All Aboard the HIPAA Omnibus
An Auditor's Perspective

Rick Dakin | CEO & Chief Security Strategist

February 20, 2013

Agenda

Healthcare Security Regulations – A Look Back

What is the final Omnibus Rule?

Changes to the HIPAA Security Rule

Shortcomings of the Omnibus Rule

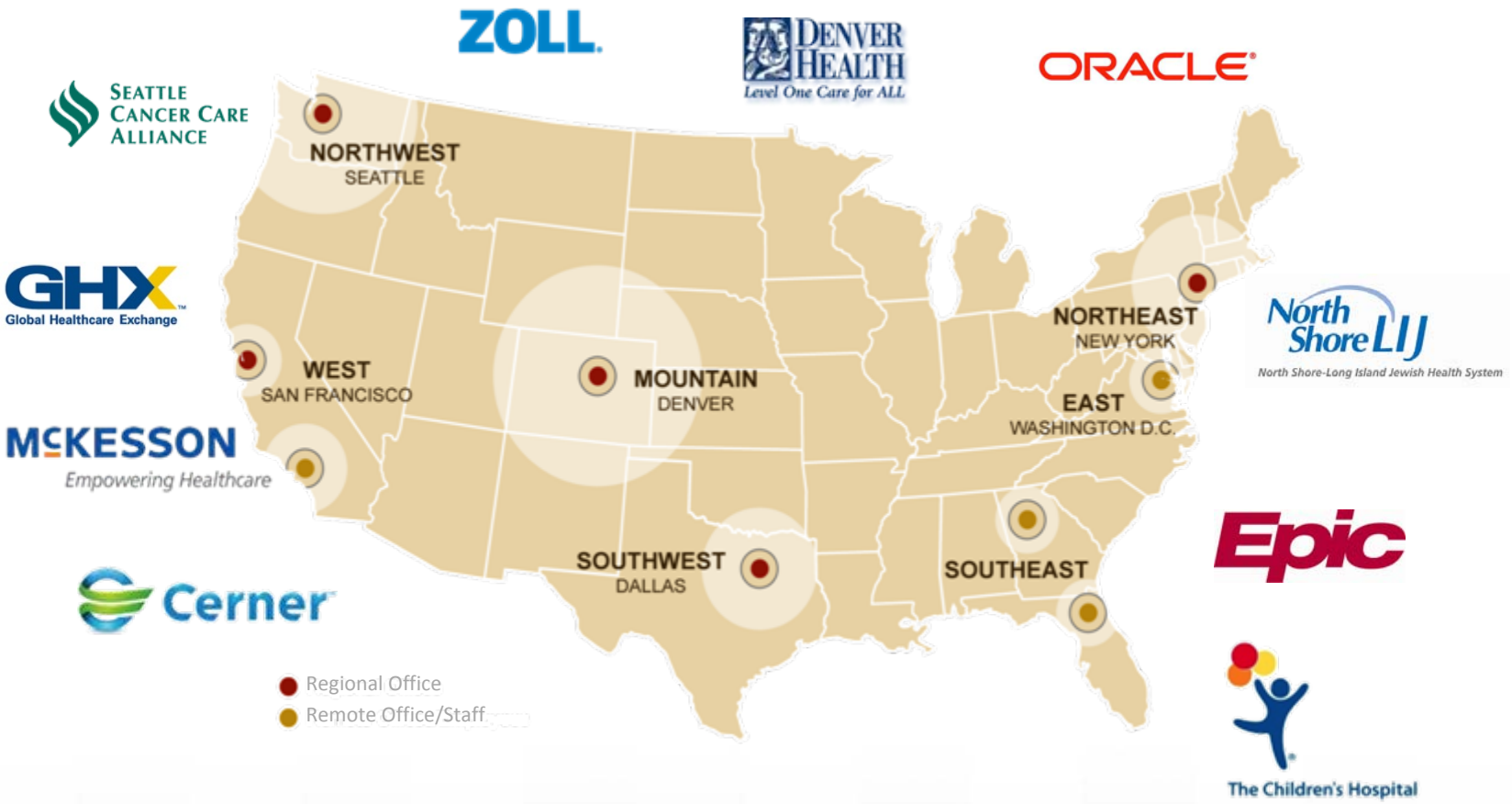
About Coalfire

Coalfire offers demonstrated leadership in all key areas of IT GRC – auditing, assessment and validation for healthcare organizations (covered entities and business associates).

