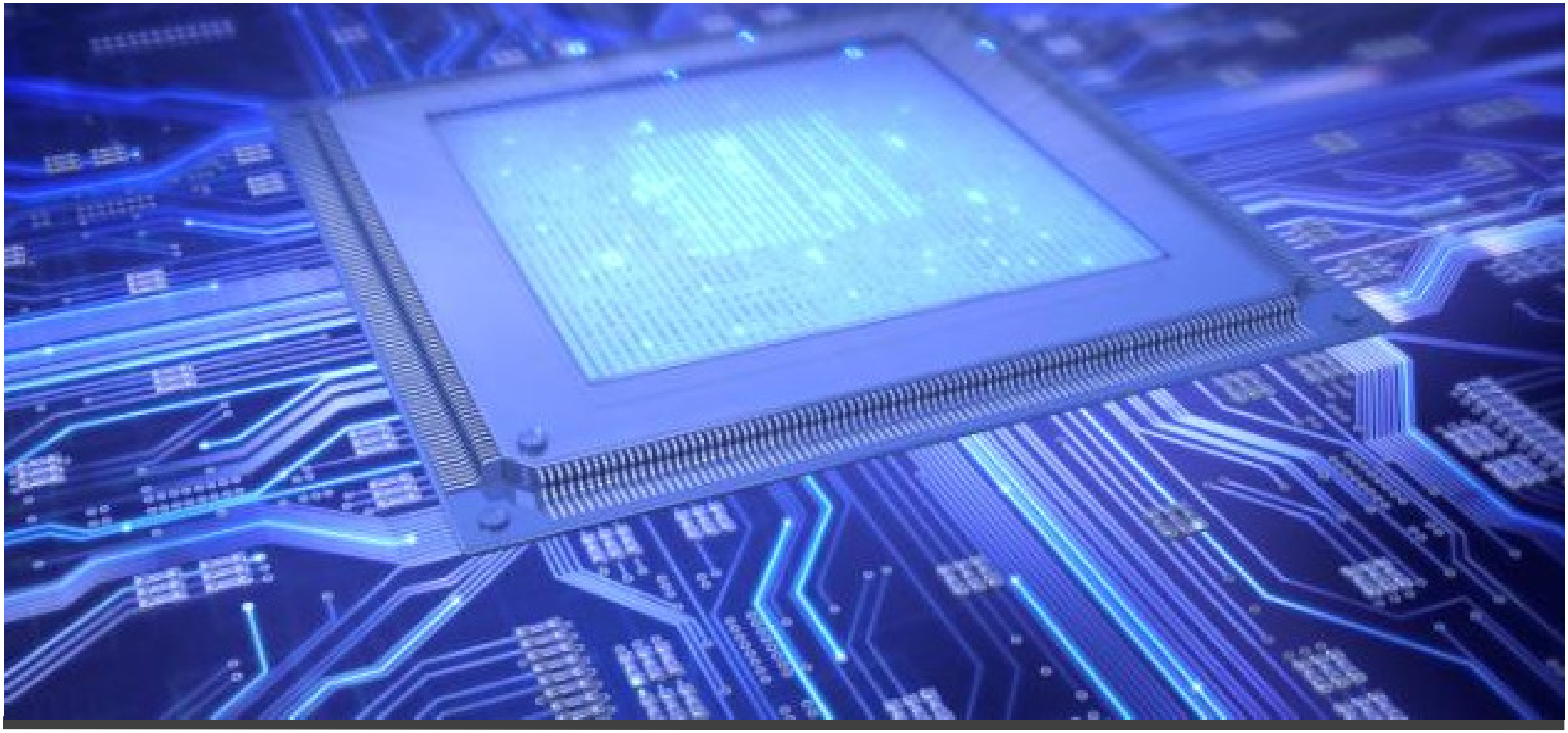


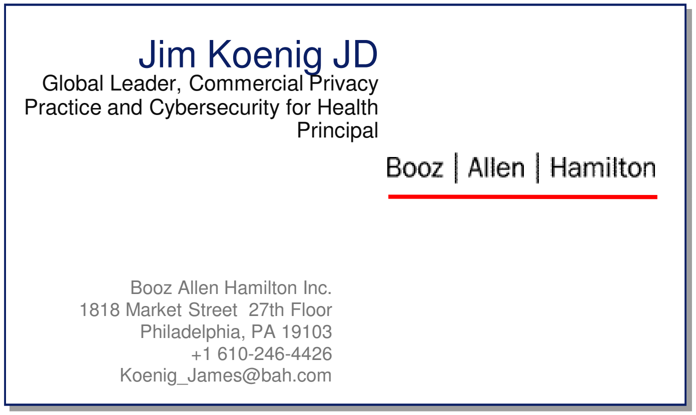
Lessons Learned from OCR Audits, Mock Audits and Enforcements – 5 Things Every Health Care Company Needs to Know Now

February 5, 2014

HIPAA Summit 2014, Washington, DC

Booz | Allen | Hamilton

Introduction



Jim Koenig JD
Global Leader, Commercial Privacy
Practice and Cybersecurity for Health
Principal

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
1818 Market Street 27th Floor
Philadelphia, PA 19103
+1 610-246-4426
Koenig_James@bah.com

Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

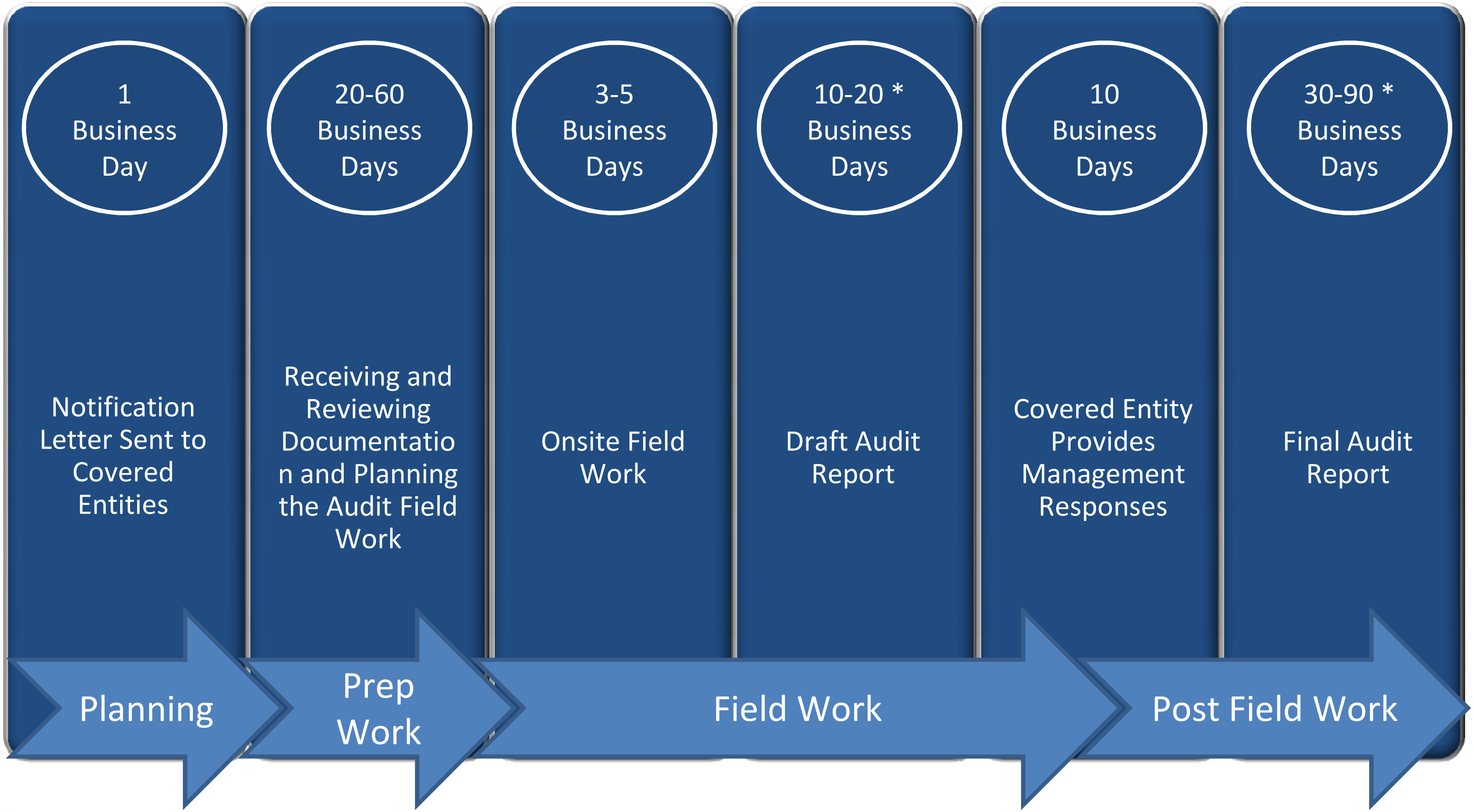
  i. Know the Rules and Areas of Non-Compliance
  ii. Know the Risks Specific to Your Organization
  iii. Know the Data and the Flows – Internal and External
  iv. Know Your Audit Process and Prepare
  v. Know the Roadmap Ahead and Be Self-Aware

Background

- **Statutory Basis.** HITECH Section 13411 requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards.
- **Audit Program.** To implement this mandate, OCR piloted a program and performed 115 audits of covered entities in 2012.
- **Goal and Objectives.** To improve covered entity and business associate compliance with the HIPAA standards
  - Examine mechanisms for compliance
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Encourage renewed attention to compliance activities
- **Scope:** Every covered entity is eligible for an audit. In 2011-2012, OCR audited:
  - Individual and organizational providers
  - Health plans of all types
  - Health care clearinghouses

  Note: Business Associates in later audit wave

Audit Timing



1 Business Day	20-60 Business Days	3-5 Business Days	10-20 * Business Days	10 Business Days	30-90 * Business Days
Notification Letter Sent to Covered Entities	Receiving and Reviewing Documentation and Planning the Audit Field Work	Onsite Field Work	Draft Audit Report	Covered Entity Provides Management Responses	Final Audit Report
Planning	Prep Work	Field Work		Post Field Work	

* Duration varies based on several factors such as, the volume and complexity of findings noted

Audit Protocols – 11 Modules

- The audit protocol is organized around 11 different modules.
- Provides established criteria, audit testing procedures, work paper reference and applicability.

1. Breach Notification

Security

2. Administrative Safeguards
3. Physical Safeguards
4. Technical Safeguards

Privacy

5. Notice of Privacy Practices
6. Rights to Request Privacy Protection of PHI
7. Access of Individuals to PHI
8. Administrative Requirements
9. Uses and Disclosures of PHI
10. Amendment of PHI
11. Accounting of Disclosures

Enforcement - Over $28 Million in Resolution Agreements & Fines for Variety of Issues an Entities – Focus on Risk

Covered Entity	Amount	Date
Adult & Pediatric Dermatology, P.C. of Massachusetts	$150,000	20-Dec-13
Affinity Health Plan	$1,215,780	14-Aug-13
WellPoint	$1,700,000	11-Jul-13
Shasta Regional Medical Center	$275,000	13-Jun-13
Idaho State University	$400,000	21-May-13
Hospice of North Idaho	$50,000	28-Dec-12
Massachusetts Eye and Ear Institute	$1,500,000	17-Sep-12
Alaska DHSS	$1,700,000	26-Jun-12
Phoenix Cardiac Surgery	$100,000	13-Apr-12
BCBS Tennessee	$1,500,000	13-Mar-12
UCLA Health System	$865,500	6-Jul-11
Massachusetts General Hospital	$1,000,000	14-Feb-11
Cignet Health	$4.3 Million	4-Feb-11
(Summary Judgment US District Court for Cignet)	$4,782,845	28-Aug-13
Management Services Organization of Washington	$35,000	13-Dec-10
Rite Aid Corporation	$1,000,000	27-Jul-10
CVS Pharmacy, Inc.	$2,250,000	16-Jan-09
Providence Health & Services	$100,000	16-Jul-08
	$18,624,125	

Fortune Telling – What You Might See

- **Results of Audits.** Provide further insight into risks and vulnerabilities, non-compliance areas and best practices.
- **Revised Protocols.** To implement this mandate, OCR piloted a program and performed 115 audits of covered entities in 2012.
- **Risk-Based Approach.** Prior audits were done on a strict compliance approach. Guidance as to how more of a risk-based approach will be utilized – different than existing healthcare use of "risk base."
- **Potentially More Audits.** A new process and to be announced scale, emphasis and approach.
- **Continued Enforcement Emphasizing Risk Assessment.** To improve covered entity and business associate compliance with the HIPAA standards

Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance

ii. Know the Risks Specific to Your Organization

iii. Know the Data and the Flows – Internal and External

iv. Know Your Audit Process and Prepare

v. Know the Roadmap Ahead and Be Self-Aware

Preliminary Analysis Discussed by OCR

- Common Privacy areas:
  - Notice of Privacy Practices
  - Access of Individuals
  - Minimum Necessary
  - Authorizations

- Common Security areas:
  - Risk Analysis
  - Media movement and disposal
  - Audit controls and monitoring

- Policies and Procedures exist but are outdated or not implemented
- HIPAA compliance programs are not a priority
- Small providers are not in compliance
- Larger entities demonstrate security challenges
- Entities are not conducting Risk Assessments
- Entities are not managing third party risks
- Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size

