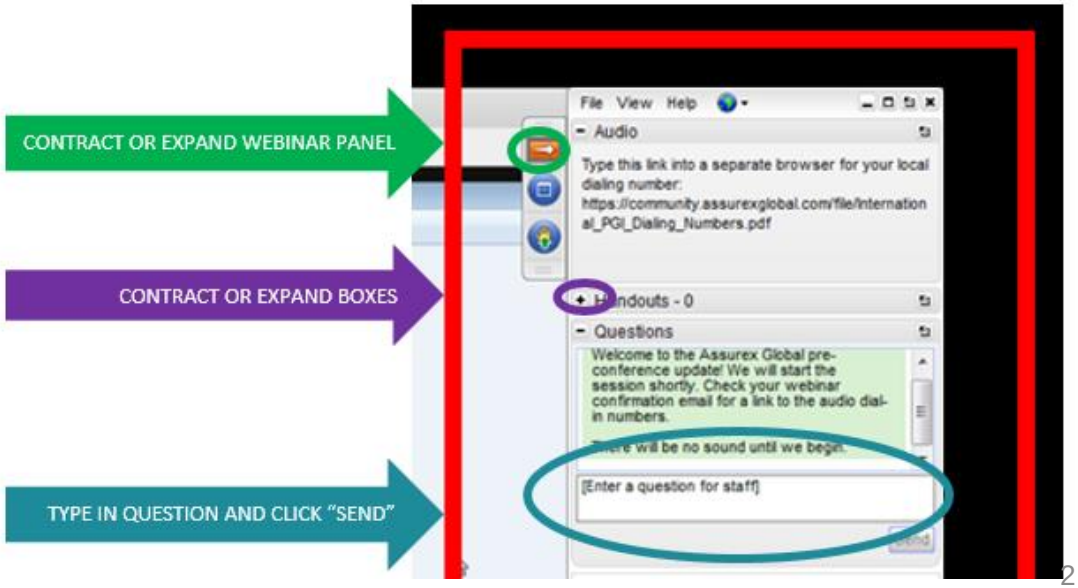
June, 23, 2016

OCR Begins New Phase of HIPAA Audits

Presented by Bob Radecki & Sarah Grcevich
Benefit Comply, LLC

OCR Begins New Phase of HIPAA Audits

- Welcome! We will begin at 3 p.m. Eastern
- There will be no sound until we begin the webinar. When we begin, you can listen to the audio portion through your computer speakers or by calling into the phone conference number provided in your confirmation email.
- You will be able to submit questions during the webinar by using the “Questions” box located on your webinar control panel.
- Slides can be printed from the webinar control panel – expand the “Handouts” section and click the file to download.



Assurex Global Partners

- Catto & Catto
- Cragin & Pike, Inc.
- The Crichton Group
- Daniel & Henry
- Frenkel Benefits
- Gillis, Ellis & Baker, Inc.
- Haylor, Freyer & Coon, Inc.
- The Horton Group
- INSURICA
- Kapnick Insurance Group
- Kinney Pike Insurance
- Lipscomb & Pitts Insurance
- LMC Insurance & Risk Management
- Lyons Companies
- The Mahoney Group
- MJ Insurance
- Parker, Smith & Feek, Inc.
- PayneWest Insurance
- R&R/The Knowledge Brokers
- RCM&D
- RHSB
- The Rowley Agency
- Seacrest Partners
- Starkweather & Shepley Insurance Brokerage
- Woodruff-Sawyer & Co.
- Wortham Insurance & Risk Management

Agenda

- Who Has to Comply
- Why Does it Matter
- HHS OCR HIPAA Audits
- Overview of HIPAA Privacy and Security Rules
- HPID Number

Who Has to Comply?

