Microsoft

OCR NIST HIPAA Security Rule Conference

Microsoft in Health
Eric Mueller, Chief Healthcare Solutions/Product Strategist
Vince Johnson, Technical Sales Professional, Client
Microsoft Health & Life Sciences

May 22, 2013

Today's topics

- Data access best practices

- DR planning / readiness

- Healthcare data

- Devices

- Best practices

- What is Microsoft doing to support HIPAA

OCR / NIST HIPAA Security Rule conference

Understanding the Challenge

IHI Triple Aim Initiative
Better Care for Individuals, Better Health for Populations, and Lower Per Capita Costs

At Microsoft Health and Life Sciences, we believe in the Institute for Health Improvement's (IHI) Triple Aim framework (http://www.ihi.org/offerings/Initiatives/TripleAim) to optimizing health system performance. New designs must be developed to simultaneously pursue the three dimensions of healthcare transformation called the "Triple Aim".

1. Improving the patient experience of care (including quality and satisfaction)
2. Improving the health of populations
3. Reducing the per capita cost of health care

This challenge continues to escalate around the world.

Microsoft believes and continues to develop devices, software services, solutions, and strategies that are key components of these new designs. By partnering with the healthcare ecosystem at large, Microsoft enables our customers to focus on patients and results that enable an entire ecosystem of integrated devices, software services and solutions.

Microsoft in Health

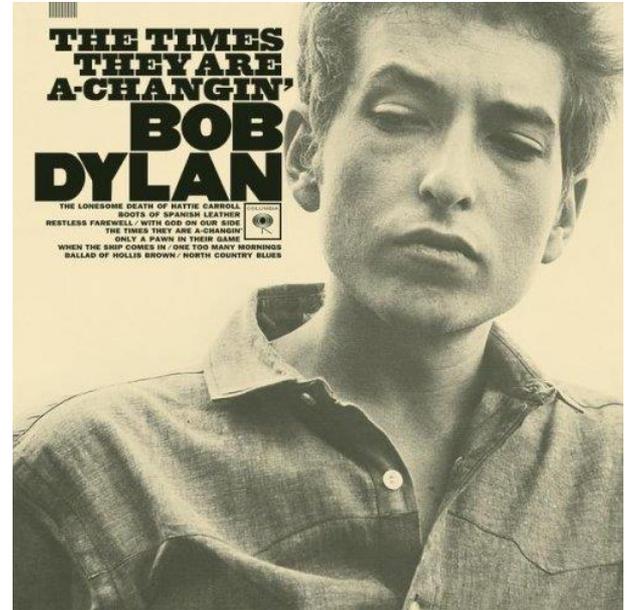Microsoft

How do you view Security?
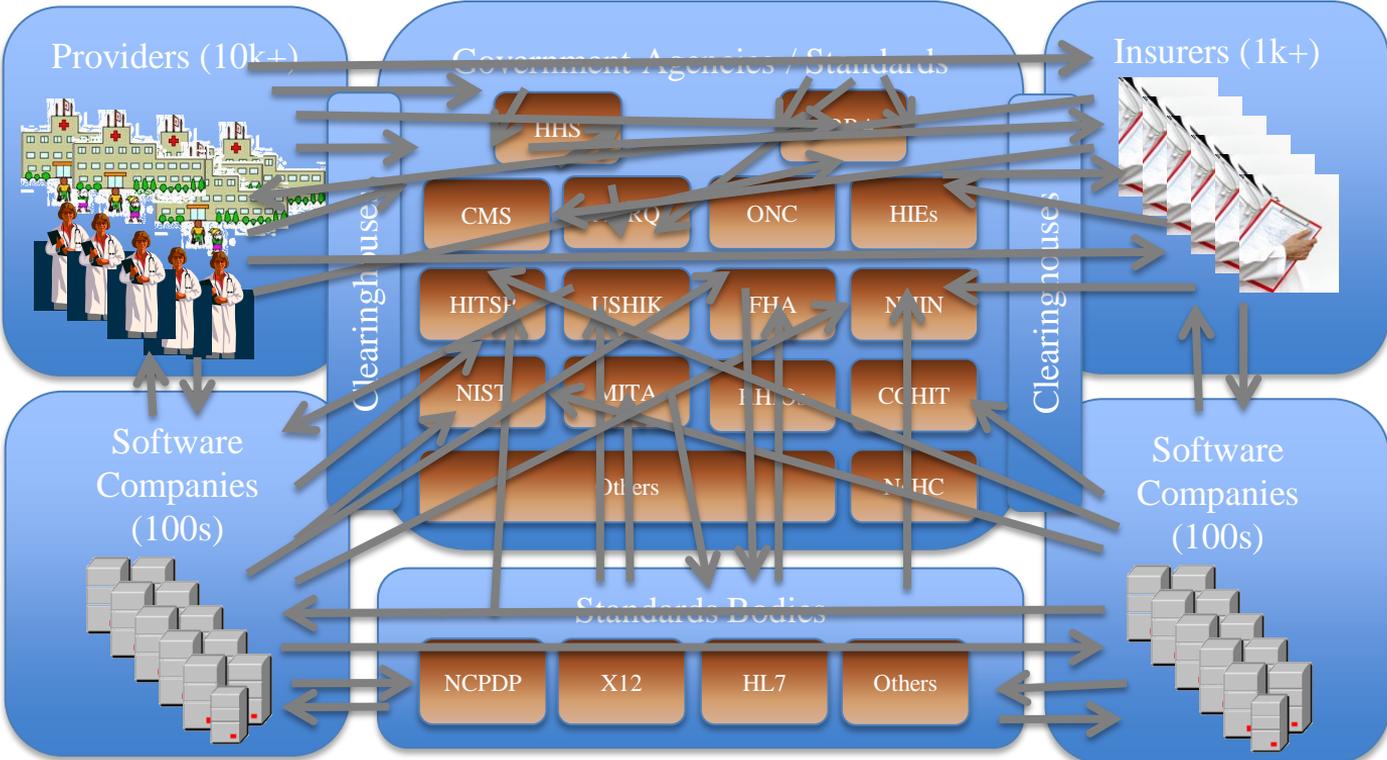
How do your users view security?

