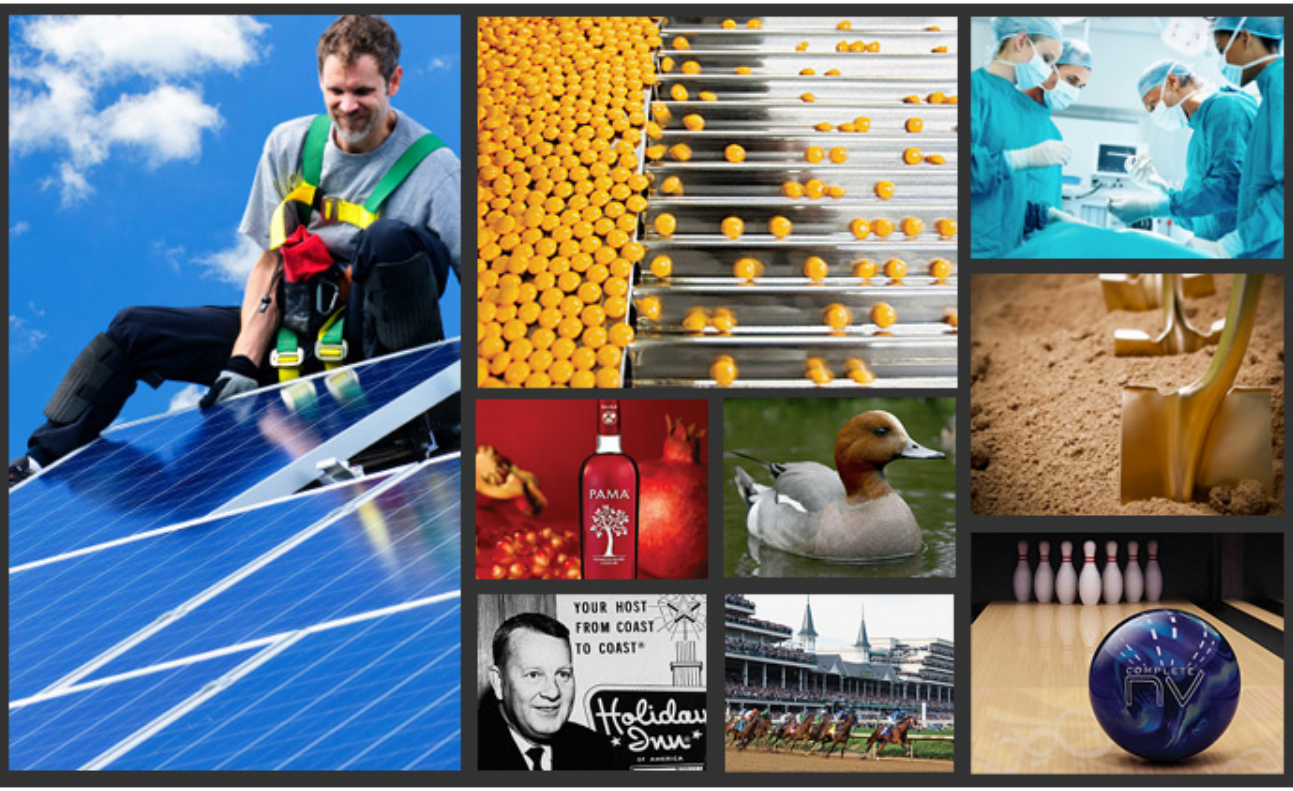
WYATT

WYATT TARRANT & COMBS LLP



LOUISVILLE.KY LEXINGTON.KY NEW ALBANY.IN NASHVILLE.TN MEMPHIS.TN JACKSON.MS

WWW.WYATTFIRM.COM

WYATT TARRANT & COMBS LLP

LEGAL ISSUES IN HEALTH IT SECURITY

Webinar Hosted by Uluro, a Product of Transformations, Inc.
March 28, 2013

Presented by:

Kathie McDonald-McClure, Esq.
Wyatt, Tarrant & Combs, LLP
500 West Jefferson Street, Suite 2800
Louisville, KY 40202
(502) 562-7526
kmcclure@wyattfirm.com

THIS IS AN ADVERTISEMENT

WYATT TARRANT & COMBS LLP

Disclaimer

The information in this presentation represents only a summary of the legal considerations associated with the use of health information technology and electronic health records and is not intended to cover all the issues or the fine points with regard to the matters discussed in this presentation. Accordingly, this presentation is not intended to be legal advice, which should always be obtained in direct consultation with an attorney about your specific facts and circumstances.

