Protecting Health Data Some Practical Suggestions

Paul L Petronelli
CTO/Medifies, Inc.
paul@medifies.com
(408) 582-8056

May 22-23
Health Technology Forum
Stanford, Ca

v.FINAL

Agenda

- Background and justification
- Guidance from responsible organizations
- How to use the guidance
- Summary

Target Audience

- Product developers, operations team

Many thanks to member of HL7 Mobile Healthcare subcommittee for providing the motivation. If you are interested in joining in, see the wiki : http://wiki.hl7.org/index.php?title=Mobile_Health

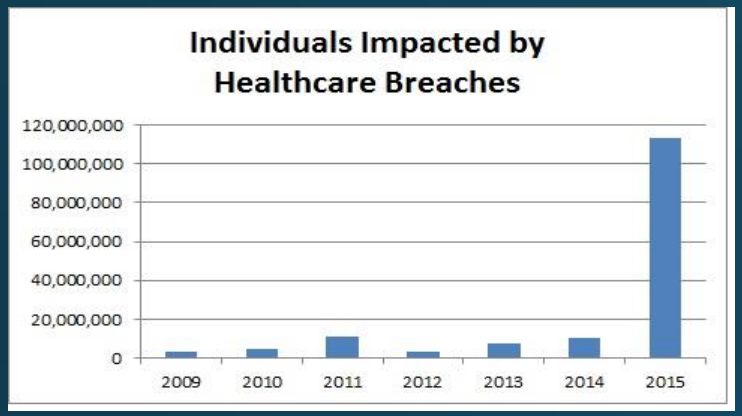
Why is this topic important

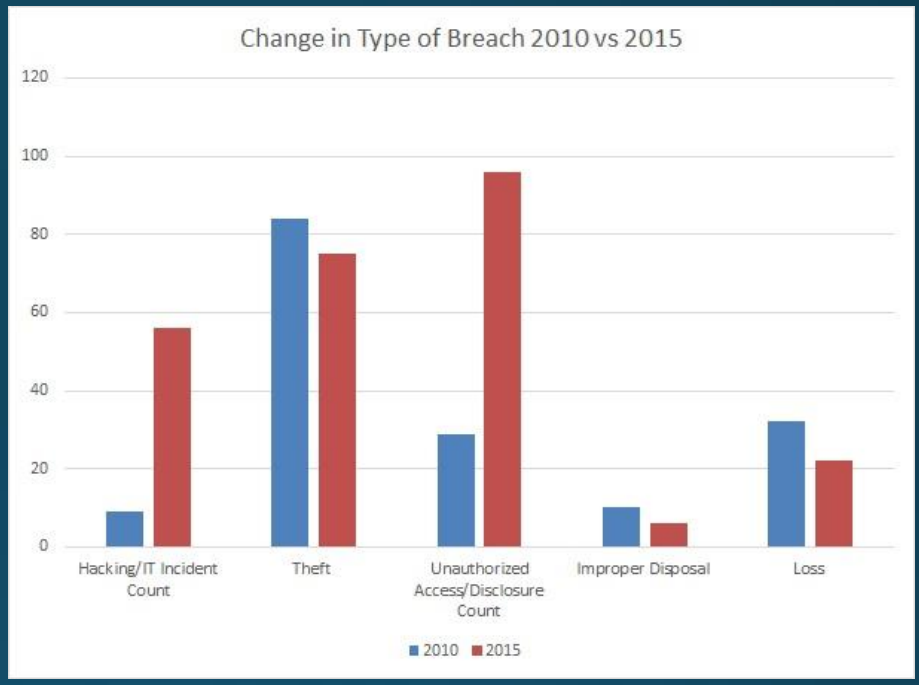
- Moral and ethical obligation to safeguard the information entrusted to our applications
- Fiduciary obligation when breaches occur
  - Cost of breach reported at ~$363 per record (across all institutions) *
- 89 Percent of Organizations Experienced Data Breaches (healthcare institutions)**
- The "value" of stolen PHI vs credit card identity is 10X (see Reuters : http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

