APPLICATION SECURITY, INC.

“HIPAA-Proof” Your Healthcare Data: Safeguards at the Database Level

Ted Julian
VP Marketing & Strategy
Application Security Inc.

Agenda

- HIPAA requirements
- HIPAA Safeguards and Databases
- How To Ground HIPAA Compliance in Databases
  - Vulnerability Management – Establish Safeguards
  - Activity Monitoring – Flag Safeguard Compromise
- Summary

HIPAA Requirements

- Privacy Rule - data that relates to:
  - Past, present, or future medical condition
  - Provision of health care
  - Past, present, or future payment
  - Requires consent and notification
- Security Rule
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
  - Organizational Requirements
  - Policies and Procedures

HIPAA Admin Safeguards

Administrative Safeguards (164.308)	
Section / Standard	**Implementation Specifications**
164.308 (a) (1) – Security Management Process	Risk Analysis ®, Risk Management ®, Sanction Policy ®, Information System Activity Review ®
164.308 (a) (2) – Assigned Security Responsibility	®
164.308 (a) (3) – Workforce Security	Authorization and/or Supervision (A), Workforce Clearance Procedure Termination Procedures (A)
164.308 (a) (4) – Information Access Management	Isolating Health care Clearinghouse Function ®, Access Authorization (A), Access Establishment and Modification (A)
164.308 (a) (5) – Security Training and Awareness	Security Reminders (A), Protection from Malicious Software (A), Log-in Monitoring (A), Password Management (A)
164.308 (a) (6) – Security Incident Procedures	Response and Reporting ®
164.308 (a) (7) – Contingency Plan	Data Backup Plan ®, Disaster Recovery Plan ®, Emergency Mode Operation Plan ®, Testing and Revision Procedure (A), Applications and Data Criticality Analysis (A)
164.308 (a) (8) – Evaluation	®
164.308 (b) (1) – Business Associate Contracts and Other Arrangement	Written Contract or Other Arrangement ®

® = Required, (A) = Addressable

HIPAA Technical Safeguards

TECHNICAL SAFEGUARDS (164.312)	
Section / Standard	**Implementation Specifications**
164.312 (a) (1) – Access Control	Unique User Identification ®, Emergency Access Procedure ®, Automatic Logoff (A), Encryption and Decryption (A)
164.312 (b) – Audit Controls	®
164.312 (c) (1) – Integrity	Mechanism to Authenticate Electronic Protected Health Information (A)
164.312 (d) – Person or Entity Authentication	®
164.312 (e) (1) – Transmission Security	Integrity Controls (A) Encryption (A)

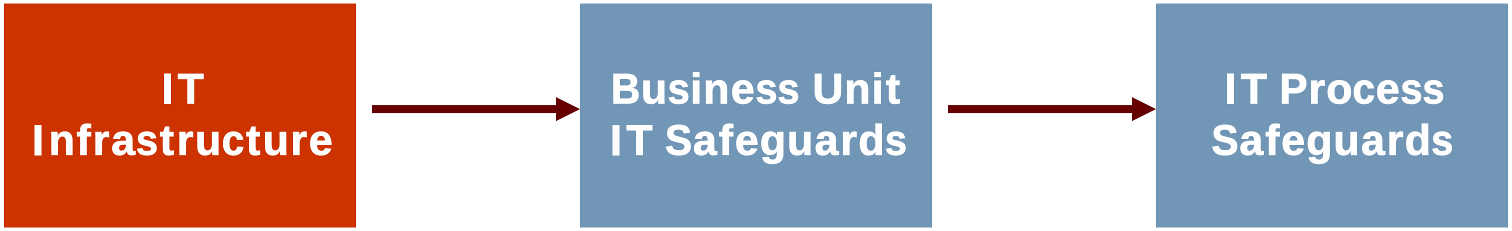
® = Required, (A) = Addressable

HIPAA Safeguard Methodology

Avoid one-offs:

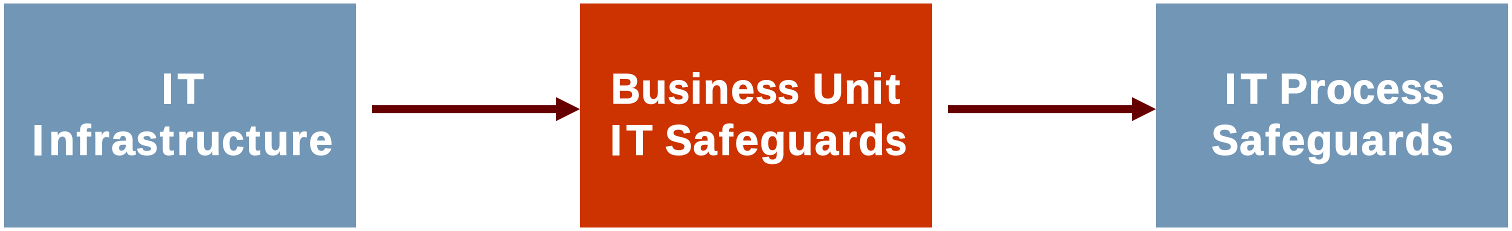
- Consider broader security control / safeguard frameworks
- Make HIPAA controls / safeguards part of this broader framework
- ISO 27001 (formerly ISO 17799) is pretty popular

HIPAA Safeguard Methodology



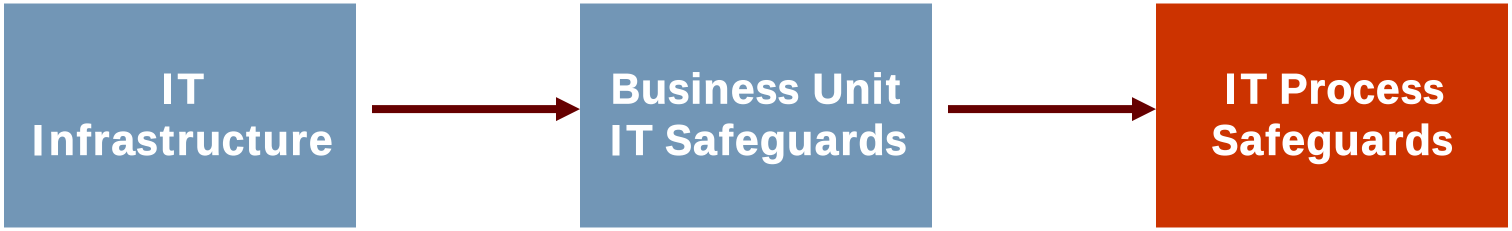
- Understand IT management & organization
- Blueprint IT infrastructure
- Identify business units that hold patient data
- Develop strategy for administering technology and applications at these business units

HIPAA Safeguard Methodology



- Identify separate application and data owners
- Evaluate IT controls and monitoring
- Engage in risk assessment of controls and monitoring

HIPAA Safeguard Methodology



- General IT process
- Application and data owner process
- Integrated application-specific process

Common Threat to HIPAA

UNAUTHORIZED PATIENT RECORD DELETION, MODIFICATION OR ACCESS

Q1: Where are patient records?

A: in transit over the network

B: on a general-purpose host

C: in a database

Are Databases Vulnerable?

	Oracle	MS SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	☑	☑	☑	☑	☑
Denial of Services & Buffer Overflows	☑	☑	☑	☑	☑
Misconfigurations & Resource Privilege Management	☑	☑	☑	☑	☑

Any Breaches?

Company / Organization	# of Affected Customers	What Was Breached	Date of Disclosure
TJX	???	DB	17-Jan-07
UCLA	800,000	DB	21-Nov-06
AT&T	19,000	DB	29-Aug-06
Debit card compromise (OfficeMax?)	200,000	DB	9-Feb-06
Card Systems	40,000,000	DB	17-Jun-05
Citigroup	3,900,000	TP	6-Jun-05
DSW Shoe Warehouse	1,400,000	DB	8-Mar-05
Bank of America	1,200,000	TP	25-Feb-05
LexisNexis	310,000	??	9-Mar-05
ChoicePoint	145,000	n/a	15-Feb-05

Total Affected Records - ’05-present: 100+ million

Source: Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm

Any Breaches?

