May 3rd, 2013

IT Security in the Era of Meaningful Use

Alabama HIMSS

Presented by Melissa Stice Larson
Director of Compliance Services, CynergisTek, Inc.

CYNERGISTEK

www.cynergistek.com

Advancing the Standard of Care Through Healthcare IT

Today's Presenter

- **Melissa Stice Larson**, Director of Compliance Services at CynergisTek, Inc.
- Certified Information Systems Auditor, Certified Internal Auditor and Certified Fraud Examiner.
- Audited Meaningful Use Readiness and Metric Validation for past three years at nation's largest faith-based Health System.
- 15 years experience in IT Auditing for Medicare, Medicaid and Healthcare compliance.

CYNERGISTEK

Why Data Security Is Important

- People **choose** to disclose their most intimate information in order to get healthy
- Physicians **earn** their trust by guaranteeing privacy
- Privacy is achieved by properly **protecting** systems and information
- Breaches of security and privacy undermine patient **confidence**
- No confidence → people avoid treatment, lie or omit information, opt-out, and potentially **GET SICKER**.
- Privacy and Security are integral to **care.**

CYNERGISTEK

Agenda

- What's Current
- Meaningful Use
- Meaningful Use Audits
- Mobile Security
- Wrap Up/Questions

CYNERGISTEK


What's Current

The Environment is Changing

- Pervasiveness of information being made available electronically has made Healthcare a target of cyber-criminals.
- Healthcare initiatives such as health information exchanges, accountable care organizations, electronic health records, mobile devices, networked medical devices, patient portals, etc. increase availability and risk.
- In general, Healthcare faces bigger risks going forward than the financial or retail sectors. The information retained is more valuable and greater access is expected.

Quote: "Criminals don't care about compliance. They only care that an organization has data which is valuable on the street."
-Bryan Thornton, Net Reaction

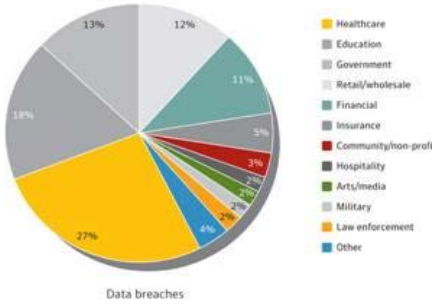
CYNERGISTEK

Risks to Health Systems & Data are Increasing

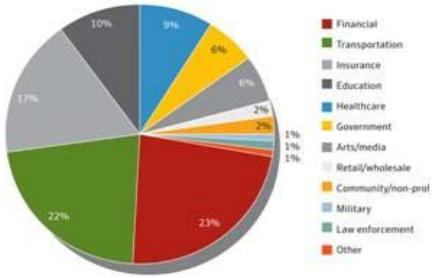
- Vulnerable networks and systems cost Healthcare billions each year and put patient safety at risk.
- In 2011 and 2012 DefCon, BlackHat and RSA all featured presentations demonstrating the vulnerability of medical systems and devices.
- Third party service providers/business associates, hackers using new/old threats, loss and theft of data.

CYNERGISTEK

2013 Threat Outlook: More Threats…



Data breaches



Identities exposed

In 2012 healthcare retains number one position in total number of breaches reported, and fifth in overall identities exposed.

The total number of breaches reported in healthcare exceeds 80 thousand when considering those less than 500 records.

Symantec Internet Security Threat Report

Quote: "Since no boundaries exist in cyber space, health care records are attractive targets for transnational organized criminal enterprises. Once the cyber criminals steal your information, recovery by law enforcement is very difficult."
-Scott E. Augenbaum, Federal Bureau of Investigation

CYNERGISTEK

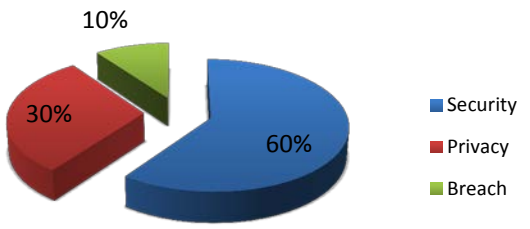
Resources Create Challenges

- Increased operations, ops tempo, numbers of users, connections, applications,
- too few skilled information security professionals in healthcare filling critical positions,
- adoption of security technologies continue to lag behind need, and
- healthcare spending on security averages half that of other regulated industries…
- EXCEPT for those who have suffered a major breach.