HIPAA Applicability

- HIPAA applies to all “Covered Entities,” including:
  - Health Care Providers
  - Health Care Clearinghouses
  - Health Plans
    - Health Plans offered by Insurance Companies
    - Employer-sponsored health plans (e.g., medical, dental, prescription, vision, health FSAs, EAPs, wellness, HRAs)
- Plans not subject to HIPAA:

  - Disability, Worker’s Compensation, HSAs

HIPAA Applicability

- When an employer offers a group health plan, HIPAA will apply to the health plan. It will also apply:
  - Indirectly to the employer as Plan Sponsor with respect to the plan administrative functions it performs
  - Directly to any vendors, called Business Associates, to which the employer delegates plan administrative functions or that access PHI as part of their services

HIPAA Applicability

- Employer/Plan Sponsor versus Group Health Plan
  - They are separate legal entities!
  - The Group Health Plan is Covered Entity, Subject to HIPAA
    - No employees
  - Employer/Plan Sponsor is not a Covered Entity, but it is responsible for overseeing and ensuring the health plan's compliance with HIPAA. Therefore, it must:
    - Designate employees to administer the group health plan
    - Distinguish between "health plan information" and "employer information" and establish firewalls between the employees that handle each type
    - Establish policies and procedures
    - Designate a Privacy and Security Official
    - Conduct a Risk Analysis

HIPAA Applicability

- Business Associates (BA)
  - Perform a function on behalf of the covered entity involving the use of PHI
    - Covered entity must enter into a Business Associate Agreement (BAA) with all Business Associates before allowing them to have access to PHI
  - Examples of Business Associates
    - Third Party Administers (TPAs) for self-funded health plans
    - Insurance agents and brokers
    - Wellness vendors
    - Law firm (maybe)
    - IT consulting firm with access to systems containing PHI
  - Business Associates are required to extend privacy and security requirements to their subcontractors through a subcontractor agreement

Employers and HIPAA

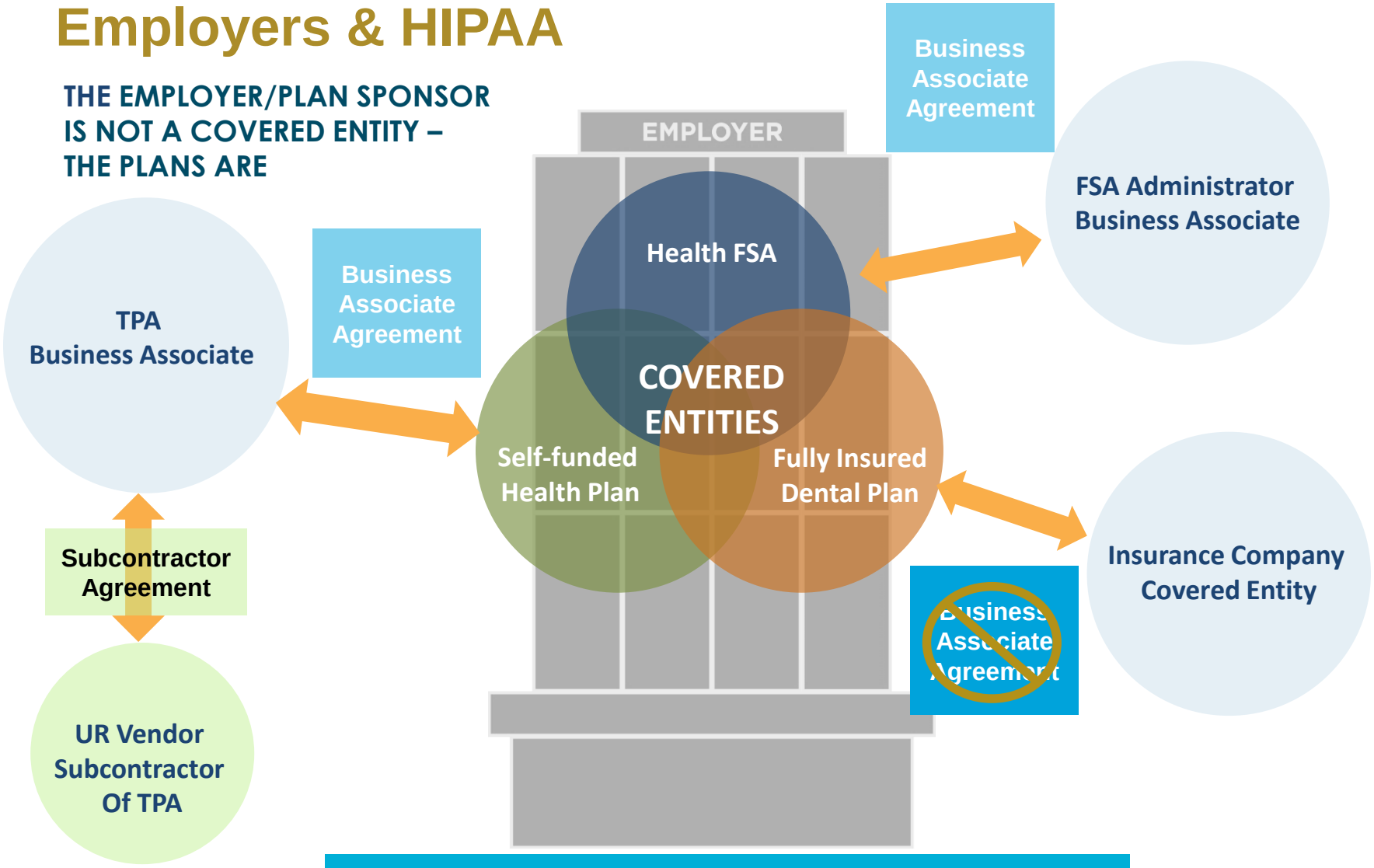
- Fully Insured Plans
  - Both the employer health plan and the insurance carrier are HIPAA Covered Entities
    - No Business Associate Agreement needed between employer and carrier
- Self-Funded Employer Plans
  - Employer-sponsored self-funded health plans are always HIPAA Covered Entities
    - Includes Section 125 Health FSAs and HRAs
    - Employer cannot avoid HIPAA requirements simply by telling TPA not to share PHI with employer
    - TPA is a Business Associate, not a Covered Entity