*Ponemon Institute annual ***Cost of Data Breach Study: Global Analysis***, sponsored by IBM. See http://www.ponemon.org

**ibid, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016

Quick look at recent breach trends





Gartner Group references:

- Notice the changes in types of breaches – increase in hacking theft and criminal actions
  - See: http://blogs.gartner.com/jack-santos/2016/01/07/2015-healthcare-breach-trends-the-wild-west-of-healthcare-data

Run your own report at the HHS Breach Portal:

- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How to “protect”

- Implement security in products we develop
- Judicious management of sites and services
- Diligence in execution
- Encryption
- Site security
- Application safeguards
- Organizational processes

Guidance

There is ample guidance in the public literature. Some sources follow:

Authoritative guidance

- ONC
- HHS
- HIPAA
- NIST
- FIPS
- FTC

Internet Guidance

- OWASP (Top 10) "Open Web Application Security Project"

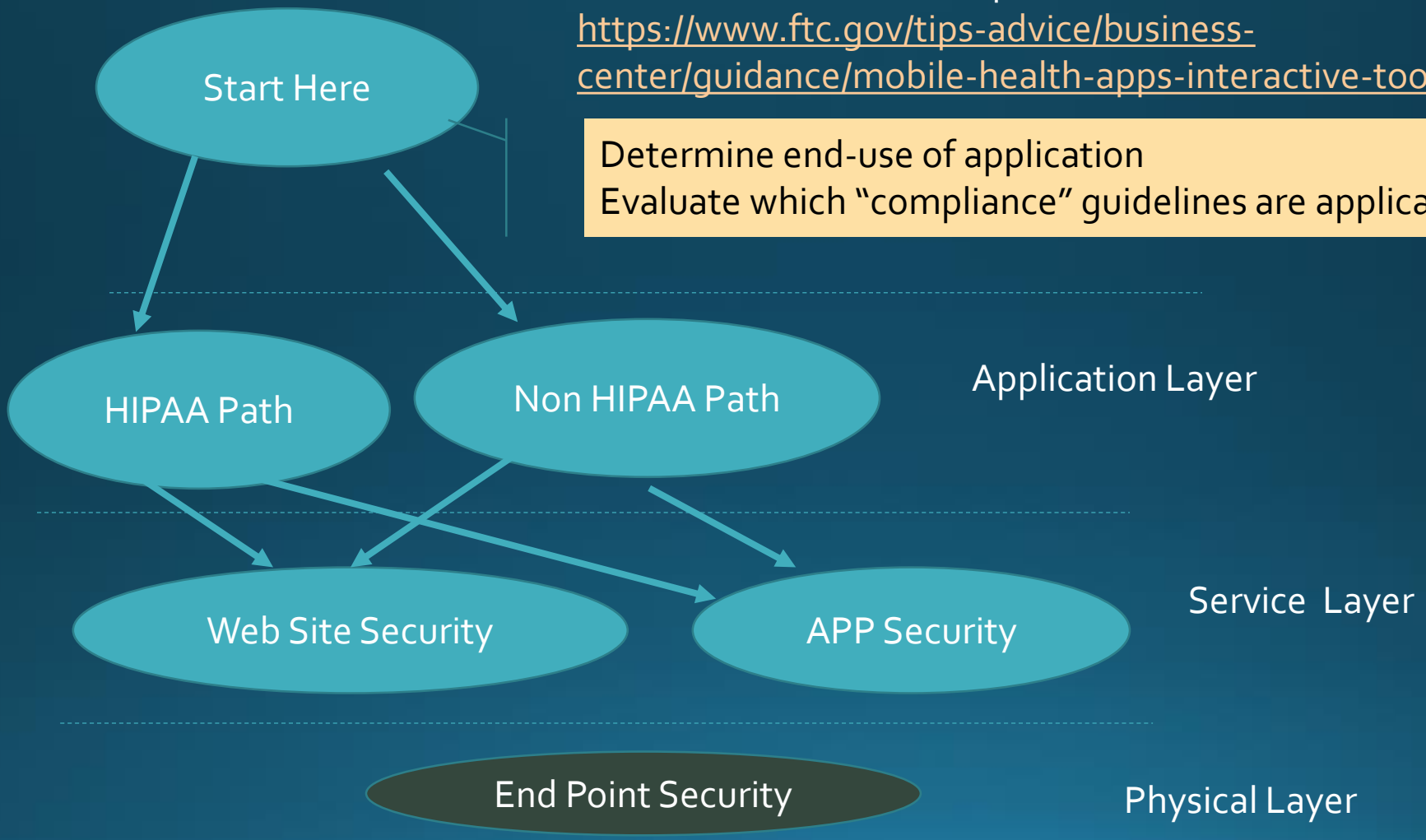
Suppliers guidance

- Cloud suppliers
- EHR vendors
- Device suppliers

Practical Process

FTC/ONC/OCR/FDA Compliance check list:
https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

Determine end-use of application
Evaluate which "compliance" guidelines are applicable



Authoritative Guidelines

- At Rest Guidance- HHS: NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
- Data In motion guidance – FIPS 140-2 validated.
  - HHS: NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs
- Data purge: NIST Special Publication 800-88, Guidelines for Media Sanitization
- Architectural: NIST: Framework for Improving Critical Infrastructure Cybersecurity , Version 1.0 , February 12, 2014

Vendor HIPAA Guidelines

Amazon

- Ref: Architecting for HIPAA Security and Compliance on Amazon Web Services, Amazon Web Service, 2015
- Amazon Web Services: Overview of Security Processes , Amazon Web Services , 2015

Microsoft

- Microsoft Azure HIPAA/HITECH Act Implementation Guidance

Google

- HIPAA Compliance & Data Protection with Google Apps

How to use guidance documents

Role	Usage
Architect	Understand guidance
Designer	Decide on approach
Implementer	Consider whether each approach introduces a vulnerability
Operations	Review vulnerabilities and exploits such as found in OWASP and other sources