- Breaches of privacy at insurers and other payers went up from 45 percent last summer to 66 percent in January.
- Most respondents experienced between one and five breaches, but 20 percent reported six or more.
- Yet, Security Rule compliance remains low:
  - Though the deadline passed over a year ago, 80% of payers and only 56% of providers have implemented the Security standards.
  - Of those claiming full compliance, many “compliant” Providers and Payers could not confirm that they had implemented all key Security standards.

Source: bi-annual Phoenix Health Systems and HIMSS study, April & October 2006

Any Breaches?

- Less than 25% of the 22,964 privacy complaints submitted between April 2003 and September 2006 were investigated
- Of the 5,400 investigated complaints, informal action was taken in 3,700 of the cases.
- In the other 1,700 investigated complaints, the accused health care organizations were pardoned

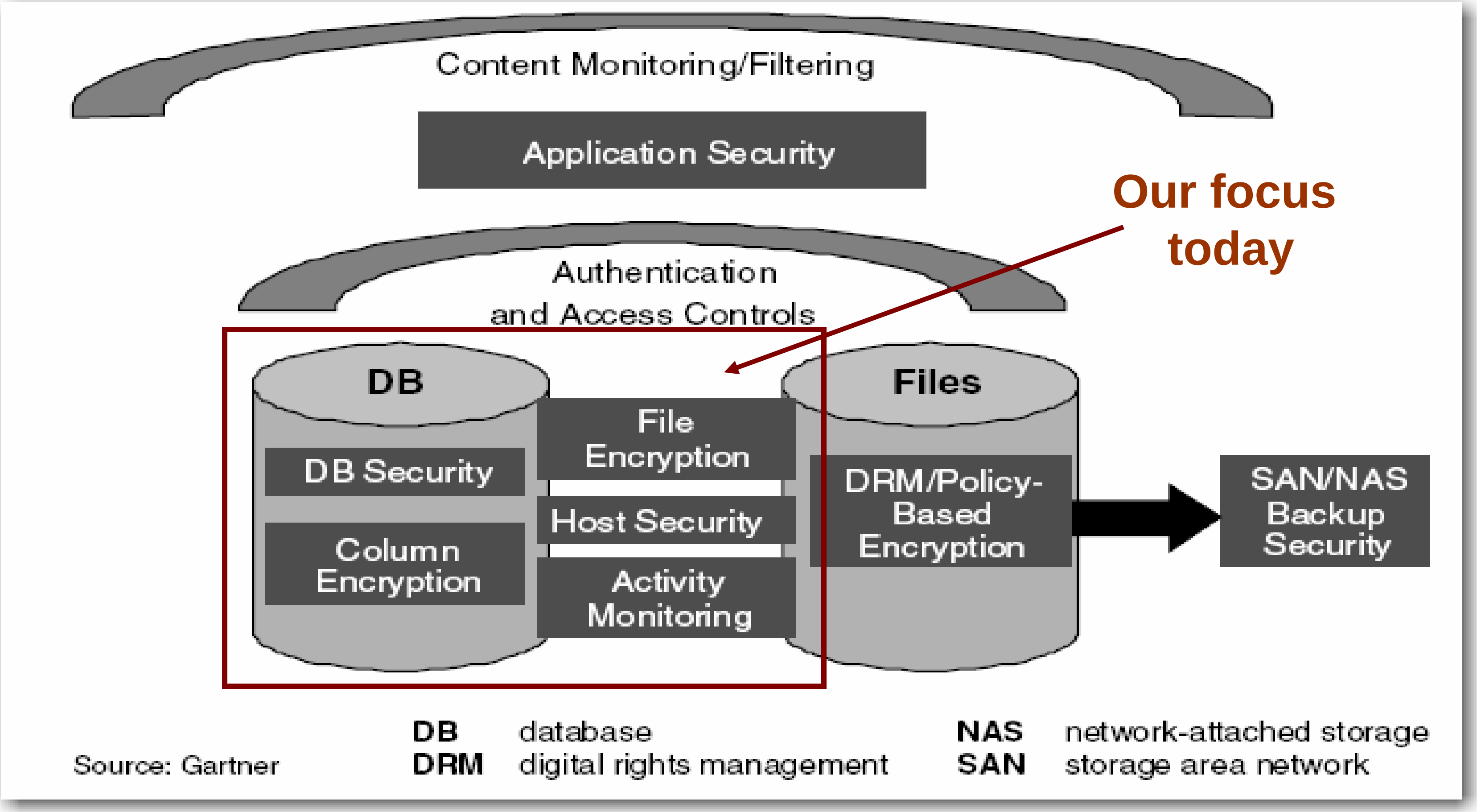
Source: The 3rd Annual Review of Medical Privacy and Security Enforcement, January 2007