THIS IS AN ADVERTISEMENT

WYATT TARRANT & COMBS LLP

Topics for Today's Webinar

1) How did we get here?
2) What is the HIPAA Security Rule
3) Who must comply with the HIPAA Security Rule
   - What is a Covered Entity (CE)
   - What is a Business Associate (BA)
4) Meaningful Use & The Security Rule Risk Assessment
5) What is Required for Security Rule Compliance
6) The HIPAA Omnibus Rule's Heightened Penalties & Enforcement
7) Government stepping up audits for compliance

Why We Are Talking About Health IT Security?

Since HIPAA was enacted in 1996, there's been a greater use of electronic data, i.e., Health Information Technology (HIT), to:

- Create
- Store
- Transmit

sensitive personal health information among healthcare providers, health plans and healthcare clearing houses.

Why We Are Talking About Health IT Security?

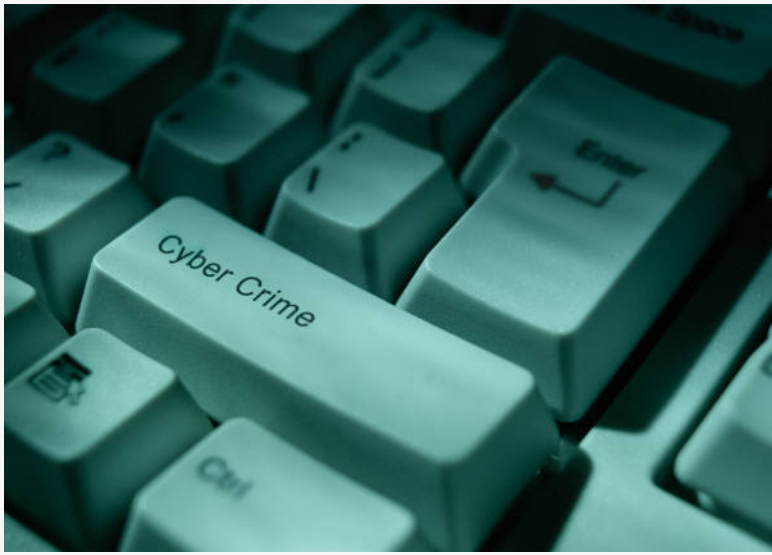
Other factors leading to increased use of HIT:

- Lifestyle choices – we want information and we want it now
- Quest for Quality – HIT viewed as a tool to improve medical decision-making specific to individual patients
- Quest for Lower Costs – HIT viewed as a tool to increase efficiency in the use of healthcare items and services

WYATT TARRANT & COMBS LLP

Why We Are Talking About Health IT Security?

- Increased risk of IT data breaches worldwide, leading to President Obama's Executive Order on Feb 12, 2013: Improving Critical Infrastructure Cybersecurity*
- Since the Breach Notification Rule became effective in Sept 2009, OCR has received breach notifications at a disturbing rate of 60,000 over a period of 1,000 days, most resulting from lost or stolen portable devices.
- Potential costs and legal risks with data breaches are substantial.



*See: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Recent Breach Settlements

- OCR settles breach incident with Hospice of Northern Idaho (HONI) for $50,000 for breach stemming from stolen, **unencrypted** laptop containing the ePHI of 441 patients. Aggravating factors:
  - HONI knew that its employees regularly used laptops as part of their field work but . . .
  - Did not conduct security risk assessment to safeguard the ePHI
  - Did not implement policies and procedures to address mobile device security as required by the HIPAA Security Rule.

Recent Breach Settlements

- OCR settles breach incident with Alaska Medicaid for $1.7M for breach arising from USB hard drive *possibly* containing ePHI which was stolen from employee's vehicle. Aggravating factors:
  - Failure to perform HIPAA Security Rule security risk assessment
  - Failure to implement adequate risk management measures
  - Failure to complete security training for its employees
  - Failure to implement device and media controls, including a failure to address device and media **encryption**

Why We Are Talking About Health IT Security?

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act)

- Enacted as part of the American Recovery & Reinvestment Act of 2009 (ARRA)
- Provides monetary incentives to "eligible hospitals" and "eligible professionals" who make a "meaningful use" of "certified electronic health records".

The HITECH Act

Goal: Nationwide interoperability of electronic health information

Increased Use of HIT: Increased risk of electronic health information breaches

How Government Has Addressed Increased HIT Breach Risks?