About Coalfire

We help our clients recognize and control IT-related risk, and maintain compliance with all major industry and government standards.

- Our approach and methods have been validated by more than 5,000 projects worldwide.
- Our healthcare team has conducted over 300 healthcare-related projects.


ZOLL
DENVER HEALTH
Level One Care for ALL
ORACLE
SEATTLE CANCER CARE ALLIANCE
NORTHWEST
SEATTLE
GHX
Global Healthcare Exchange
NORTHEAST
NEW YORK
North Shore LIJ
North Shore-Long Island Jewish Health System
WEST
SAN FRANCISCO
MOUNTAIN
DENVER
EAST
WASHINGTON D.C.
McKESSON
Empowering Healthcare
Epic
SOUTHWEST
DALLAS
SOUTHEAST
Cerner
Regional Office
Remote Office/Staff
The Children's Hospital


ADVISORY SERVICES
AUDIT & ASSESSMENTS
COALFIRE LABS
DIGITAL FORENSICS
PENETRATION TESTING
CLOUD & VIRTUALIZATION
APPLICATION SECURITY
NAVIS SERVICES

Coalfire

Healthcare Security Regulations - HIPA

HIPAA – 1996

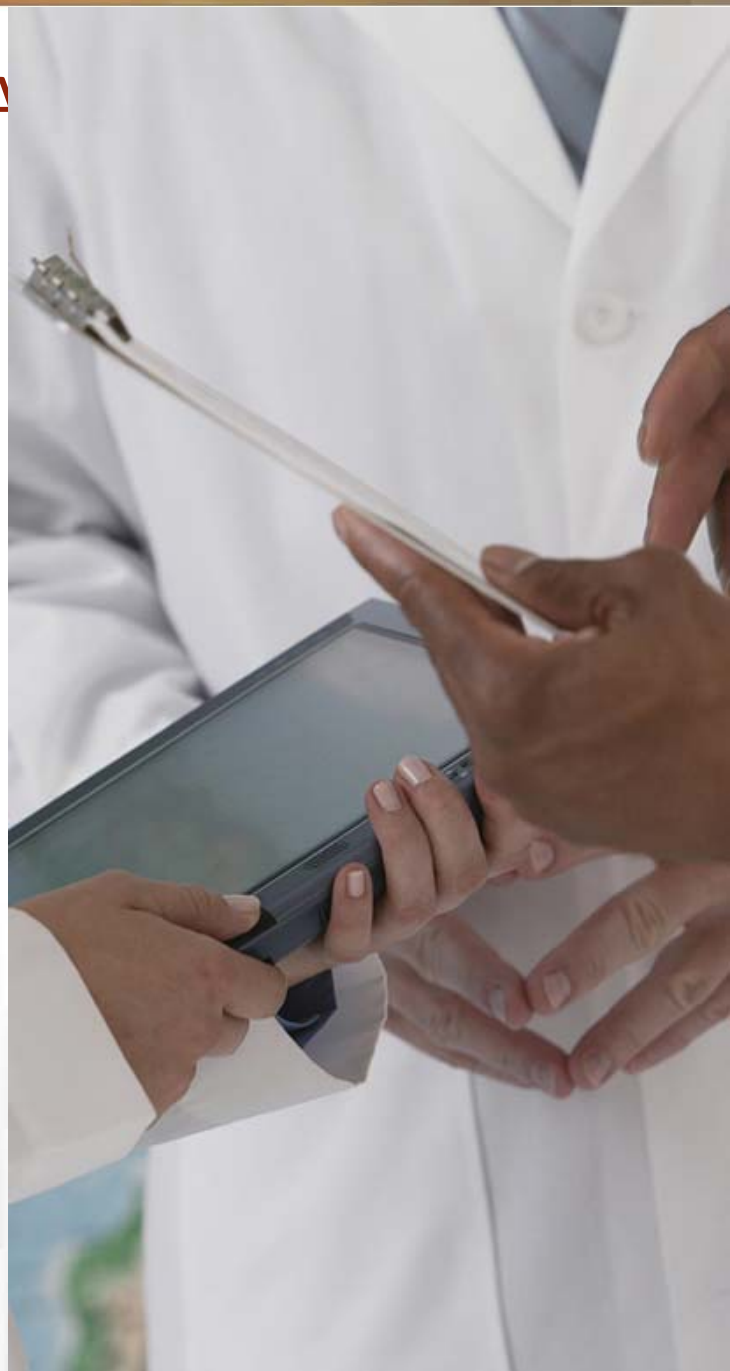
Enacted - 2/20/2003

Applicable to - Covered Entities

Goal -

To simplify the administrative processes of healthcare and to protect patient privacy.