Forrester on HIPAA & Data

- Forrester predicts protecting databases for HIPAA, including non-production, “will become a key requirement…all personal information (PI) and personal health information (PHI) in any data repository or file be secured at all times, and only privileged users should have access” [1]

[1] Source: “Trends 2006: DBMS Security,” Forrester Research, Nov 2005

Gartner on HIPAA & Data



Our focus today

Source: Gartner

DB	database	**NAS**	network-attached storage
DRM	digital rights management	**SAN**	storage area network

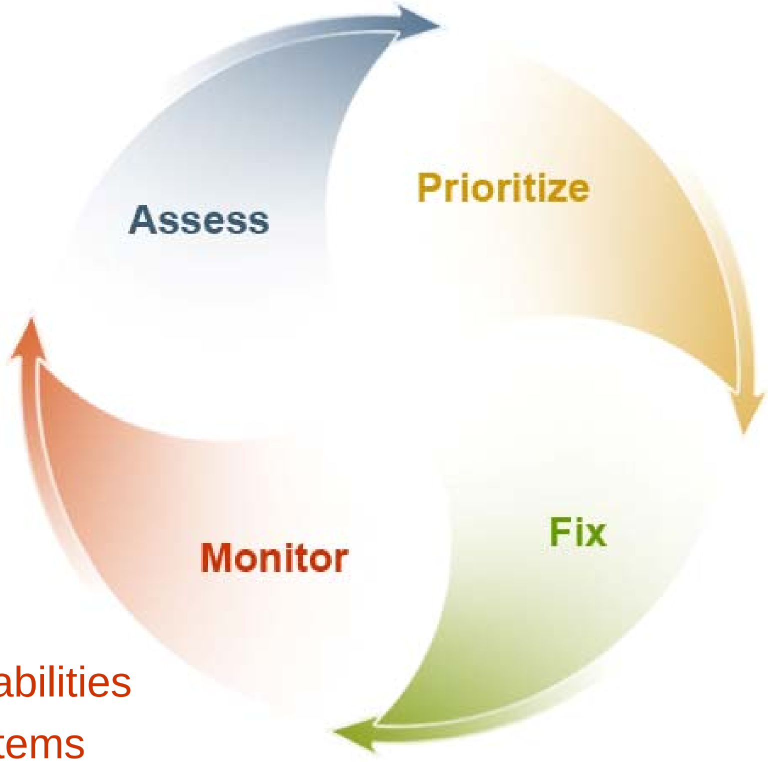
HIPAA & Databases

- Yikes! What can we do!? How can we:
  - establish safeguards on the database
  - tighten security on the crown jewels
  - ground HIPAA compliance in our databases

Grounding HIPAA In the Db

Apply the vulnerability management lifecycle...