The HITECH Act and its implementing regulations:

- Ramp up compliance ⇒ make BAs and their Subcontractors directly liable
- Ramp up enforcement ⇒ increase penalties
- Make compliance with HIPAA's Security Rule a condition of receiving the HITECH Act's monetary incentives for making a "Meaningful Use" of certified electronic health records

Security Rule Compliance – An Element of Meaning Use

- **Eligible Hospitals** and **Eligible Professionals,** planning to attest to **Meaningful Use**, must perform a security risk assessment in compliance with the **HIPAA Security Rule**.
- Because Stage 2 Meaningful Use builds on Stage 1, Security Rule Compliance is required to qualify for the incentives under both Stage 1 and Stage 2.

Security Rule Compliance – An Element of Meaning Use

Stage 1 Meaningful Use Objective reads:

- Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Stage 1 Meaningful Use Core Measure* reads:

- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process."

***Measure 14 for Eligible Hospitals and Critical Access Hospitals** (http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/14_Protect_Electronic_Health_Information.pdf).
***Measure 15 for Eligible Professionals** (http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/15_Core_ProtectElectronicHealthInformation.pdf).

Security Rule Compliance – An Element of Meaning Use

Attestation Requirement:

- To meet this MU criteria, the Eligible Hospital or Critical Access Hospital or Eligible Professional who seeks to qualify for the MU incentives must attest "YES" to having:
  - Conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and
  - Implemented security updates as necessary and corrected identified security deficiencies prior to or during the EHR reporting period.

Stage 2 Meaningful Use – *Secure* Patient Messaging

Core Objectives:

- Eligible Professionals: >5% patients use **secure** electronic messaging to communicate with EP on relevant health information
- Eligible Hospitals: >50% of patients provided online access to PHI with >5% of patients actually accessing PHI

Who Else Must Comply with the HIPAA Security Rule?

- Covered Entities
  - Health Care Providers who transmit any information electronically in connection with certain transactions
  - Health Plans
  - Health Care Clearinghouses
- Business Associates & Business Associate's Subcontractors

See 45 CFR §§ 160.102, 164.500

Must all Health Care Providers Comply?

- Any person or organization who:
  - furnishes, bills or is paid for health care in the normal course of business ("Health Care Provider") and
  - transmits health information electronically in connection with a transaction covered by the HIPAA Transaction Rule, either directly or through a Business Associate

  is a "Covered Health Care Provider" and must comply with the HIPAA Security Rule.

See 45 CFR §§ 160.102

What Transactions are Covered?

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment or disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization

See 45 CFR § § 162.1101 –162.1802

What Health Plans are Covered Entities?

- Any individual or group plan (or combination) that provides, pays for the cost, of medical care is a CE, including:
  - HMOs
  - Group Health Plans
  - Original Medicare
  - Medicare Advantage
  - Medicaid
  - Health insurance issuers
- But not employer plans with less than 50 participants and that are self-administered, Excepted Benefit Plans* (see next slide), certain government funded programs

See 45 CFR §§ 160.103

What Health Plans are Covered Entities?

***Excepted Benefit Plans** are those that provide **excepted benefits,** such as*:

- coverage for accident, disability income insurance, or any combination thereof;
- coverage issued as a supplement to liability insurance;
- general liability insurance and automotive liability insurance;
- workers' compensation or similar insurance;
- automobile medical payment insurance;
- credit only insurance;
- coverage for on-site medical clinics;
- other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

See 45 CFR §§ 160.103

What is a Health Care Clearinghouse?

- A public or private entity that translates data content or format for another entity from a nonstandard format into standard data elements or a standard transaction or vice versa
- Examples:
  - billing service
  - repricing company
  - community health management information system or community health information system
  - “value-added” networks and switches

See 45 CFR §§ 160.103

Who is a Business Associate?

- A person who creates, receives, maintains or transmits PHI on behalf of a Covered Entity or Organized Health Care Arrangement and who is NOT a workforce member of the Covered Entity. BA functions can include:
  - Accounting, legal and consultant services
  - Claims processing or administration services, billing, benefit management, practice management, repricing services
  - Utilization review, quality assurance, patient safety activities
  - Health Information Organizations (e.g., HIO, E-prescribing gateway or other person providing data transmission services for PHI) that have routine access to PHI
  - Personal health records vendors
- Subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate

Who is NOT a Business Associate?

- A Covered Entity can be a Business Associate but not merely by virtue of coordinating patient care when performing such function on its own behalf. For example:
  - Provider gives PHI to payer for payment does not make the payer a BA of provider.
  - Hospital and physician each treating patient at the hospital is not a BA of the other.