Enforcement - Very limited



Healthcare Security Regulations - HITEC

HITECH - part of ARRA – 2009

Applicable to -
Covered Entities and Business Associates

Goal -

Designed to accelerate adoption of EHR systems among providers. Also expanded the scope of privacy and security protection under HIPAA. Added breach notification obligation.

Enforcement -

Increased enforcement potential for non-compliance.

Healthcare Security Regulations – Meaningful Use

Meaningful Use Guidelines for EHR – 2010

Goal -

To provide an incentive program for using EHRs and encourages compliance measures set forth in HIPAA and HITECH.

Applicable to -

Eligible professionals, eligible hospitals, and CAHs.

Enforcement (incentive) -

$27B is provided for attesting to 15 core objectives over 4 years.

OCR Audit Pilot Program

- OCR awarded a $9.2M contract for pilot program.
- **Objective** was to use the audits as an opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities.
- OCR identified a pool of **covered entities** for audits that broadly represent the wide range of healthcare providers, health plans and healthcare clearinghouses (all sizes).
- **115** audits were completed by the end of 2012.
- Preliminary results were released in June 2012 and an official **Audit Protocol**. Final results and the plan to continue the audits in 2013 to come.

The HIPAA Omnibus Rule - Highlights

- Applies many security and privacy requirements to business associates (BAs) and their subcontractors.

  And imposes direct civil money penalty liability on business associates for violations of applicable HIPAA provisions.

- A final version of the HIPAA breach notification rule. An interim final version has been in effect since September 2009.

  The new version clarifies requirements for when a breach must be reported to authorities.

The HIPAA Omnibus Rule - Highlights

- A rule stating that using genetic information for insurance underwriting purposes is a privacy violation under HIPAA, as well as discriminatory under the Genetic Information Non-Discrimination Act (GINA).

- The HIPAA Omnibus Rule is going to be a big deal because it's likely to set the tone for the HIPAA Rules for at least the next three years.

"There will be blood" until the healthcare industry gets the message that this isn't your daddy's HIPAA anymore.

What is Missing?

The Omnibus Rule's new Security Rule changes primarily affect BAs, but there are areas that were missed.

More rigorous testing and audit program guidelines

- Incorporate results from the pilot OCR audits
- Either adopt HITRUST standards or publish more comprehensive assessment criteria

Adoption of new medical technologies

- Cloud computing environments
- Mobile devices
- Internal/external vulnerability scans and penetration testing

More Rigorous Audit & Assessment Guidelines

HITRUST

- While HITRUST is not an OCR approved or endorsed organization, it raises the bar on securing ePHI.
- The end result of HITRUST assessment can be certification…indicating the organization's control environment meets the 135 HITRUST control specifications.

PCI-Like Assessment Criteria

- OCR has started publishing assessment criteria, but it is not yet comprehensive or adequate to achieve any level of certification.

More Rigorous Audit & Assessment Guidelines

Penetration Testing

- The maturity of the ePHI control environment cannot be fully assessed without vulnerability scanning or penetration testing.

Medical Device Testing

- Buyer beware. No current medical device has been certified to enable HIPAA Security Rule compliance.
- Many devices actually prevent native compliance to HIPAA Security Rule Implementation Specifications.