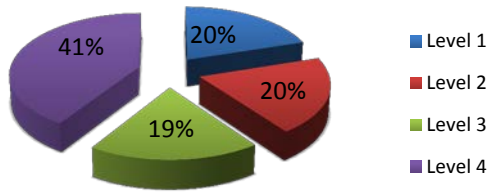
CYNERGISTEK

The Numbers Tell the Story

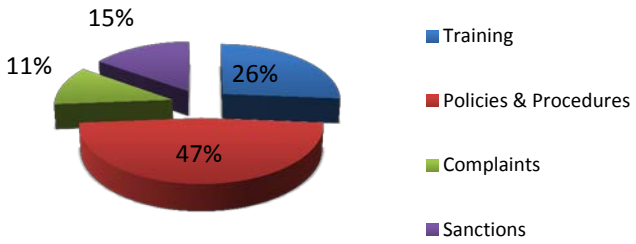
By Rule



By Level



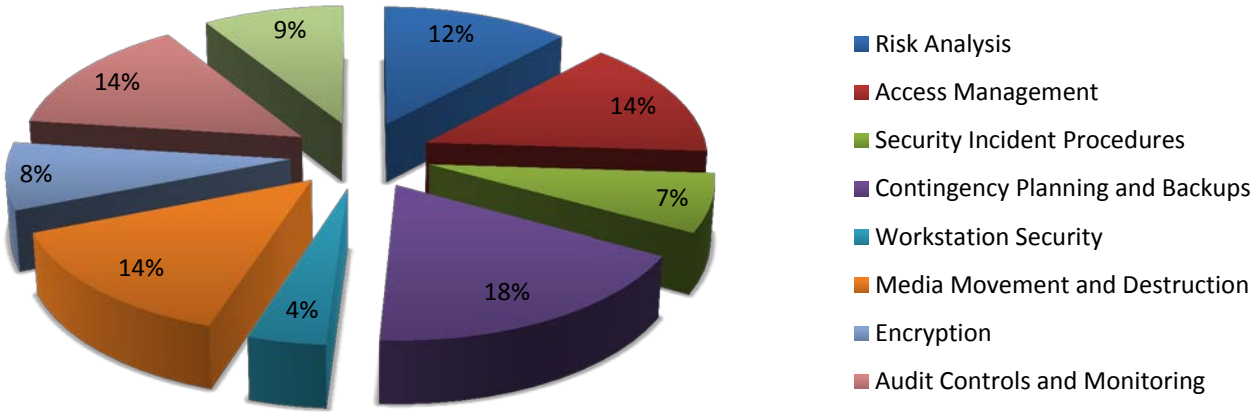
By Type



Quote: "If compliance is hard for large organizations, it is almost insurmountable for small ones. Organizations are being told they need to 'do it' but they don't always know where to start."
- Bryan Thornton, Net Reaction

CYNERGISTEK

Security: Resources, Technology & People



CYNERGISTEK


Meaningful Use

Regulations Create Challenge

- HITECH introduced multiple changes to HIPAA Privacy and Security, many of which are recent. The Omnibus Rule was issued Jan. 2013 (Accounting for Disclosures).
- Meaningful Use requirements for Stage 1, 2 & 3 privacy & security.
- There are anticipated changes to other rules such as CLIA, SAMHSA, the Common Rule, etc.
- Continued development of State Laws with greater specificity.
- ***New*** Federal laws proposed in response to incidents. (Protect Our Health Privacy Act of 2012)
- Potential for more change following the outcomes of OCR random audits and report of overall compliance.

