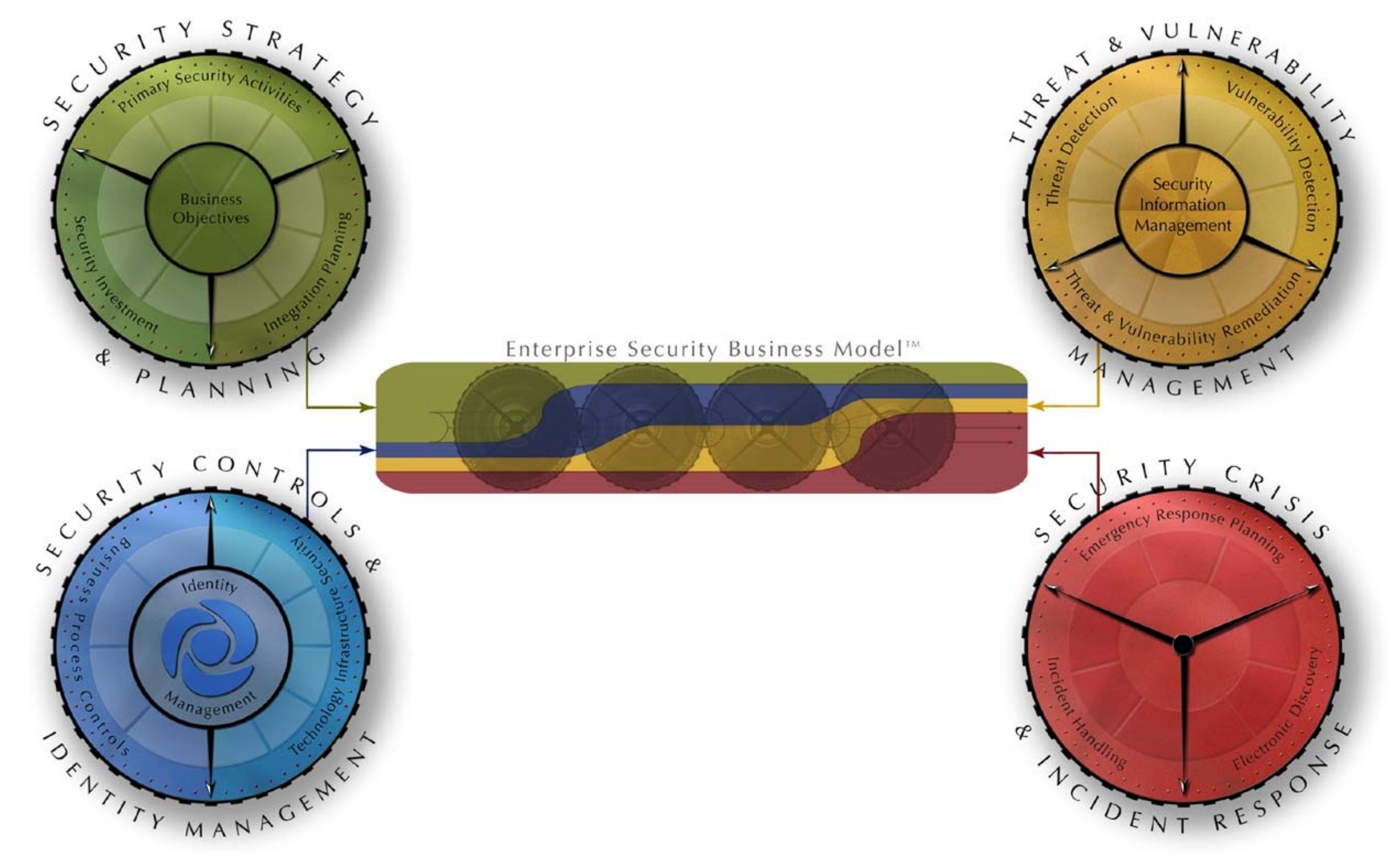
- Value of Enablement (Security of Inclusion)
- Value of Protection (Security of Exclusion)

Comprehensive vision of security activities from a business perspective

ESBM Alignment with HIPAA Security



Security Services That Support These Activities


Security Strategy & Planning
Primary Security Activities
Business Objectives
Security Investment
Integration Planning
Threat & Vulnerability Management
Threat Detection
Vulnerability Detection
Security Information Management
Threat & Vulnerability Remediation
Enterprise Security Business Model™
Security Controls & Identity Management
Business Process Controls
Identity Management
Security Technology Infrastructure
Security Crisis & Incident Response
Emergency Response Planning
Incident Handling
Electronic Discovery

QUESTIONS???