

Influence the Future of Information Security in the Healthcare Industry

# HITRUST Kick-Off Summit

April 28, 2008



# Welcome

# Anti-Trust Statement

- As a public Summit, anti-trust issues are mitigated
- Review of HITRUST's anti-trust guidance
  - Avoid discussion that could evidence intent to use information security for anti-competitive purposes
  - No discussions of the following:
    - Potential competitive effects of HITRUST on any entity regardless of participation
    - Grounds for excluding any entity wanting to participate in HITRUST (other than those defined in the Participating Organization Agreement)
    - Potential restrictions on competitive activities
    - Pricing, rates or changing market share
- Copies of HITRUST's Anti-Trust position statement are available at the registration desk

# Next Two Days

- Goals and Expectations
  - Better understanding of current state and challenges relating to information security in the healthcare industry
  - Provide information on the HITRUST Common Security Framework (CSF)
  - Discuss the CSF development structure, approach and final deliverables
- Format
  - Interactive
  - Audience participation required

# Next Two Days

- Housekeeping
  - Breaks
  - Tonight
    - Cocktail Reception and Dinner (5:45 PM)
  - Tomorrow
    - Breakfast (7:30 AM)
    - Session (8:30 AM)
- Presentation material
  - Will be available starting Wednesday at [www.hitrustalliance.org/summit](http://www.hitrustalliance.org/summit)

# Agenda Structure

- Day One
  - Information security in the healthcare industry
    - Situation
    - Challenges
    - Issues
    - Current state
- Day Two
  - HITRUST Common Security Framework
    - Program structure
    - Development approach
    - Deliverables
    - Timeline

# HITRUST Background

- HITRUST was formed after my many months of discussions with organizations in and out of the healthcare industry
- These discussions took many shapes and sizes and originated from many different types of organizations and, in many cases, varying types of concerns:
  - Lack of an industry best practice and guidance
  - Inconsistent expectations from external and internal auditors
  - Limitations in securing funding for information security
  - Costs associated with implementing inappropriate solutions
  - Numerous and inconsistent trading partner requirements and audits
  - Criticism by customers over sophisticated security verses their competitor
  - Risks associated with data breach and loss
- How are information security practices being established, maintained and verified in the healthcare industry?

# HITRUST Overview

- Created to establish and oversee trust in the electronic flow of information through the healthcare system
- Establishing a common security framework that allows for more effective and secure creation, access, storage and exchange of personal health information
- Establishing an accreditation program to verify consistent implementation of the HITRUST Common Security Framework for internal and external purposes
- Supporting education relating to healthcare information security to industry, regulators and policy makers
- Brings together a broad array of healthcare organizations and stakeholders to collaboratively address information security
- Overseen by an Executive Council providing leadership and guidance

# Executive Council

**Paul Connelly**  
Vice President and  
Chief Information Security Officer  
Hospital Corporation of America

**Frank Grant**  
Senior Director – US Healthcare  
Cisco Systems, Inc.

**Nick Mankovich**  
Senior Director, Product Security & Privacy  
Philips Healthcare

**David Thomas Nassef**  
Vice President,  
Office of the Executive Chairman  
Pitney Bowes Inc.

**Russell Pierce**  
Chief Information Security Officer  
CVS Caremark

**Jim DeMaioribus**  
Senior Director, Health Care Strategy  
Johnson & Johnson Health Care Systems, Inc.

**Kimberly S. Gray, Esq., CIPP**  
Chief Privacy Officer  
Highmark Inc.

**Jon Moore**  
Chief Information Security Officer  
Humana Inc.

**Daniel Nutkis**  
Chief Executive Officer  
HITRUST

Influence the Future of Information Security in the Healthcare Industry

# **Common Security Framework Kick-Off Summit**

## **Need for a Common Security Framework in the Healthcare Industry**

David Yakimischak, SureScripts

Russell Pierce, CVS/Caremark Corporation

Chris Kidd, University of Utah Health Sciences

Jon Moore, Humana

Amry Junaideen, Deloitte & Touche LLP

# Agenda

- Purpose and objectives
- Background
- Introductions
- Facilitated discussion
- Open Q&A

# Purpose and objectives

Discuss the need, benefits and requirements of a common security framework

# Background

- Biggest pain point: multiple requirements from numerous sources
  - Volume
  - Inconsistency
  - Duplication
  - International implications
  - Implementation standards
  - Lack of value

# Introductions

- Introductions
  - David Yakimischak, SureScripts
  - Russell Pierce, CVS/Caremark Corporation
  - Chris Kidd, University of Utah Health Sciences
  - Jon Moore, Humana

Name

Title and role in the organization

Brief summary of experience



# Facilitated discussion



# Open Q&A

# Common Security Framework Kick-Off Summit

State of world-wide information  
security standards affecting  
U.S. healthcare organizations

MODERATOR

Nick Mankovich

Philips Healthcare

# Presentations and Discussion

- The landscape of information security standards,
- the existing gaps and barriers, and
- the way forward to a common security framework.