Microsoft in Health
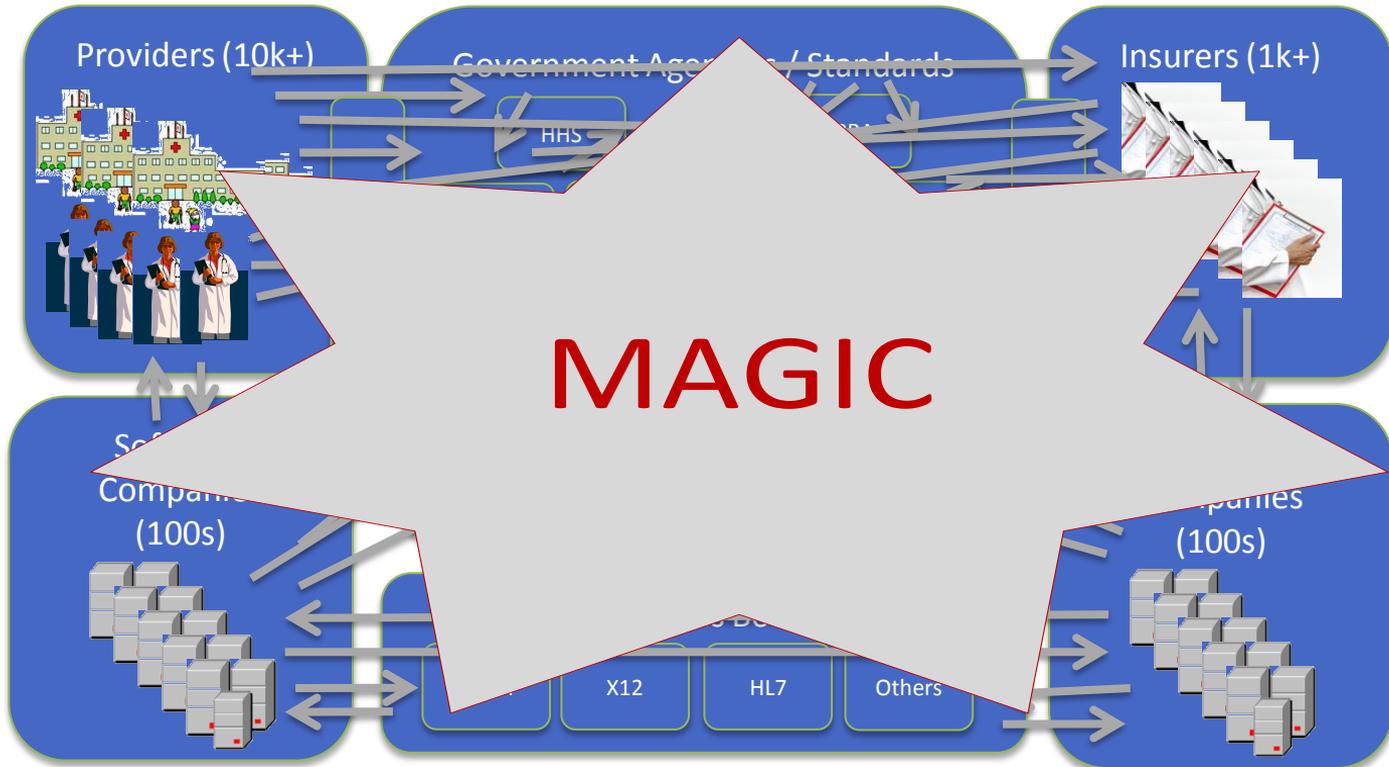
The State of Security