Table of Contents

I. The Audits, Protocols and Enforcements

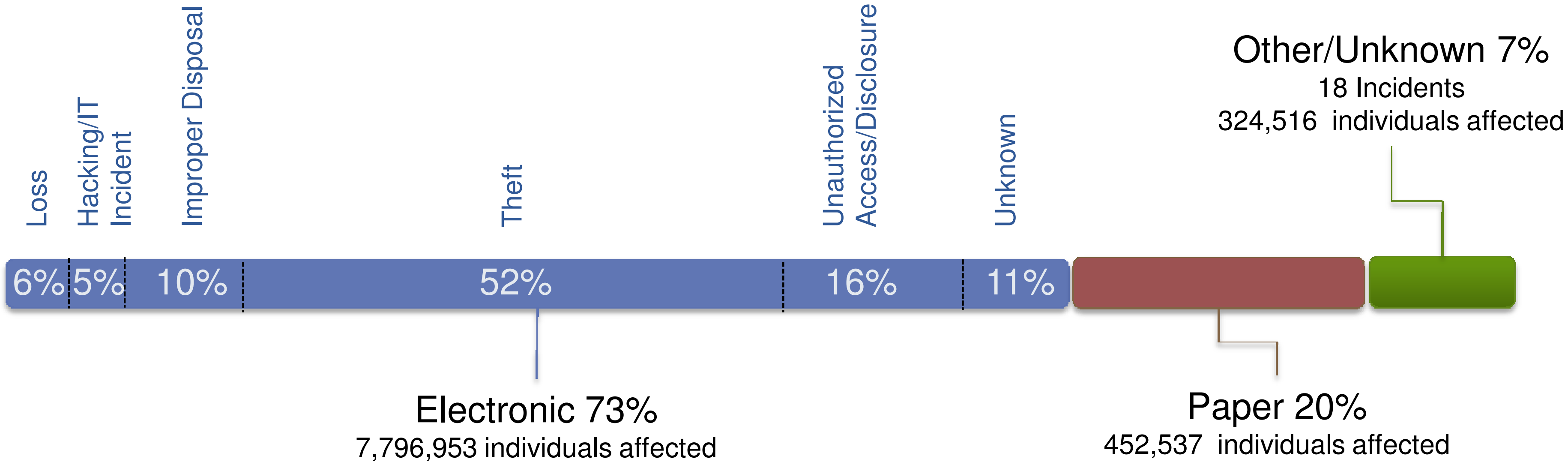
II. Lessons Learned - Five Things You Need to Know Now

- i. Know the Rules and Areas of Non-Compliance
- ii. Know the Risks Specific to Your Organization
- iii. Know the Data and the Flows – Internal and External
- iv. Know Your Audit Process and Prepare
- v. Know the Roadmap Ahead and Be Self-Aware