Then conduct your own Risk Assessment here:
www.HealthIT.gov/security-risk-assessment

Snapshots* from Practice

Attacks

- Institutions are witnessing "phone calls from IT" requesting password, etc.
- The most vulnerable point in a system is the human, or "soft target"
  - Subject to Phishing emails
  - Phone calls
- Advance Persistent Threat (APT) used to be only in government networks, now the criminal and organized threats attacking healthcare institutions

Safeguards

- Assume there will be a breach and prepare for it (not *if* but *when*)
- Never assume anything inside the corporate firewall is safe

*Informal survey. Your results may vary and 'values' change frequently.

Further Snapshots from Practice

Countermeasures

- NIST recommends AES, not DES and 128 bit key. For RSA 2048 bit key
  - In practice, AES 256 used instead of AES 128
- Internal training applies to all employees not just IT
  - Guard against device loss and unattended devices
  - Increase awareness of sensitivity of data being handled

Operational Measures

- OWASP 'top 10 ' is updated on an annual basis – schedule a periodic reassessment
- Planting of "honey pots" to attract malicious attackers
- Network Segmentation
  - SDN is a technology to enforce this approach

Process Suggestions for Product Users

Ask yourself: " how can our customers use the features/tools/and visibilities in our products to satisfy their security requirements?"

To increase organizational sensitivity to security issues, integrate security concerns into the organizational structure and processes

- Perform Risk Assessment
- Document and inventory PHI
- Develop PHI Security Strategy
- Educate and train employees
- Implement processes, technologies and policies
- Establish an incident response plan and team

By Michelle McNickle, reporting on ID Experts opinions in HealthCare IT News, Sept 30, 2011

Summary

- Many cases a matter of diligence, persistence and methodology
- Raise the level of sensitivity to security issues
- Integrate security planning into product development process along with other system engineering activities
- Address security in multiple layers
- Prepare the organization for a possible breach
  - Establish an incident response team
- Air Force motto: "readiness is our business" can be applied to health informatics systems