Employers and HIPAA

- Access to PHI
  - Plan Sponsor is “Hands-Off” PHI (Fully Insured only)
    - Access only “Summary Health Information” & Enrollment/Disenrollment Data
    - Limited privacy obligations, but must still comply with security requirements
  - Plan Sponsor is “Hands-On” PHI (Fully Insured or Self-funded)
    - Access to PHI beyond Summary Health Information & Enrollment/Disenrollment Data
    - Must certify HIPAA compliance to plan before can release PHI
    - Privacy and security requirements apply (but limited obligations for Notice of Privacy Practices if fully insured).

Employers & HIPAA

THE EMPLOYER/PLAN SPONSOR IS NOT A COVERED ENTITY – THE PLANS ARE



Audio Trouble? Dial 1-719-867-1571 Access Code 265313

So What Does an Employer Really Need to Do?

- Establish written HIPAA policies and procedures
  - Privacy policies on appropriate use and disclosure, limited access, physical safeguards, etc.
  - Security policies on securing data, access rights, etc.
  - Polices on dealing with a HIPAA breach
  - Sanctions for employees who violate HIPAA policies
- Designate privacy and security officials
- Create/update plan documents, notice of privacy practices, business associate agreements, etc.
- Conduct security risk assessment
- Provide HIPAA training for employees who are involved in the operation of the health plan

Common Employer Misperceptions

- All I need to do is send a Notice of Privacy Practices
- My insurance company sends a privacy notice so I don't have to
- All I need to do is have my employee attend HIPAA training
- I am fully insured so I don't have to do anything
- I am a small employer so HIPAA does not apply to me

Why Does It Matter

HIPAA Enforcement

- HIPAA enforced by Department of Health and Human Services Office of Civil Rights (OCR)
  - Enforcement has been complaint driven
    - Privacy notices have HHS contact information
    - HHS has a website where individuals can report violations
    - OCR investigates the complaints
- HITECH increases enforcement of HIPAA
  - HHS required to conduct periodic compliance audits – Phase 2 Audits of covered entities and business associates are currently underway
  - Penalties collected with be used to finance additional enforcement
  - Significant increase in potential penalties

HIPAA Privacy & Security Penalties

HIPAA Violations	Penalties	
Civil Penalties	**Each Violation**	**All violations of an identical provision in a calendar year**
Due to unknowing violation	$100 - $50,000	$1,500,000
Due to reasonable cause but not willful neglect	$1,000 - $50,000	$1,500,000
Due to willful neglect that is timely corrected	$10,000 - $50,000	$1,500,000
Due to willful neglect not timely corrected	$50,000	$1,500,000
Criminal Penalties	**Fines**	**Imprisonment**
Clearly applicable to individual employees (not just the entity) – for “knowing misuse”	$50,000 - $250,000	1-10 years