The Risk Landscape

	2010-2011	2012-2013
Records Lost	15,681,270	9,594,959

Breach Data Composite for 2012 and 2013



Source: US Department of Health and Human Services Office for Civil Rights

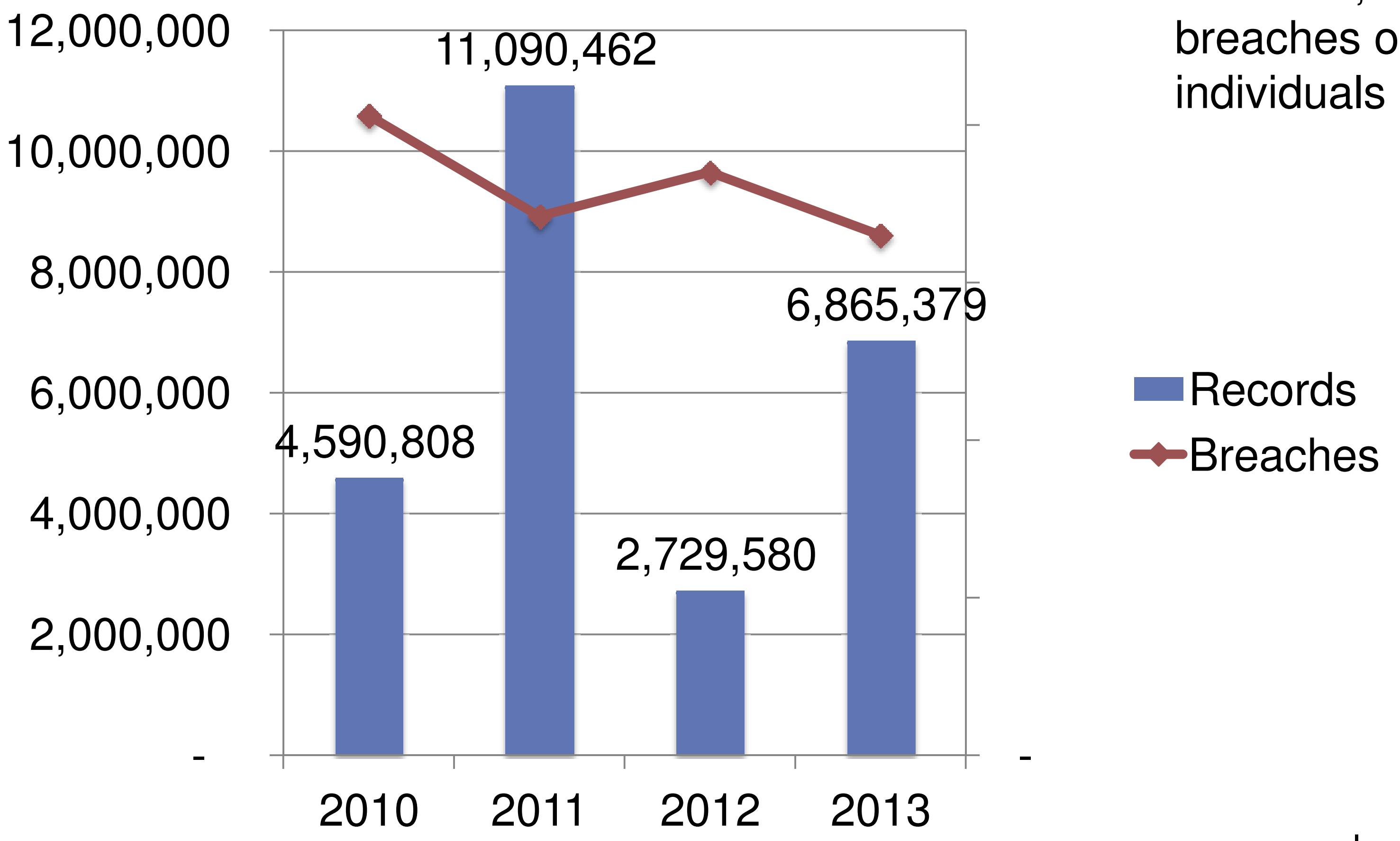
Booz | Allen | Hamilton

Number of Individuals Impacted vs. Number of Breaches

- *Number of Breaches Consistent*
- *Number of People Impacted Up*

	2010-2011	2012-2013
Records Lost	15,681,270	9,594,959 **(-39%)**

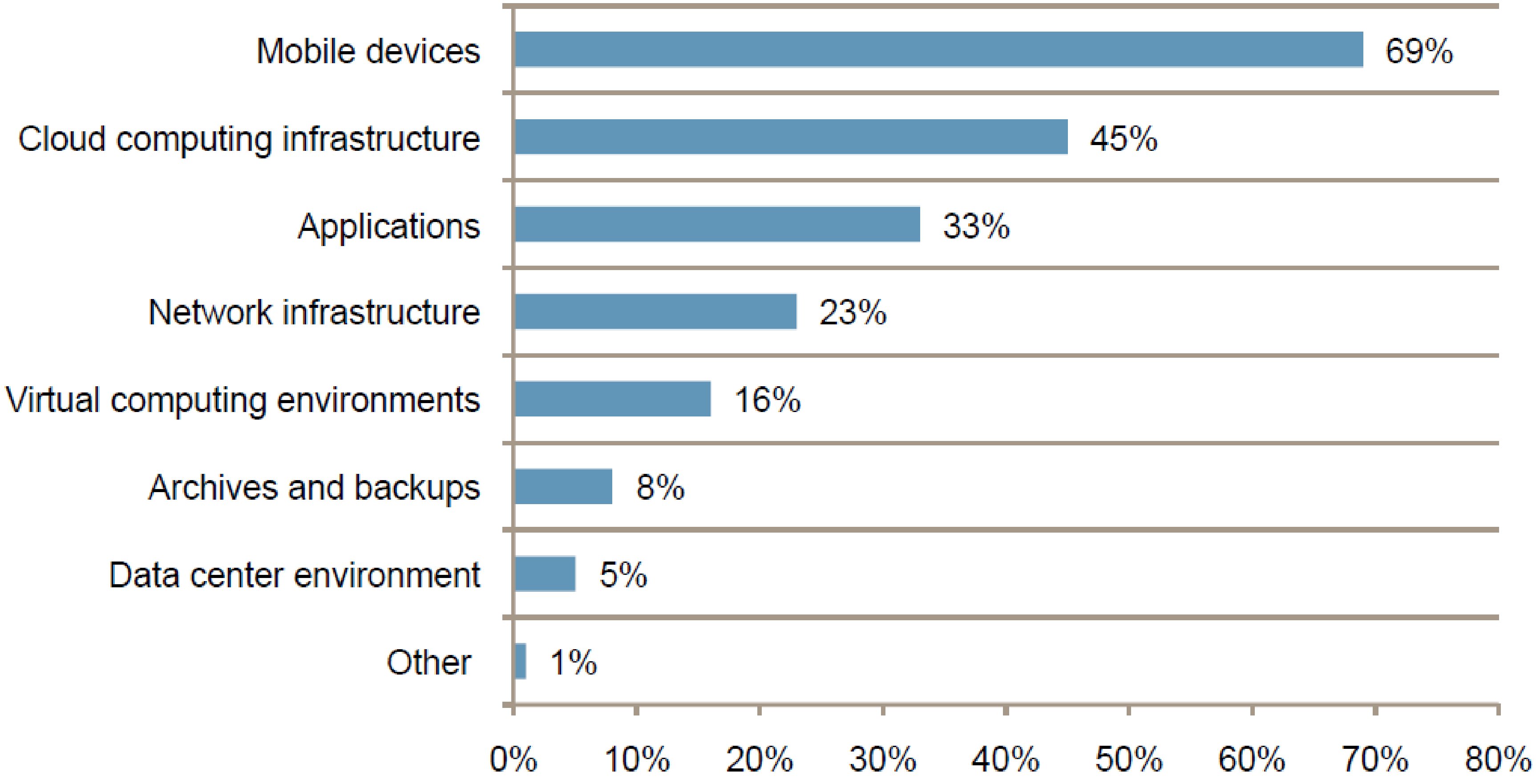
Note: 90,000+ reports of breaches of under 500 individuals for 2013



Booz | Allen | Hamilton

Source: US Department of Health and Human Services Office for Civil Rights

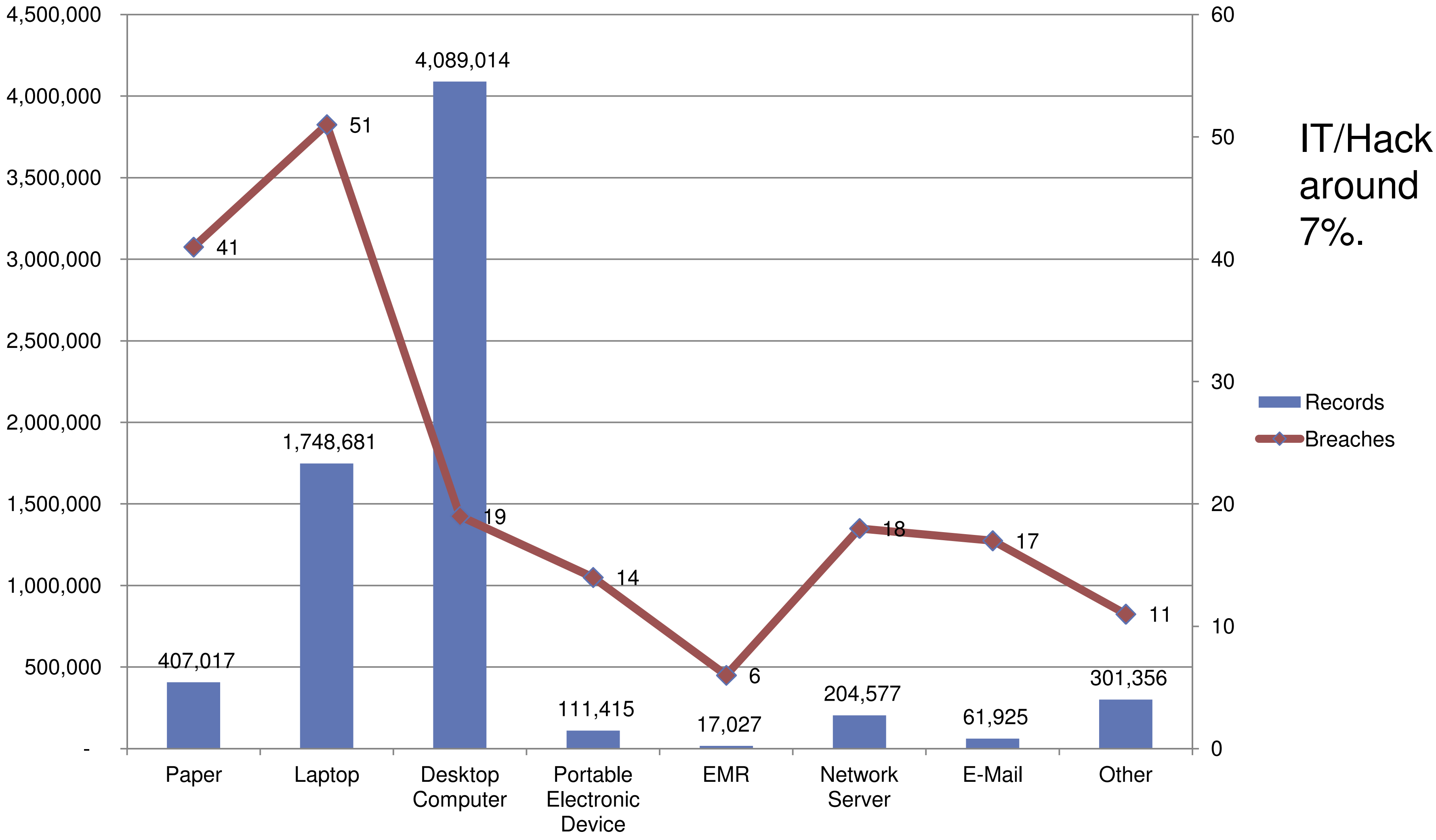
What Is The Greatest Risk to PHI & Other Regulated Data?