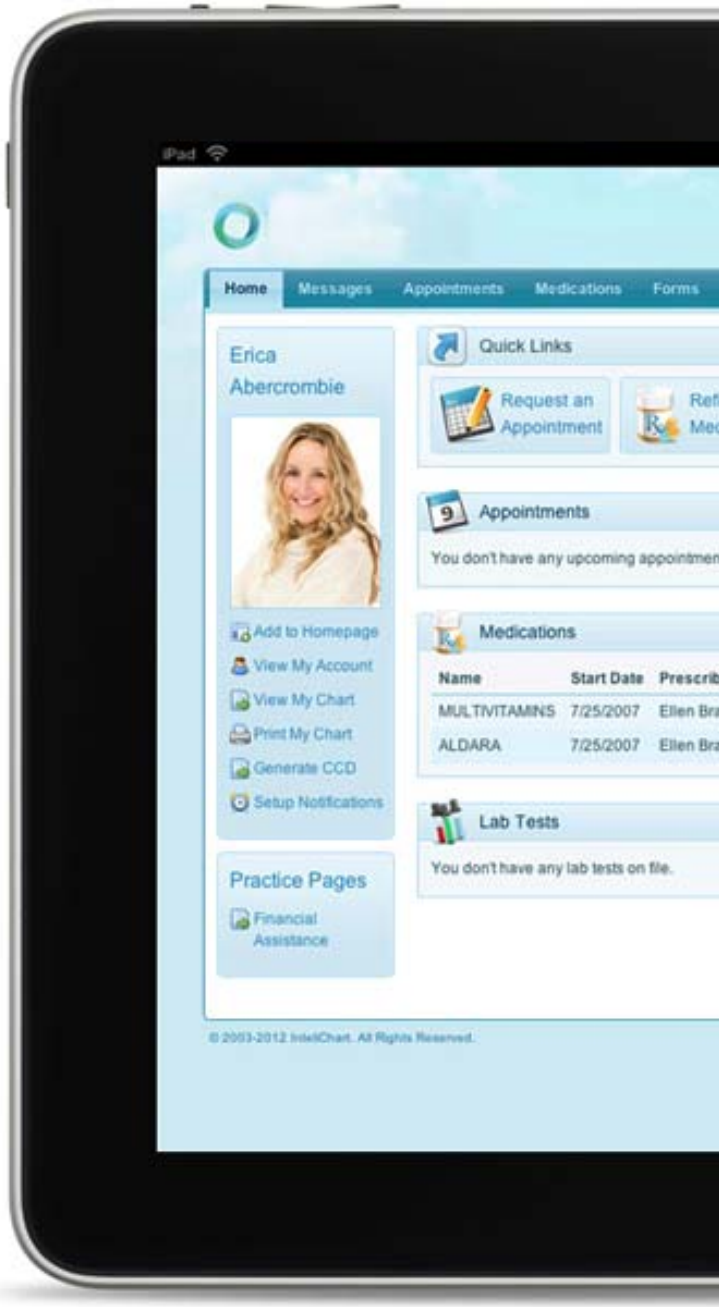
Emerging Trends in Healthcare IT

Mobile Devices

- Smartphones and tablets represent over 90% of the net-new growth in device adoption for the coming four years.

Cloud Services

- By 2016, 40% of enterprises will make proof of independent security testing a precondition for using any type of cloud service.



Source: Gartner Research, 2012

Emerging Trends in Healthcare IT

Content Management

- At year-end 2016, more than 50% of Global 1000 companies will have stored customer-sensitive data in the public cloud.

IT Risk and Compliance

- HITECH did not update the HIPAA Security Rule to accommodate health record migration to the cloud.
- Texas HB 300 sets a new standard for managing access controls to individual health records. And now, Utah S.B. 20.

Source: Gartner Research, 2012

Healthcare and Cloud Computing

- A privacy advocate has demanded federal guidance on how to protect health information in the cloud.
- Smaller healthcare organizations are turning to cloud providers to host electronic health records to help reduce start-up costs.
- What if a cloud-based product or service used by a healthcare organization is illegally accessed? Who's liable?
- CSPs are BAs and now must be compliant per the Omnibus Rule.

Technology is ahead of policy.

Healthcare and Cloud Computing

- Solutions that allow physicians to receive encrypted email on mobile devices.
- Solutions that allow doctors to securely text-message each other to coordinate patient care.
- Develop policies and procedures that are scalable to ensure protected data sharing within the organization and beyond.