HHS OCR Audit Details

- OCR Audits Phase I
  - 2011 – 2012 pilot audit program
  - 115 Covered Entities audited
- OCR Audits Phase II
  - Broad rage or CEs selected and send and email requesting information
    - Sample of request - http://www.hhs.gov/sites/default/files/ocr-address-verification-email.pdf
    - CE must complete a screening questionnaire
    - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html
  - From this pool CEs and Business Associates will be selected for Desk audit to be completed in 2016
  - Some audits will include follow up on-site audits

HHS OCR Audit Details

- OCR Audits Phase II (cont.)
  - HHS has published a detailed description of Phase II Audit Protocol
    - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
  - HHS protocol document includes description of what auditors will be looking for – Here are a few examples:
    - *"Obtain and review policies and procedures regarding uses and disclosures. Evaluate whether the uses and disclosures of PHI are consistent with the entity's notice of privacy practices."*
    - *"Does the covered entity enter into business associate contracts as required? Do these contracts contain all required elements? Obtain and review policies and procedures related to the identification of business associates and the creation and establishment of business associate agreements."*
    - *"Obtain and evaluate group health plan documents to determine if they restrict the use and disclosure of PHI to the plan sponsor"*

HIPAA Privacy and Security Basics

HIPAA Basics

- What is PHI?
  - PHI stands for “Protected Health Information,” which is individually identifiable health information that is created, maintained, or transmitted by a covered entity.
  - Health Information is broadly defined
    - Relates to the provision of care to, physical or mental health of, or payment for the provision of health care to an individual.
    - Information can be health information even if there is no diagnosis or condition referenced
    - Includes genetic information
  - Health information is individually identifiable if it identifies the individual (or if there is a reasonable basis to believe that the information could be used to identify the individual).
    - HHS has established 18 separate identifiers that must be removed in order for health information to be considered “de-identified” and therefore not individually identifiable.
    -

HIPAA Basics

- What information is not PHI?
  - Enrollment/disenrollment information held by the employer (but will become PHI in the hands of the health plan!)
  - De-identified information (as determined by removal of 18 identifiers or an actuarial analysis
  - Employment records
  - Medical information held by the employer that is unrelated to the health plan (e.g. medical documentation for sick leave, drug test results)

HIPAA Privacy Rules

HIPAA Privacy Rule

- HIPAA restricts the use of PHI
  - To certain uses allowed by the law
  - To times when the individual gives a specific authorization to use the information
- Uses allowed without an individual's authorization
  - Treatment, Payment & Health Care Operations (TPO)
    - For our purposes this means that the plan can use PHI for legitimate plan administration purposes, but other uses are strictly limited
  - Other uses allowed without an individual's authorization
    - Required by law, public health, etc.

HIPAA Privacy Requirements

1. Organized Health Care Arrangement
2. Privacy Official
3. Policies and Procedures
4. Group Health Plan
5. Health Plan Identifier Number
6. Uses and Disclosures
7. Minimum Necessary
8. Authorizations
9. Personal Representatives
10. Business Associates
11. Limited Data Set
12. De-Identification
13. Notice of Privacy Practices
14. Safeguards
15. Breaches
16. Complaints
17. Access
18. Accounting
19. Amendments
20. Confidential Communication
21. Restrictions
22. Workforce Training
23. Sanctions & Mitigation

HIPAA Privacy Rule

- What can the health plan release to or share with the plan sponsor/employer?
  - Enrollment/disenrollment information
  - PHI (for plan administrative functions)
    - Requires plan amendment, certification and firewall
  - De-identified information
  - Summary health information
    - Health plan information that has most individually identifiable information removed
  - PHI (pursuant to an authorization)

Employer Use and Disclosure of PHI Issues

- Common Employer Use & Disclosure Issues
  - Use of PHI for employment purposes prohibited without authorization
    - FMLA
    - Health related work rules
  - Spouse or adult children
    - Restrictions on what can be disclosed to spouse
      - Limited to that individual's own information unless there is an authorization
    - Additional information can be disclosed to "subscriber"
      - Reimbursement related information
      - EOBs example

HIPAA Security Rules

HIPAA Security Rules

- Security Standards and Implementation Specifications
  - The Security Rule contains 22 standards that must be addressed
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
    - Organizational, Policies and Procedures and Documentation Requirements
- Security Risk Analysis
    - Employers required to conduct a HIPAA security risk analysis
- Security measures are appropriate and reasonable
  - Considerations - Size, complexity, mission, purposes of EPHI created, maintained, sent and received…..