Source: Ponemon The Risk of Regulated Data ion Mobile Devices and in the Cloud (2014)

Booz | Allen | Hamilton

What Is Your Greatest Risk – How Do You Measure?

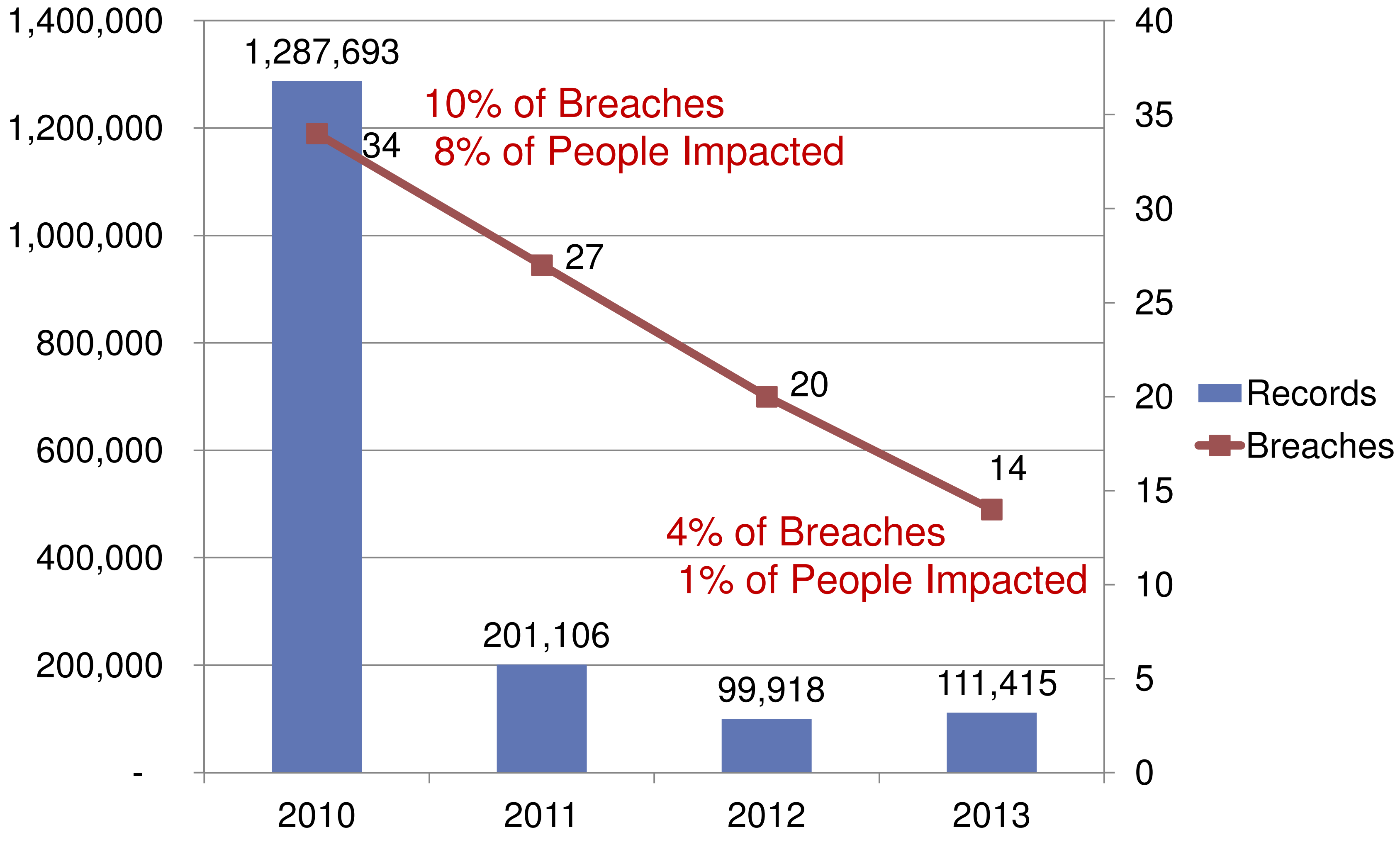


IT/Hack around 7%.

Source: US Department of Health and Human Services Office for Civil Rights

Booz | Allen | Hamilton

Portable Devices Over the Last 4 Years – Decreasing Risk?



10% of Breaches
8% of People Impacted

4% of Breaches
1% of People Impacted

Source: US Department of Health and Human Services Office for Civil Rights

Booz | Allen | Hamilton

Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

i. Know the Rules and Areas of Non-Compliance

ii. Know the Risks Specific to Your Organization

iii. Know the Data and the Flows – Internal and External

iv. Know Your Audit Process and Prepare

v. Know the Roadmap Ahead and Be Self-Aware

Revolution in HIT and New Healthcare Delivery Models

- **Health Information, IT and Sharing Revolutions.** Stimulus Bill provided funds driving healthcare information and analytics, but healthcare organizations go from 0 to 11 in IT maturity.