FOCUS: outlining the various US and International standards and standards activities relevant to healthcare organizations.

# Day 1, Standards Session

1.	How do standards fit into the problem?	Jesse Bowen, Partner, Accenture Technology Consulting – Security, Chicago, IL
2.	What are the applicable world standards?	Mark Schiller, Director, Security Strategy Office, Hewlett Parkard, Fort Collins, CO
3.		Taiye Lambo, Founder & CTO, eFortresses, Inc., Atlanta, GA
4.	Where do we think HITRUST should start?	Kevin Walker, Director & Senior Systems Strategist Cisco Systems Inc., San Jose, CA
5.	DISCUSSION	Panel and audience

# Day 1, Standards Session

1. Introduction	<b>Nick Mankovich</b> , Sr. Director Product Security & Privacy Philips Healthcare, Andover, MA
2. How do standards fit into the problem?	<b>Jesse Bowen</b> , Partner, Accenture Technology Consulting – Security, Chicago, IL
3. What are the applicable world standards?	<b>Mark Schiller</b> , Director, Security Strategy Office, Hewlett Parkard, Fort Collins, CO  <b>Taiye Lambo</b> , Founder & CTO, eFortresses, Inc., Atlanta, GA
4. Where do we think HITRUST should start?	<b>Kevin Walker</b> , Director & Senior Systems Strategist Cisco Systems Inc., San Jose, CA
5. DISCUSSION	Panel and audience

# Challenges of Current Standards

- So many from which to choose!
  - Compliance and certification
  - Management, organization, and process
  - Technical: controls vs. technology implementation
- One size does not fit all
  - Standards are often not designed for scalability
  - Generic vs. proscriptive: “room for interpretation” leads to ambiguity when inconsistently applied
  - Lack of repeatability

# What Should Be the Goal?

- Adaptability
  - Scalable to different sized organizations found within the healthcare industry
  - Suitable for all organizations, regardless of industry segment or business model
- Guidance that is practical and useful for building a security organization
  - Implementation details that produce consistent, effective results
  - Appropriate level of specificity to speed deployment without creating new operational burdens

# Survey of Security Standards: Practice and Compliance

- International: Practice and Compliance
  - ISO: Security Practices and Compliance
    - ISO/IEC 27000 Series (from ISO/IEC JTC1)
      - ISO 27001 – Certification standard against which organizations' ISMS may be certified (published in 2005)
      - ISO 27002 – Code of practice (previously known as ISO 17799 and before that BS 7799 Part 1. Last revised in 2005, and renumbered ISO/IEC 27002:2005 in July 2007). Provides guidance for the controls listed in Annex A of ISO 27001
      - ISO 27006 – Guide to the certification/registration process (published in 2007)
      - ISO 27005 – Standard for information security risk management (ETA 2009)
    - COBIT
      - Control Objectives for Information and related Technology (COBIT)
      - From: ISACA (Information Systems Audit and Control Association) and ITGI (IT Governance Institute)
      - Current version: COBIT 4.1
      - Encouraged for Sarbanes-Oxley (SOX) Compliance

# Survey of Security Standards: Practice and Compliance

- International: Practice and Compliance *(Continued)*
  - ITIL
    - IT Service Management
    - Basis for BS 15000
    - Evolved to ISO/IEC 20000 certification standard
  - Recommended Overview Reading:  
“Aligning COBIT, ITIL and ISO 17799 for Business Benefit: A Management Briefing from the IT Governance Institute and the Office of Government Commerce

[http://www.isaca.org/Template.cfm?Section=COBIT\\_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22493](http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22493)

# Survey of Security Standards: Technical Standards

- Technical Security Standards (Billions and Billions):
  - Addressing Interoperability, Strength of Function, etc. e.g.
    - ISO
      - i.e. Fast Track Trusted Computing
    - IEEE
      - i.e. Key Management
    - OASIS
    - IETF
      - i.e. IPv6
    - Liberty
    - Trusted Computing Group
    - Common Criterion (Evaluation Standards)
      - Recognized by International Treaty
    - Jurisdiction Specific...e.g.
      - U.S. Gov't: NIST, FIPS, HIPAA