IT Security in a Meaningful Use Era

C&SO HIMSS Meeting

Presented by:

Mac McMillan
CEO CynergisTek, Inc.
Chair, HIMSS Privacy & Security Task Force

Discussion Guide

Introduction

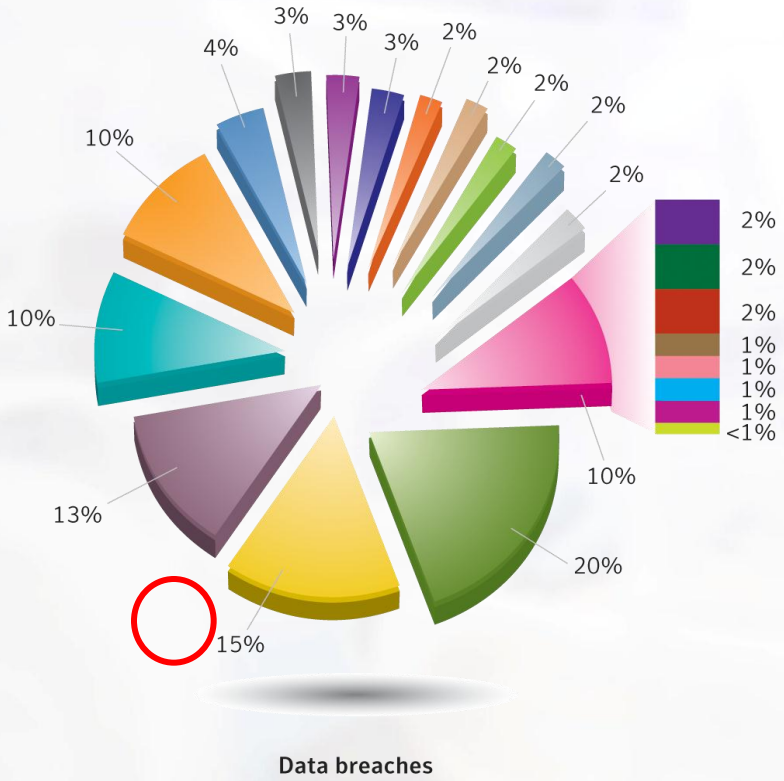
- Meaningful Use & Security
- HIPAA/HITECH Compliance
- Health Information Exchange Implications

Mac McMillan
CEO CynergisTek, Inc.
Chair, HIMSS Privacy & Security Policy Task Force

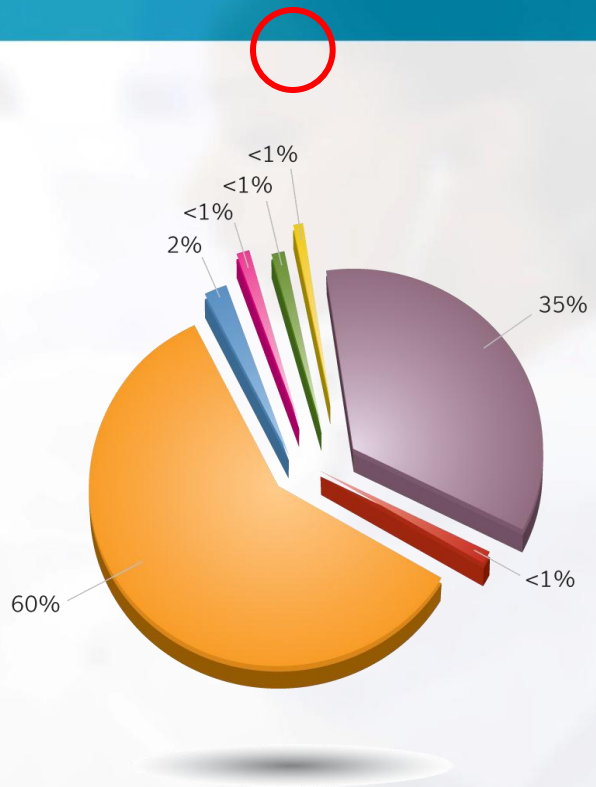
Why is Data Security Important?

- People **choose** to disclose their most intimate information in order to get healthy
- Doctors **earn** their trust by guaranteeing privacy
- Privacy is achieved by properly **protecting** systems and information
- Breaches of security and privacy affect patient **confidence**
- No confidence → people avoid treatment, lie or omit information, opt-out, and potentially **GET SICKER**.
- No one should ever have to choose between getting healthcare and privacy. **We all deserve both**.