See 45 CFR §§ 160.103

Who is NOT a Business Associate?

- Persons or organizations where access to protected health information is not necessary to do their job for the Cover Entity:
  - Janitors
  - Electricians
  - Copy machine repair persons

See 45 CFR §§ 160.103

WYATT TARRANT & COMBS LLP

The HIPAA Security Rule – What is it?

- The HIPAA Security Rule establishes a national set of security standards for protecting health information held or transferred in electronic form.

- Covered Entities and Business Associates must implement technical and non-technical safeguards to secure electronic PHI (ePHI).

Security Rule Objective

- Protect *privacy* of electronic protected health information (ePHI):
  - utilizing HIPAA's standards, which
  - require implementation of *safeguards* to secure ePHI.

Security Risk Assessment

To ensure the confidentiality, integrity, and availability of ePHI held by the entity:

1. **Identify** reasonably anticipated threats (breach risks) to the security or integrity of the ePHI
2. **Protect** against these threats w/safeguards
3. **Educate** workforce to ensure compliance

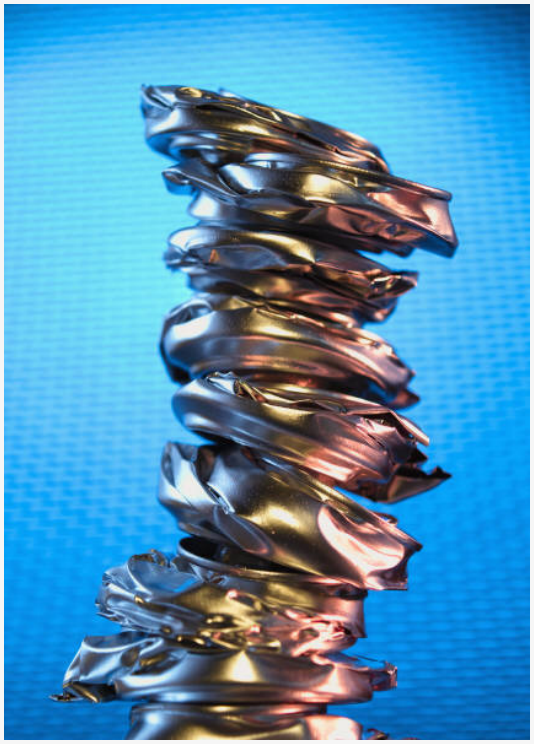
Breach – *New Definition!*

- A breach of PHI arises when there is an impermissible use or disclosure of PHI, unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a *low probability* that the PHI has been *compromised* (or one of the other exceptions to the definition of breach applies).
  - The proposed harm standard is replaced with a risk assessment standard.

(*See* HHS Omnibus Final Rule, January 17, 2013)

Avoid Breach – Encrypt it!

- Avoid a breach by rendering otherwise unsecured protected health information **unusable**, **unreadable**, or **indecipherable** to **unauthorized individuals**.
- OCR's "gold standard" – **Encryption** per standards set by National Institute of Standards and Technology (NIST)
- OCR guidance on the NIST standards for making unsecured PHI unusable, unreadable, or indecipherable: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.



Security Risk Assessment

- Safeguards should focus on:
  - prevention
  - detection
  - containment and
  - correction
- of potential security violations

Security Risk Assessment

- Assessment must be “environment specific”
  - Analyze the needs in light of the environment
  - Implement safeguards appropriate to the environment

Security Risk Assessment

- Environment considerations:
  - Size and complexity of operations
  - Hardware and software infrastructure
  - Costs of security measures
  - Likelihood & impact of potential risks to ePHI

Security Risk Assessment

- To reduce the vulnerability to a breach of ePHI to a reasonable and appropriate level, EHs and EPs must implement appropriate security measures in three areas:
  1. administrative
  2. physical
  3. technical

Administrative Measures

- **A security official** responsible for developing and implementing security policies and procedures.
- **Policies and procedures** that authorize access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).
- **Training workforce members** about the security policies and procedures.
- **Appropriate sanctions** against workforce members who violate the policies and procedures.
- **Periodic assessments** of how well security policies and procedures meet Security Rule requirements.