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

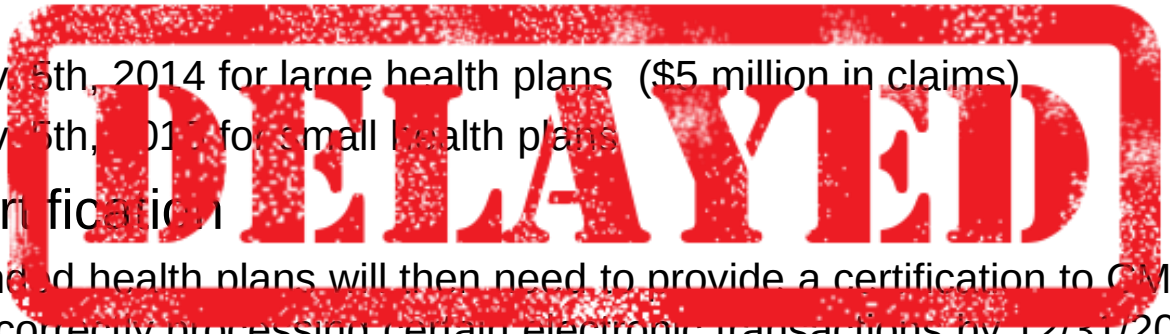
Business Associate Contract or other arrangement	164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	164.314(b)(1)	Implementation Specifications	(R)

Policies and Procedures	164.316(a)		(R)
Requirements for Group Health Plans	164.316(b)(1)	Time Limit	(R)
		Availability	
		Updates	(R)

Health Plan ID Number

Health Plan ID Number

- Self-funded Employers Must Get an HPID
  - HIPAA requires Covered Entities (CE) to follow specific standards for certain electronic transactions
  - Most self-funded health plans must obtain a Health Plan ID Number (HPID) from CMS
    - Nov 5th, 2014 for large health plans ($5 million in claims)
    - Nov 5th, 2015 for small health plans
- 2015 Certification
  - Self-funded health plans will then need to provide a certification to CMS that the plan is correctly processing certain electronic transactions by 12/31/2015



Review – What Does an Employer Really Need to Do?

- Establish written HIPAA policies and procedures
  - Privacy policies on appropriate use and disclosure, limited access, physical safeguards, etc.
  - Security policies on securing data, access rights, etc.
  - Polices on dealing with a HIPAA breach
  - Sanctions for employees who violate HIPAA policies
- Designate privacy and security officials
- Create/update plan documents, notice of privacy practices, business associate agreements, etc.
- Conduct security risk assessment
- Provide HIPAA training for employees who are involved in the operation of the health plan

Resources

- **Government Resources**
  - HHS HIPAA Privacy Page
    - http://www.hhs.gov/hipaa/for-professionals/privacy/
  - HHS HIPAA Security Rule
    - http://www.hhs.gov/hipaa/for-professionals/security/
  - HHS HIPAA Audit Program Page
    - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/

- **Private Resources**
  - EBIA HIPAA Manual
    - http://store.tax.thomsonreuters.com/accounting/Pension-and-Benefits/EBIAs-HIPAA-Portability-Privacy-and-Security/p/102834512
  - KnowHIPAA.com
  - HIPAAcow.org – HIPAA collaborative of Wisconsin

Assurex Global Partners

- Catto & Catto
- Cragin & Pike, Inc.
- The Crichton Group
- Daniel & Henry
- Frenkel Benefits
- Gillis, Ellis & Baker, Inc.
- Haylor, Freyer & Coon, Inc.
- The Horton Group
- INSURICA
- Kapnick Insurance Group
- Kinney Pike Insurance
- Lipscomb & Pitts Insurance
- LMC Insurance & Risk Management
- Lyons Companies
- The Mahoney Group
- MJ Insurance
- Parker, Smith & Feek, Inc.
- PayneWest Insurance
- R&R/The Knowledge Brokers
- RCM&D
- RHSB
- The Rowley Agency
- Seacrest Partners
- Starkweather & Shepley Insurance Brokerage
- Woodruff-Sawyer & Co.
- Wortham Insurance & Risk Management

Thank you.

June, 23, 2016

OCR Begins New Phase of HIPAA Audits

Presented by Bob Radecki & Sarah Grcevich
Benefit Comply, LLC