Threats Are Increasing



Data breaches



Identities exposed

- Administration/human resources
- Arts/media
- Biotech/pharmaceutical
- Business consulting
- Community/non-profit
- Computer hardware
- Computer software
- Education
- Financial
- Government
- Health care
- Hospitality
- Information technology
- Insurance
- Law enforcement
- Manufacturing
- Military
- Other
- Real estate
- Retail/wholesale
- Telecom
- Transportation
- Utilities/energy

Internet Security Threat Report

- Good news – few exposed identities
- Bad news – the number of breaches is high (reporting mandates is part contributor)

Consumer Expectations

- Individuals should have means of direct, secure access to e-health information
- Individuals should know how their e-health information may be used and who has access to it
- Individuals should have control over whether and how their information is shared
- Systems for e-health data exchange must protect the integrity, security, privacy and confidentiality of an individual's information
- Governance and administration of e-health networks should be transparent and publicly accountable

A Perception of Insecurity

- Public distrust of government/corporate management of data:
  - Business associate for Stanford Hospital exposes 20,000 patient's information for more than a year
  - Business associate of Tricare exposes 4.9 Million patients data
  - Business associate of HealthNet losses nine servers from data center
  - 330 major breaches since 2009 involving over 11.8 Million individuals

Healthcare Concerns

- Pervasiveness of information being made available electronically has made Healthcare a target of cybercriminals. (1 in 6 attacks in 2009 were HC, greatest growth in attacks in 2010 in HC)
- In general Healthcare faces bigger risks going forward than the financial or retail sectors because the information they have is more valuable and theres greater access.
- Cybercrime in Healthcare is in its infancy, but only because health information sharing is in its infancy, it will grow with the opportunity.

Affect of State Breach Laws

- *NEW* State Breach Laws:
  - CA SB 24 – Last of five breach notification laws in California requiring notification to State AG if breach affects more than 500 individual records
  - TX HB 300 – Texas medical records privacy law that requires notifications to individuals in all 50 states of a breach by any company doing business in Texas
- Federal/State laws concerning HIV. Mental Health, Substance Abuse, etc.

Meaningful Use

Meaningful Use Privacy & Security

- Meaningful Use means providers need to show they are using certified EHR technology in ways that can be measured in quality and quantity.
- The requirement is the same as under the original HIPAA security rule; provide for the confidentiality, integrity and availability of ePHI.
- Attestation is different from compliance with HIPAA. One is a formal statement of eligibility to receive Federal funding, the other readiness with respect to a compliance standard.
- Both Stage 1 and 2 are focused primarily on adoption and implementation of an EHR.

Meaningful Use Stage 1

- **Privacy & Security**
  - Conduct, or review, a risk assessment in accordance with 45 CFR 164.308(a)(1)
  - Remediate deficiencies identified prior to or during the attestation period

- **EHR Security Functionality**
  - Access control
  - Emergency access
  - Automatic log off
  - Audit logs
  - Integrity
  - Authentication
  - General encryption
  - Encryption when exchanging information
  - Accounting of disclosures

Meaningful Use Privacy & Security

- Common areas of concern in MU risk analysis:
  - Incomplete risk analysis scope
  - Insufficient documentation
  - Use of generic accounts
  - Lack of system activity review
  - Lack of encryption or compensatory measures

Meaningful Use Privacy & Security

- Meaningful Use Stage 2 privacy and security requirements added last week during Health Information Technology Standards Committee.
- Reinforced requirements already levied such as risk analysis and enablement of security functionality.
- Recommends additional requirements for encryption, authentication and auditing.

Meaningful Use Stage 2

- **Privacy & Security**
  - Patients are offered secure messaging online and at least 25 patients have sent secure messages on line
  - Patient portal controls:
    - Single Factor Authentication
    - Audit trail for access
    - Establish data provenance
    - Secure download ability
    - Warning message before downloading PHI

- **Privacy & Security**
  - Perform, or update, security risk assessment and address deficiencies
  - Address encryption for data at rest, in data centers and on mobile devices (e.g. Laptops, PDAs, etc.)
  - EPs and EHs attest to this policy

Meaningful Use Stage 2

- **Privacy & Security**
  - 2-Factor authentication for controlled substances
  - Entity level digital certificates
  - Capability to detect and block programmatic attacks or attacks from a known, but unauthorized user (such as auto lock out after a certain number of attempts)

HIPAA & HITECH

HIPAA & HITECH Security

- Recurring challenges in data security:
  - Two thirds of all breaches still result from non encrypted devices and media
  - Inadequate risk assessment, evaluation or system activity monitoring
  - Inadequate/reactive auditing
  - Lack of readiness or inability to demonstrate processes/compliance
  - Unsupported systems and applications

HIPAA & HITECH Security

- Recurring challenges in data security:
  - Lack of entity authentication/weak security on wireless segments
  - Lack of auditing of users with elevated privileges
  - Unfiltered web mail and social media outlets
  - Over reliance on generic logins
  - Transmission security vulnerabilities
  - Device and media security weaknesses
  - Inadequate vender management

HIPAA & HITECH Security

- Vender breaches account for nearly 42% of all breaches now. Vender management needs to improve:
  - Data Access – Minimum Necessary
  - Data Retention Policy - Termination
  - Technological Infrastructure – Integrity/3rd Parties
  - Business Continuity – Procedures/Tests
  - Incident Response Plan - Notifications