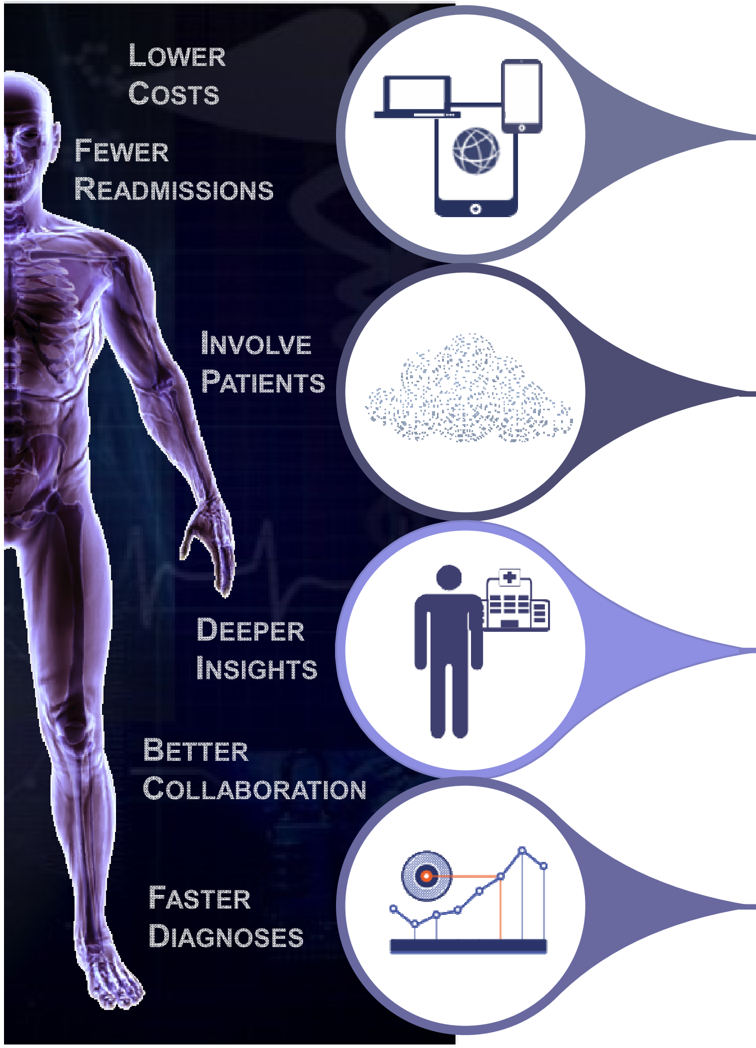
- **Care without Walls.** Healthcare using new channels and new technologies to deliver treatments – i.e. telemedicine, social media, care without walls.

- **New, but Vulnerable, Healthcare Ecosystem.** All the new data sharing and movement of data creates new capabilities and a broad set of new data privacy/security vulnerabilities.

- **More Vendors and Business Associates Needed to Enable and Support.** New business partners, business associates and independent contracts needed to deliver and host new healthcare delivery methods and new technologies.

- **New Cyber Threats Attacking Healthcare.** Many providers, payors, pharma, medical device and business associates have been the target of cyber attacks and incidents. New Cybersecurity Framework being release by NIST in 12 days. HITRUST and NH-ISAC conducting an industry cyber exercise, offering cyber monitoring services and are forums for sharing best practices.

As data becomes ubiquitous and interconnected, compliance must manage a complex and dynamic information ecosystem



Lower Costs

Fewer Readmissions

Involve Patients

Deeper Insights

Better Collaboration

Faster Diagnoses

New Ways to Connect

Engaging a broad population of people on a personal basis, wherever they are, whenever they want to connect

- Bring Your Own Device - BYOD
- Telemedicine/Mobile Health
- Networked medical devices
- Social Media
- Remote Patient Monitoring

New Types of Information

Collecting, exchanging, and communicating an exponentially growing amount of information

- Electronic Health Records
- Personal Health Information
- Financial Data
- Multi-Media
- Internet-of-things

New Care Delivery Models

Putting patients at the center of care delivery, and treating all aspects of their health, through every stage of their lives

- Patient-Centered Care
- Process Reengineering
- Population Health
- Continuum of Care
- Preventative Care

New Insights to Uncover

New analytic capabilities derived from the “Big Data” flowing through the ecosystem

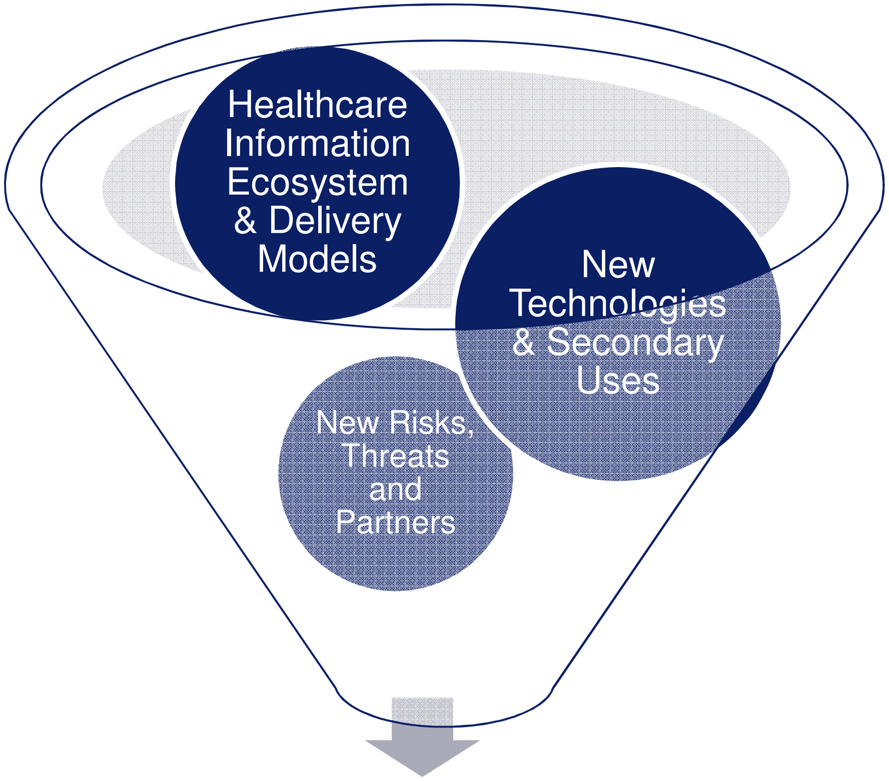
- Data Aggregation
- Clinical Analytics
- Predictive Modeling
- Population Analytics
- Real-time Analytics

New Delivery Models, New Channels and Secondary Uses Result in New Dataflows and New Business Associates/Vendors

Industry drivers:

- Stimulus Bill & Meaningful Use Funds for EHRs
- New Health Delivery and Payment Models (e.g., Telemedicine, P4P)
- New Technology (i.e., CAMS Stack – Cloud, Analytics, Mobile and Social)
- New Risks (e.g., knowledgeable insider, medical identity theft, cybersecurity, third-party/BA)

75% of Healthcare organizations indicate they have or plan to use data for secondary and new uses; **48%** have implemented privacy and security safeguards


Healthcare Information Ecosystem & Delivery Models
New Technologies & Secondary Uses
New Risks, Threats and Partners