CYNERGISTEK

Meaningful Use I

- Core measures 12 and 14 refer to security requirements
- Conduct or review a Risk Analysis in accordance with §164.308(a)(1) and remediate deficiencies
- Risk Analysis must be completed prior to attestation, remediation must occur within attestation period (12 months)
- Enable 8 security features of the EHR

CYNERGISTEK

Meaningful Use II

- Perform and/or update security risk analysis **and** address deficiencies (explanation of encryption practices)
- EP: Use secure electronic messaging to communicate with patients on relevant health information
- Record (log) actions related to health information, audit log status and encryption of end user devices
- Encryption has to meet NIST specification and be approved by FIPS 140-2
- Synchronization of clocks must meet Network Timing Protocol (NTP) v3 or v4

CYNERGISTEK

Meaningful Use Stage II

- Authenticate users against unique identifiers and proscribed accesses
- Default: audit all access, permit restricted access and monitor for tampering
- Permit an end user to create an audit report for a specific period of time and permit sorting by specific criteria
- Permit amendments or comments to a patient record while preserving the original record content

CYNERGISTEK

Meaningful Use Stage II

- Default: automatic logoff after a predetermined time
- Permit access to patient information, in time of emergency, by identified set of users
- Ensure integrity of patient information within the EHR and information exchanged by creating a message digest
- Optional – record disclosures made for treatment, payment and operations for purposes of accounting for disclosure

CYNERGISTEK


Meaningful Use Audits

MU Audits

- Figloiozzi & Co. were designated by CMS to perform the Meaningful Use (Stage 1) audits.
- Figloizzi & Co. has sent letters requesting:
  - Proof of EHR certification for the technology they used to meet Program requirements.
  - Documentation to support the method (observation services or all emergency department visits) they chose to report emergency department admissions. The differentiation of the method used for reporting ED admissions is key as it determines which patients were included in the denominators of specific core measures and menu items.

CYNERGISTEK

MU Audits

- Figloizzi & Co. has sent letters requesting (con't):
  - Supporting documentation with regard to the completion of core set objectives and measures. A hospital should be able to general MU reports that substantiate the patient encounters that were utilized to verify attestation metrics. Including evidence of HIPAA Risk Assessment.
  - Supporting documentation regarding the completion of "menu set" or voluntary, objectives and measures.
- The audit letters have generally requested a two-week response time is specified.
- Unclear how audit candidates are selected but appear to have been attested at least one year prior to audit.

CYNERGISTEK

MU Audits

- Figloizzi & Co. have conducted both desk audits and on-site audits. They have traveled to a select number of audit locations.
- Other - OIG Evaluation of CMS's role in MU
  - OIG indicated that CMS was facing obstacles in overseeing the Medicare EHR incentive program in a Nov. 2012 report.
  - OIG indicated that CMS did not require supporting evidence during the attestation process.
  - CMS did not verify the calculation of individual metrics.
  - Recommended that CMS provide examples of the types of evidence that would be acceptable.

CYNERGISTEK


Mobile Security

Mobile Device Security



90% of companies will support corporate applications on personal mobile devices by 2014 – Gartner, Nov. 2011

By 2016, over **350** million will use their smartphones for work. –Forrester, April 2012

900 Million Tablets in the market
980 Million Smartphones shipping annually
by 2015 –Gartner, Sept. 2011

Embrace the inevitable, the Borg will prevail…

CYNERGISTEK

Mobile Devices Uses

- Email, calendars, contacts
- Text messages
- Pictures
- Video Recording
- Audio Recording
- Internet Access
- Application Access
- Uploading/downloading data, images and music
- Scanning barcodes/QR Codes
- Transactions
- **Every once in a while a phone call is made…maybe**

CYNERGISTEK

Mobility Gains Versus Pains

- Productivity gains of 9 hours a week for Federal workers using mobile devices, according to a study by the Telework Exchange.
- Workers reported gains in productivity, collaboration and most of all communication.
- 55% of workforce members report using personal devices in workplace, a third say they don't use passwords to protect their device, 61% say their organizations don't have BYOD policies.
- Nurses reported advantages including: enhanced quality of care due to readily available data, ease of disseminating and storing data, decreased data error, decrease in time spent of data management, facilitates clinical documentation, quick access to drug and clinical references.
- Texting **IS** a part of the workflow for more than 95% of workforce members.