- Inventory assets
- Identify vulnerabilities
- Develop baseline

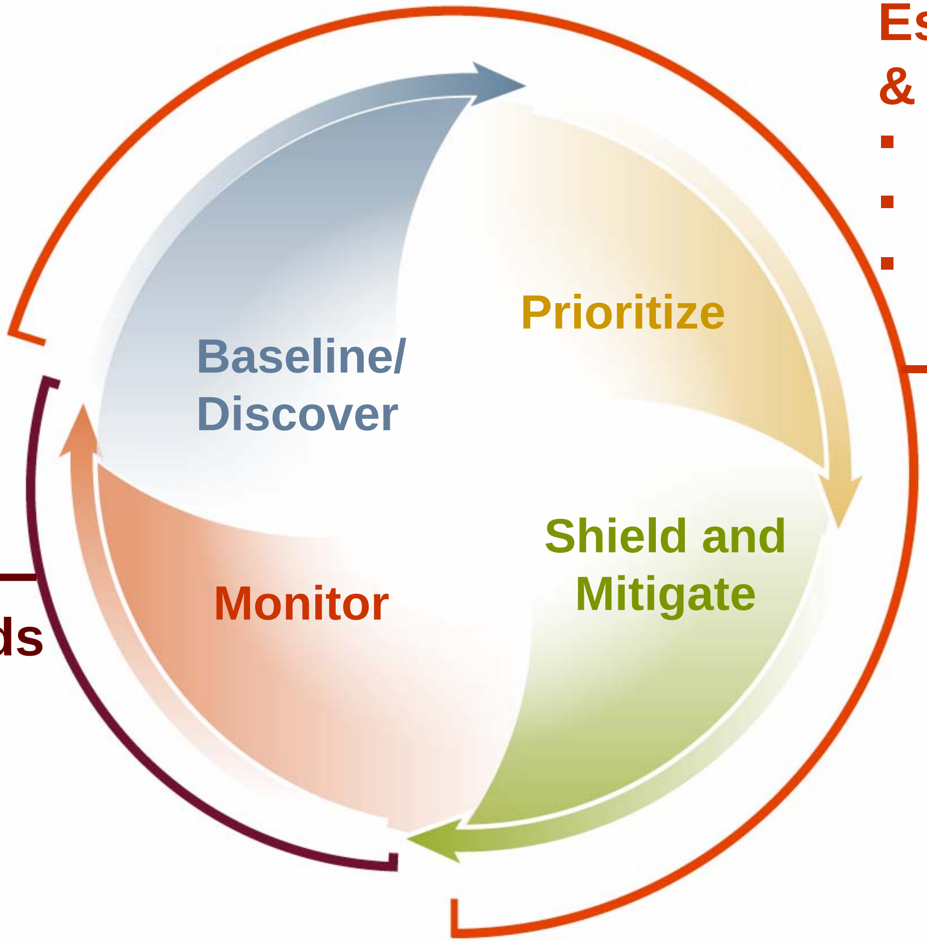


- Prioritize based on vulnerability data, threat data, and asset classification
- Document security plan

- Monitor known vulnerabilities
- Watch unpatched systems
- Alert other suspicious activity

- Eliminate high-priority vulnerabilities
- Establish controls
- Demonstrate progress

Grounding HIPAA In the Db



Establish Safeguards & Track Progress

- Document systems
- Establish controls
- Demonstrate continuous improvement

Monitor Safeguards & Flag Violations

- Who did it?
- What did they do?
- When did they do it?

Real-time Activity Monitoring

Five Components of Activity Monitoring

Auditing Component	What Is It?	Why Do It?
Access & Authentication	What systems were accessed, when, and how	Establish system controls and gather system information
Users & Administrators	Who did it and what did they do	Establish user controls and gather user information
Suspicious Activity	Flags misuse	Insider threats
Vulnerability & Threat	Identifies threats	External threats
System Changes	Baselines desired state, flags variations	Maintain controls & flag misconfigurations

Vuln Mgmt Process Benefits

- Common agreement on safeguards
- Start with simple stuff
- Add more safeguards and more systems over time
- Easy to demonstrate continuous improvement

Summary: HIPAA To The Db

- There are no silver bullets that bring HIPAA safeguards to the database
- Vulnerability management and activity monitoring can help
  - aligns with existing people, process, and technology
  - solutions can automate the process
- End result is significant:
  - Security for the crown jewels
  - Repeatable and demonstrable HIPAA compliance, grounded in the database

For More Information:

Ted Julian

VP Marketing & Strategy

Application Security Inc.

tjulian@appsecinc.com

http://www.appsecinc.com

APPLICATION
SECURITY, INC.

Thank you!