HIPAA & HITECH Security

- Common trends from security surveys:
  - Half of respondents say their organization's ability to counter threats is less than adequate
  - 25% report they have suffered breaches
  - The single biggest concerns are mistakes by staff followed closely by insider threats
  - User education is generally viewed as ineffective

HIPAA & HITECH Security

- Steps to improve readiness/reduce risks:
  - Conduct a thorough risk assessment/use third party for objectivity/due diligence
  - Develop detailed remediation roadmap/create ongoing project
  - Ensure IT security personnel receive appropriate training
  - Implement robust system and user audit practices
  - Implement rigorous vender management

HIPAA & HITECH Security

- Technologies you should be considering:
  - Encryption
  - Privacy audit monitoring
  - Network log monitoring
  - Intrusion Detection Systems
  - Data Loss Prevention
  - Security Incident Event Monitoring
  - Network Access Control

HIE Privacy & Security Considerations

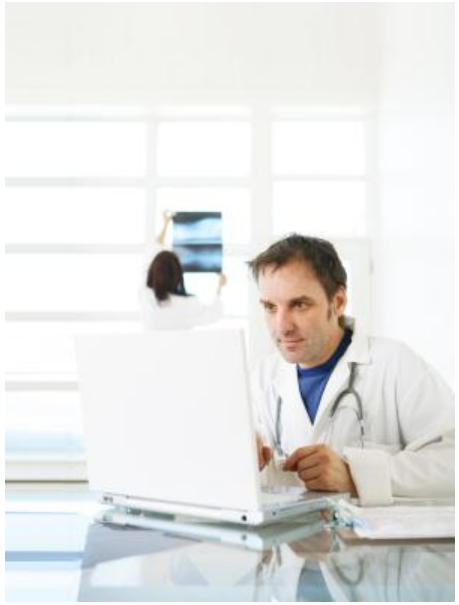
Increased Risk

- Data aggregation accentuates risk:
  - Data aggregations increases the value of the centralized store thereby creating a lucrative target for attackers
  - Increases the number of legitimate users who access the centralized store thereby multiplying the number attack vectors
  - Creates attractive target for others requesting access to information for non healthcare related purposes

Privacy & Security Considerations

- **Legal issues**
  - Variations in State Laws
  - Other Federal Laws
  - Participation Agreements
  - Business Associate Agreements

Privacy & Security Considerations

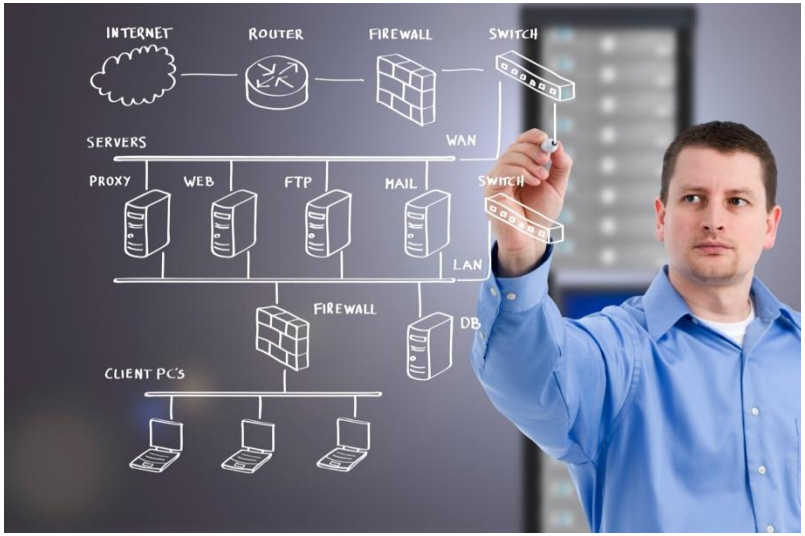


- **Minimum Necessary**
  - Routine releases/access
  - Non-Routine releases/access
  - Limited Data Set vs Minimum Necessary
- **Access to Health Information**
  - Authorization
  - Audit & Accounting
  - Patient Access
  - Designated Record Set

Privacy & Security Considerations

- **Identity Management**
  - Patient identification processes
  - Privacy concerns (accuracy/exposure)
  - Search rules narrowly defined
- **Opt-in/Opt-out**
  - Defined process/decision points
  - Federal/State preemption analysis
  - Patient education

Privacy & Security Considerations



- **Quality of Information**
  - Standards for content/definitions
  - Participants responsibility
  - A common dictionary
- **Security & Communications**
  - A common framework for controls
  - EHR certification standards
  - Consistent risk management approach

Privacy & Security Considerations

- **Other Operational Impacts**
  - Multistate Considerations
  - HIV, Mental, Substance Abuse Data
- **Patient Education**
  - Consumer Trust Issues
  - Quality of Care Benefits
  - Patient Rights

Questions

Thank you.

For Additional Information please contact:

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555

Stephanie.crabb
Stephanie.Crabb@cynergistek.com
(954)298.4702