CYNERGISTEK

Common Health Scenarios

- More and more Medical staff are turning to their mobile devices to communicate because its easier, faster, more efficient…
  - Sharing lab or test results
  - Locating another physician for a consult
  - Sharing images of wounds and radiology images
  - Updating attending staff on patient condition
  - Getting direction for treatment
  - Locating a specialist and collaborating with them
  - Transmitting trauma information or images to Eds
  - **Prescribing or placing orders**

CYNERGISTEK

The Problem With Texting

"It is not acceptable for Physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting."

"This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record."

The Joint Commission
November 2011

CYNERGISTEK

The Environment Changes Again

- Proliferation of mobile technology rampant
- The network is disappearing, by 2016 mobile will be standard
- Mobile technology is part of mainstream workflow
- Moved from Corporate issue to BYOD
- Mobile apps/apps stores arrive
- Perimeter expands again to “access anywhere, any time, any device”
- Mobile devices used routinely to communicate with/and about patients
- Shrinkage happens

CYNERGISTEK

Need For Strong Policies

- Use of personal devices for business optional
- Workforce can use personal device as long as agree to policy
- Workforce members must allow agent deployed on device
- Must agree that Health System (HS) data used or stored on device is HS property
- HS can revoke permission to use at any time
- Workforce member agrees to inspection or possession upon request
- Workforce member agrees to remote wipe is lost or stolen
- Workforce member will remove all HS property when no longer using device
- Workforce members must agree to use HS procured software for access to HS data

CYNERGISTEK

Strategies

- **Segmentation** – Place all personal devices on a separate network segment that restricts access based on role and need
- **Mobile Device Management** – Control mobile devices through the deployment of an MDM technology
- **Virtualization** – Access data through virtual connections that do not allow data to be stored/transferred locally (VDI)
- **Network Access Control (NAC)** – Restrict devices that can connect to the network with tools that permit real time interrogation
- **Data Loss Prevention (DLP)** – Provide data centric controls through data leakage solutions that permit enforcement of rules
- **Encryption** – Utilize both device and data encryption solutions

CYNERGISTEK

Mobile Applications

- There are more than 50,000 healthcare applications for the iPad/iPhone
- Many applications are not tested before fielded (beware of free)
- Not all application developers understand security or include it in their creations
- Most organizations are developing their own apps/app stores
- Control apps through network credentials and MDM
- Understand that FDA has not yet spoken

CYNERGISTEK

Best Practices

- **Require Passcodes** – one of the simplest things we can do to protect our devices is use a good pass code
- **Enforce Encryption** – for iOS this is fairly straight forward, 3Gs and beyond use encryption when passcode is enabled, for Android not so much
- **Restrict Device Features as Appropriate** – consider which features you will permit, iCloud, video or photo streaming, Youtube, etc.
- **Pay Attention to Apps** – use MDM to containerize and manage apps, provide app store
- **Encrypt Email/Text** – use an appropriate email and texting encryption solution
- **Distribute Settings OTA** – use MDM to create and push settings, added benefit when user leaves
- **Enforce Policies** – use MDM to alert to non compliant situations, and enforce corrections
- **Monitor Devices** – monitor your devices for compliance and connectivity

CYNERGISTEK

Commonly Cited by OCR

- § 164.310(d)(1) Device and Media Controls (Required) Policies and procedures that cover the receipt and removal of hardware or media containing ePHI in and out of the facility.
- § 164.312(a)(2)(iv) Encryption and Decryption Access Control: Data at Rest (Addressable) Implement measures to encrypt and decrypt ePHI
- § 164.312(e)(2)(ii) Encryption Transmission Security: Data in Motion (Addressable) Implement measures to encrypt ePHI when appropriate.

CYNERGISTEK


Wrap Up/Questions

Today's Reality

- An evolving and more directed threat will become increasingly more dangerous and present **real risk to both confidentiality and patient safety.**
- Digitization of data, automation of processes and services and the consumerization of the network will continue to increase the requirement for **more sophisticated protections**.
- To create an enterprise capable of meeting tomorrow's protection requirements and ensure reliable information services will **require greater commitment of resources.**

CYNERGISTEK

Thank You

For more information please check out the CynergisTek blog site.

www.cynergistek.com

Melissa Stice Larson
Director, Compliance Services
Melissa.Stice-larson@cynergistek.com
(972) 999-9623

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

CYNERGISTEK