Healthcare and Mobile Devices

Less control, shared environments

Healthcare and Mobile Devices

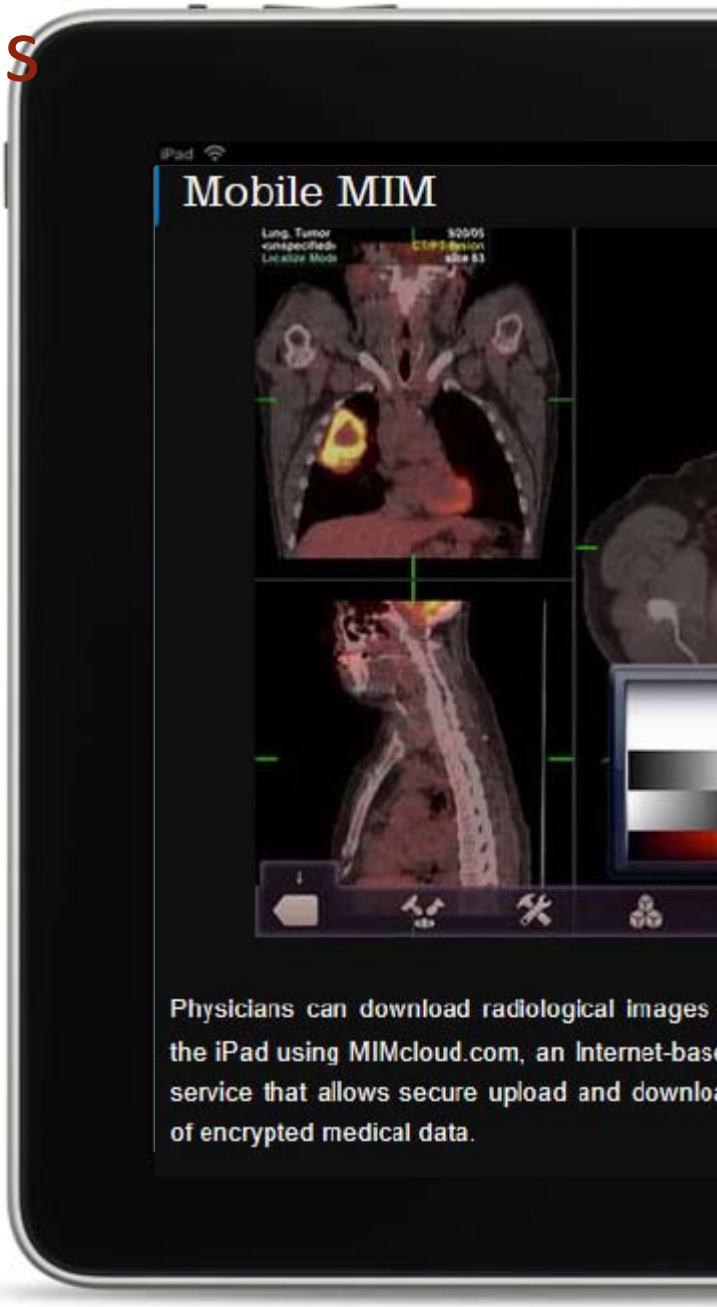
PHYSICIANS

- 83% own at least one mobile device
- 25% leverage mobile devices in Practice
- 81% use personal device to access ePHI
- Theft = 66% of reported data breaches

PERSONAL Mobile Device

- Authentication unlikely
- Data encryption unlikely
- Malware protection? Monitoring?
- Policy compliance? No

Source: American Bar Association, Health eSource newsletter, Oct 2011 Volume 8 Number 2



Healthcare and Mobile Devices

In Dec 2012, the HHS offered tips for HCOs when it comes to mobile device security – due to the high number of breaches caused by lost or stolen devices
http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Healthcare and Mobile Devices

This resource provides tips for securing mobile devices, frequently asked questions, videos depicting common risk scenarios, and five steps for protecting mobile data.

1. Decide whether mobile devices will be used for patient data
2. Assess risks and vulnerabilities
3. Identify mobile risk management strategy, privacy safeguards and security
4. Develop, document and implement mobile device and security policies
5. Train staff

Annual risk assessments MUST address mobility and other emerging technology issues. AND, a risk assessment is not enough – the risks MUST be mitigated.

Summary

Based on OCR's breach investigations and an analysis of 20 of the 115 HIPAA compliance audits conducted in 2012, the most common deficiency is the *lack of a thorough and timely risk assessment*.

e thing that bubbles up is risk

That's a consistent deficiency," said Mr.

Questions

Rick Dakin | CEO & Chief Security Strategist
877.224.8077 ext. 7001
Rick.Dakin@coalfire.com
www.coalfire.com