In the past, the cost of compliance was higher than the cost of the fines

That was then….

Microsoft in Health

ePHI Breaches Consume the HeadLines

From FierceITHealth

- Lost USB drive compromises info for Medicaid recipients

- Louisiana hospital breach impacts more than 8,300 patients

- Implanted cardiac devices could be subject to tampering

- Across the U.S., healthcare organizations suffer data breaches

- VA medical center faces lawsuit after data breach

- Healthcare organizations leaving themselves open to breaches

Microsoft
in Health

You may be surprised who has access to PHI....

Microsoft
in Health

Allowing and Monitoring ePHI Access

1. Appoint Data Custodians for specific Job roles
2. Granting and Auditing Access to ePHI
   a) User Accounts
   b) Failed Login Attempts
   c) Administrator Account
   d) User Account Lifecycle
   e) User Notifications of Data and Network Use
3. Improper Data/Network Use Formal Sanctions
   a) Accountability
   b) Employee handbooks
   c) Social Engineering
   d) Training Security Awareness
4. Proper Access of ePHI Monitoring
   a) Awareness of sensitive data

Microsoft
in Health

Story #2 – Who are you handing your information too?

Disaster Recovery - Think about who is helping you through a crisis.

Microsoft
in Health

Managing Security During a Disaster

1. DR Planning
   a) Emergency Data Access
   b) Hot/Warm/Cold site planning
   c) Cloud Planning
   d) Business Associates
2. Hardware Support
   a) Disposition of Hard Drives with ePHI
   b) Disposition of Electronic media
3. Data Retention Process
   a) Archived
   b) Deleted

Microsoft in Health

Know the value of your data

Why is patient data valuable?

Microsoft
in Health

Assign Responsible Party to Secure Data

1. Appoint Data Custodian
2. Documenting and Responding to Security Incidents
3. Security Patching
4. Software certification policies (versioning, and maintenance)
5. Consequences of Outdated software

Figure 2 Data governance framework

CONFIDENTIAL

Microsoft
in Health
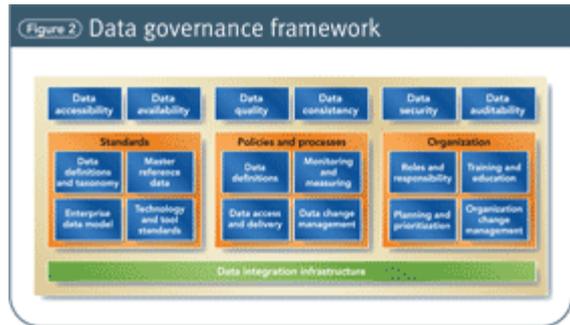
Devices.....

Devices are here.....

- Laptops, tablets, mobile devices
- Best practices should be consistent throughout
- Story about examples....

Microsoft
in Health

Are devices outpacing your security?

Add some punch……

- Laptops, tablets, mobile devices
- Best practices should be consistent throughout
- No governance is not acceptable

Microsoft
in Health

Bring Your Own Device (BYOD)

How do you stand?

- What's the best practice
- Whose device is it?
- Am I really saving costs?

Microsoft
in Health

Securing Devices

1. HIPAA, USGCB, DoD GPOs
2. Encrypt Data at Rest (thumb drives, Database Encryption)
3. Client Server Network Encryption
4. Web Encryption and Security
5. File level vs. folder level encryption
6. Device Governance (Desktops vs. laptops vs. handhelds)
7. Anti-Virus/Malware/Network Intrusion
8. Security Compliance Manager 3.0

Microsoft
in Health

Q&A

mshug.org

Microsoft

Real Impact for Better Health
www.microsoft.com/health

OCR / NIST HIPAA Security Rule conference

Microsoft
in Health