Physical Measures

- **Limit physical access** to facilities while ensuring that authorized access is allowed.
- **Policies and procedures** to
  - specify proper use of and access to workstations and electronic media;
  - address the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of ePHI

WYATT TARRANT & COMBS LLP

Technical Measures

- **Policies and procedures**:
  - allowing only authorized persons to access ePHI;
  - ensuring that ePHI is not improperly altered or destroyed.
- **Electronic measures** to confirm that e-PHI has not been improperly altered or destroyed
- **Hardware, software, and/or procedural mechanisms** to record and examine access and other activity in information systems that contain or use ePHI
- **Technical security measures** to guard against unauthorized access to e-PHI that is transmitted over an electronic network

Security Risk Assessment

- **Document** the chosen security measures and the rationale for adopting those measures

- **Continually review and modify** security measures to meet changes in environment and maintain reasonable and appropriate security protections

WYATT TARRANT & COMBS LLP

Business Associates & Subcontractors Directly Liable

- The HIPAA Omnibus Rule implemented the HITECH Act's requirement that Business Associates and Subcontractors have direct responsibility for complying with the HIPAA Security Rule.

Business Associates & Subcontractors Directly Liable

BAs and BA Subcontractors must:

- Develop written security program that describes how they will meet each of the standards, safeguards and requirements, including:
  - Technological controls (e.g., passwords, firewalls, physical facility controls) restricting access to HIT data
  - Policies and procedures
  - Workforce training
  - Updates to security program to respond to new security risks

Patient Portal Risks

- HIPAA Security Rule compliance
  - activate firewalls, install encryption
  - can the patient portal software vendor guarantee its own HIPAA Security Rule compliance
- Business Associate Agreement (if vendor to store or have access to ePHI)

Patient Portal Legal Pitfalls

- Vendor access to ePHI for marketing? "NO" – place this in writing
- Charging for access or online consults? check third-party payor contracts
- Online advertising for other providers, vendors or medical devices and products? Consider ethical, anti-kickback, state anti-fee splitting and Sunshine Act issues

Heightened Penalties & Enforcement

- Tiered penalty structure
- $100 to $50,000 per violation, depending on culpability of the CE or BA, up to $1.5M cap per calendar year for multiple violations
- Criminal penalties up to 10 years in prison

Heightened Penalties & Enforcement

- If violation is attributable to situations where the CE or BA knew or should have known had it exercised reasonable diligence to discover the violation, the minimum penalty is $1,000 per violation.
- A CE can be held liable for violations of its BAs; under agency law, BAs can be held liable for violations of its Subcontractors.

Factors Impacting the Amount of Penalty

- Number of individuals affected
- Time period over which violation occurred
- Did violation cause physical or reputational harm
- Did violation hinder patient's ability to receive health care
- Previous indications of noncompliance
- Corrections of previous noncompliance
- Did you play well with OCR
- Responses to prior complaints
- Would a large penalty put you out of business

Conduct Risk Assessment to Reduce Risk of Exposure

- **Biggest reason Covered Entities face problems during OCR investigation of data breach: The failure to conduct a Security Rule Risk Assessment.**
- Identify all vendors who have access to individually identifiable health information, and get a written Business Associate Agreement in place on or before September 22, 2013, and take steps to ensure that such vendors are protecting this information according to the new HIPAA Omnibus Rule.
- Covered Entities can be held liable for violations of their Business Associates. Business Associates can be held liable for violations of their subcontractors and so on.

Government Audits

- Office of Civil Right (OCR) audits
  - OCR HIPAA Audit program: Analyzes selected Covered Entity (and eventually BA) processes, controls, and policies of pursuant to the HITECH Act audit mandate.
  - Comprehensive audit protocol available at:

    http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Office of Inspector General (OIG) Work Plan for 2013
  - Will audit EHR incentive payments for a failure to meet Meaningful Use criteria related to compliance with HIPAA Security Rule Security Rule risk assessment.

WYATT TARRANT & COMBS LLP

Resources

- HIPAA Security Rule Risk Assessment, 45 C.F.R. §§ 164.308(a)(1)(ii)(A)
- HHS Office of Civil Right Guidance on Risk Analysis Requirements under the HIPAA Security Rule: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- CMS Covered Entity Decision Tree: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/coveredentitycharts.pdf
- OCR Enforcement: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
- OIG 2013 Work Plan (pp. 51, 117, 131): https://oig.hhs.gov/reports-and-publications/archives/workplan/2013/Work-Plan-2013.pdf
- HHS HIPAA/HITECH Omnibus Final Rule released January 17, 2013: https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf

THANK YOU!

Kathie McDonald-McClure
Wyatt, Tarrant & Combs, LLP
500 West Jefferson Street, Suite 2800
Louisville, KY 40202
(502) 562-7526
kmcclure@wyattfirm.com

Visit Wyatt's **HITECH Law Blog** @
www.healthitlawblog.wordpress.com

THIS IS AN ADVERTISEMENT