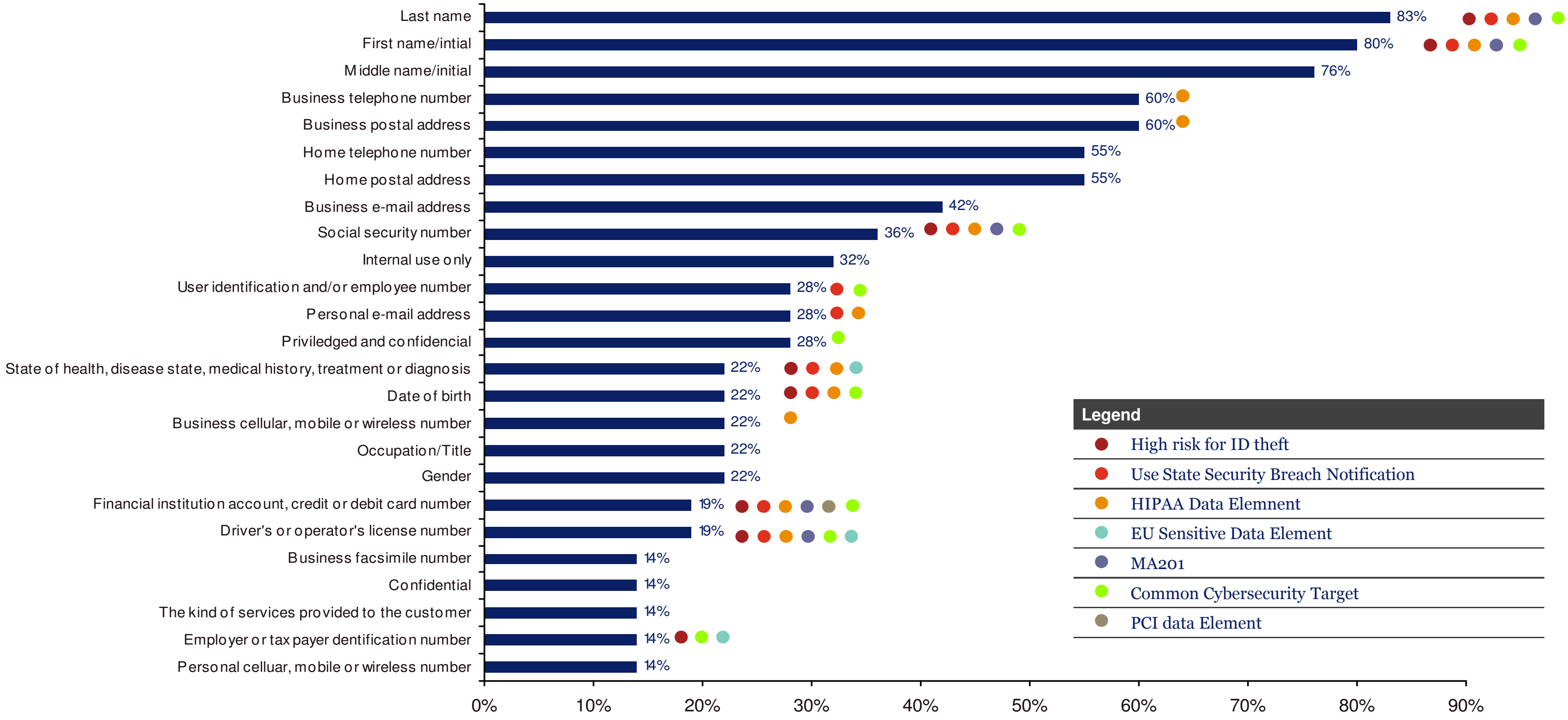
New Laws, Information Demands and New Privacy Requirements

Booz | Allen | Hamilton

Data Element Inventories Being Developed for Incident Response

Data element inventory - Top 25 data elements. Used in new 4-point test to determine if there is little chance the PHI has been compromised.

Data Element Inventory Analysis. This report inventories and analyzes the extent and locations of high-risk and regulated personal information data elements. This chart graphically represents the concentrations of high-risk and regulated personal information and information at higher risk of identity theft or cybersecurity attack across the organization.



What Others Are Doing

- Data mapping
- Data use and data element inventories
- Enhancing BAs with minimum security provisions, pre-contract assessments and post-contract audits
- Updating Incident response plans
- Enhancing access controls and access monitoring
- Building cyber capabilities

Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

   i. Know the Rules and Areas of Non-Compliance
   ii. Know the Risks Specific to Your Organization
   iii. Know the Data and the Flows – Internal and External
   iv. Know Your Audit Process and Prepare
   v. Know the Risks Specific to Your Organization

So You Got a Letter . . . A Few Tips for Audit Success

Process

- **Prepare.** Many organizations conduct mock audits or other exercises to prepare and practice.

Documentation

- **Omnibus Rule Update.** Ensure that the documentation for Programs is reviewed and updated, as necessary, to comply with the new Omnibus Rule requirements. Continue to monitor communications from OCR for revisions to the Protocol based on Omnibus.

- **Mapping of Documentation.** Map policy documents to the specific areas of the document request list from OCR. The mapping document furnished along with Program documentation is helpful.

- **Include a Log of Revisions/Updates.** The policies and procedures can include a revision history at the end of each document that provides a log of each revision/update that was made over time.

So You Got a Letter . . . A Few Tips for Audit Success (cont.)

Interviews

- **Prepare Responses for 10 Key Topics.** We suggest focusing preparations and responses for, at a minimum, each topic below. Note, this is not an OCR list.

  1. Business Associates
  2. Training
  3. Sanctions
  4. Minimum Necessary Use
  5. Accounting for Disclosures
  6. Authorizations
  7. Incident Response
  8. Breach Tracking/Analysis/Notification
  9. Notice of Privacy Practices
  10. Physical Security

- **Pay Attention to Trends.** Watch (i) OCR trends and compliance protocol changes, (ii) common areas of non-compliance and (iii) areas of enforcements and breaches.

So You Got a Letter . . . A Few Tips for Audit Success (cont.)

Interviews

- **Tell the Story - Emphasize Strengths of the Plan Programs.** Identify in advance and stress a number of strengths and tools to promote culture of compliance and maturity to the OCR auditor -- (i) training, (ii) assessments for BAs; (iii) data sharing/governance programs; (iv) processes for obtaining authorizations and delivering NPPs; and (v) incident response.
  - Provide prepared responses and emphasize strengths early in discussion.
  - Use questions to discuss program approach, not limited confirmations.

- **Interview Responses Should Be Truthful, Direct, and Concise.** All questions from the OCR auditors should be answered truthfully, directly, and concisely. Interviewees should be cautious of over-answering.

- **Know the Audience and Avoid Acronyms.** OCR auditors will have varying levels of experience with respect to health industry business operations and regulatory compliance requirements and programs.
  - Interviewees should be prepared to provide simple, brief backgrounds of industry and operations if necessary.
  - The use of acronyms and industry jargon should be avoided.

Table of Contents

I. The Audits, Protocols and Enforcements

II. Lessons Learned - Five Things You Need to Know Now

   i. Know the Rules and Areas of Non-Compliance

   ii. Know the Risks Specific to Your Organization

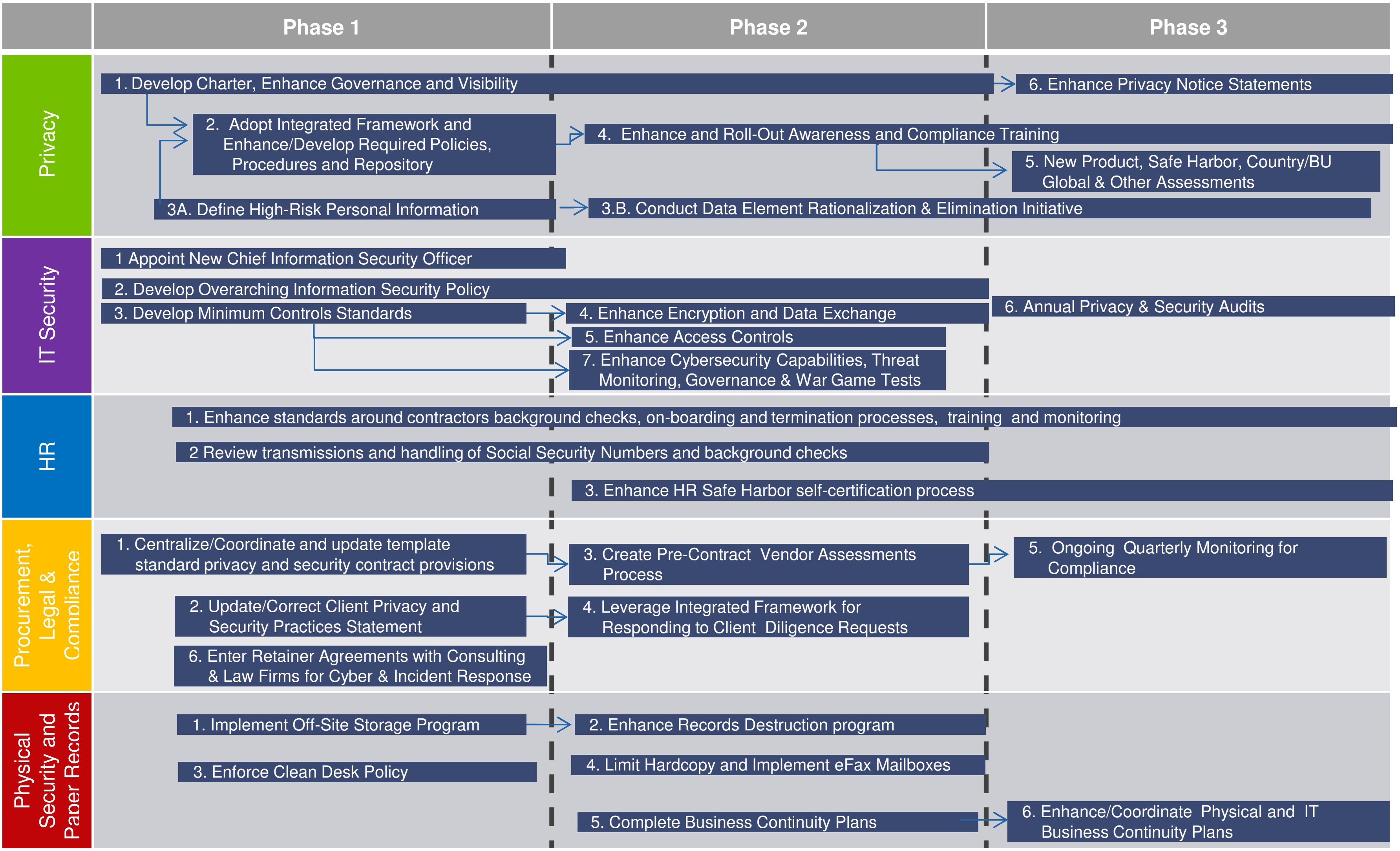
   iii. Know the Data and the Flows – Internal and External

   iv. Know Your Audit Process and Prepare

   v. Know the Roadmap Ahead and Be Self-Aware

Integrated Privacy & Security Program Initiative Roadmap - The Secret Sauce – A Risk Management Plan You Follow

This page sets forth a typical, illustrative Gantt chart roadmap illustrating how such initiatives are typically coordinated/timed and the related key dependencies typically in 18 months, but can be accelerated to 12 months or spread over 24 months).



Phase 1

Phase 2

Phase 3

Privacy

1. Develop Charter, Enhance Governance and Visibility

6. Enhance Privacy Notice Statements

2. Adopt Integrated Framework and Enhance/Develop Required Policies, Procedures and Repository

4. Enhance and Roll-Out Awareness and Compliance Training

5. New Product, Safe Harbor, Country/BU Global & Other Assessments

3A. Define High-Risk Personal Information

3.B. Conduct Data Element Rationalization & Elimination Initiative

IT Security

1 Appoint New Chief Information Security Officer

2. Develop Overarching Information Security Policy

3. Develop Minimum Controls Standards

4. Enhance Encryption and Data Exchange

6. Annual Privacy & Security Audits

5. Enhance Access Controls

7. Enhance Cybersecurity Capabilities, Threat Monitoring, Governance & War Game Tests

HR

1. Enhance standards around contractors background checks, on-boarding and termination processes, training and monitoring

2 Review transmissions and handling of Social Security Numbers and background checks

3. Enhance HR Safe Harbor self-certification process

Procurement, Legal & Compliance

1. Centralize/Coordinate and update template standard privacy and security contract provisions

3. Create Pre-Contract Vendor Assessments Process

5. Ongoing Quarterly Monitoring for Compliance

2. Update/Correct Client Privacy and Security Practices Statement

4. Leverage Integrated Framework for Responding to Client Diligence Requests

6. Enter Retainer Agreements with Consulting & Law Firms for Cyber & Incident Response

Physical Security and Paper Records

1. Implement Off-Site Storage Program

2. Enhance Records Destruction program

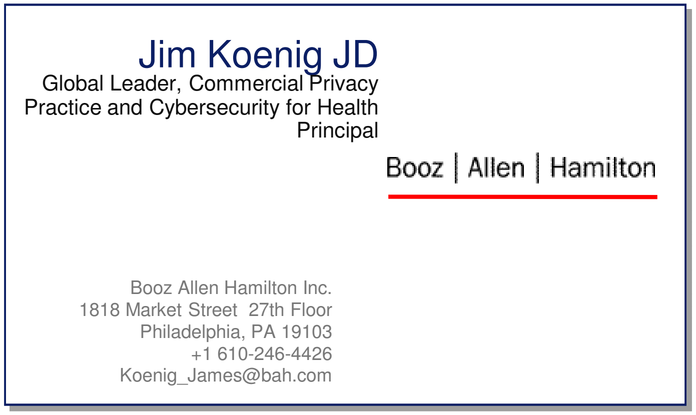
3. Enforce Clean Desk Policy

4. Limit Hardcopy and Implement eFax Mailboxes

5. Complete Business Continuity Plans

6. Enhance/Coordinate Physical and IT Business Continuity Plans

Contact for Inquiries



Jim Koenig JD
Global Leader, Commercial Privacy
Practice and Cybersecurity for Health
Principal

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
1818 Market Street 27th Floor
Philadelphia, PA 19103
+1 610-246-4426
Koenig_James@bah.com