HIPAA Privacy and Security for Employers in the Age of Common Data Breaches

April 30, 2015

Assurex GLOBAL

HIPAA Privacy and Security for Employers in the Age of Common Data Breaches

- 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.

HIPAA Privacy and Security for Employers in the Age of Common Data Breaches

April 30, 2015

Assurex Global Partners:

- Catto & Catto
- Celedinas Insurance Group
- Cottingham & Butler
- Cragin & Pike, Inc.
- The Crichton Group
- Engle-Hambright & Davies
- 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
- Roach Howard Smith & Barton
- The Rowley Agency
- Starkweather & Shepley Insurance Brokerage
- Woodruff-Sawyer & Co.
- Wortham Insurance & Risk Management

Assurex GLOBAL

Agenda

- HIPAA Background
- Privacy and Security Basics
- Privacy Rules 101
- Security Rules 101
- HIPAA Breach Notifications
- HPID Update
- HIPAA Compliance Summary

Los Angeles Times
Business / The Economy Hub

Anthem is warning consumers about its

THE TENNESSEAN
A GANNETT COMPANY

Search

HOME | NEWS | COUNTIES | SPORTS | BUSINESS | MUSIC | TRAVEL | LIFESTYLE | OPINION | OBITUARIES | TPA PUBLIC NOTICES | USA TODAY

Community Health Systems data breach affects 4.5M

TIONS | HOME | SEARCH

The New York Times

BUSINESS DAY

Premera Blue Cross Says Data Breach Exposed Medical Data

By REUTERS MARCH 17, 2015

Assurex GLOBAL

Audio trouble? Dial 1-719-867-1571 Access Code 265313
Copies of this presentation are available through your benefits advisor.

HIPAA Background

HIPAA History

Health Insurance Portability and Accountability Act of 1996

HIPAA Title II Administrative Simplification

- Privacy Standards April 14, 2003
- Electronic Data Interchange Standards ("EDI") October 16, 2003
- Security Standards April 20, 2005

Amended by the American Reinvestment and Recovery Act (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (2009)

Omnibus HIPAA Final Rule (January 25, 2013)

HIPAA Background

- HIPAA applies to all “Covered Entities”
  - Health Care Providers
  - HMOs, Insurance Companies
  - Employer sponsored health plans
    - Medical
    - Dental
    - Prescription drug plans
    - Vision
    - HFSA
    - Some EAPs
    - HRA
    - Most Long Term Care Plans
  - Plans not subject to HIPAA
    - HSA, life insurance, disability & workers compensation

Employers and HIPAA

- Fully Insured Plans
  - Both the employer health plan and the insurance carrier are HIPAA Covered Entities
    - No BA 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

Employer Plans and HIPAA

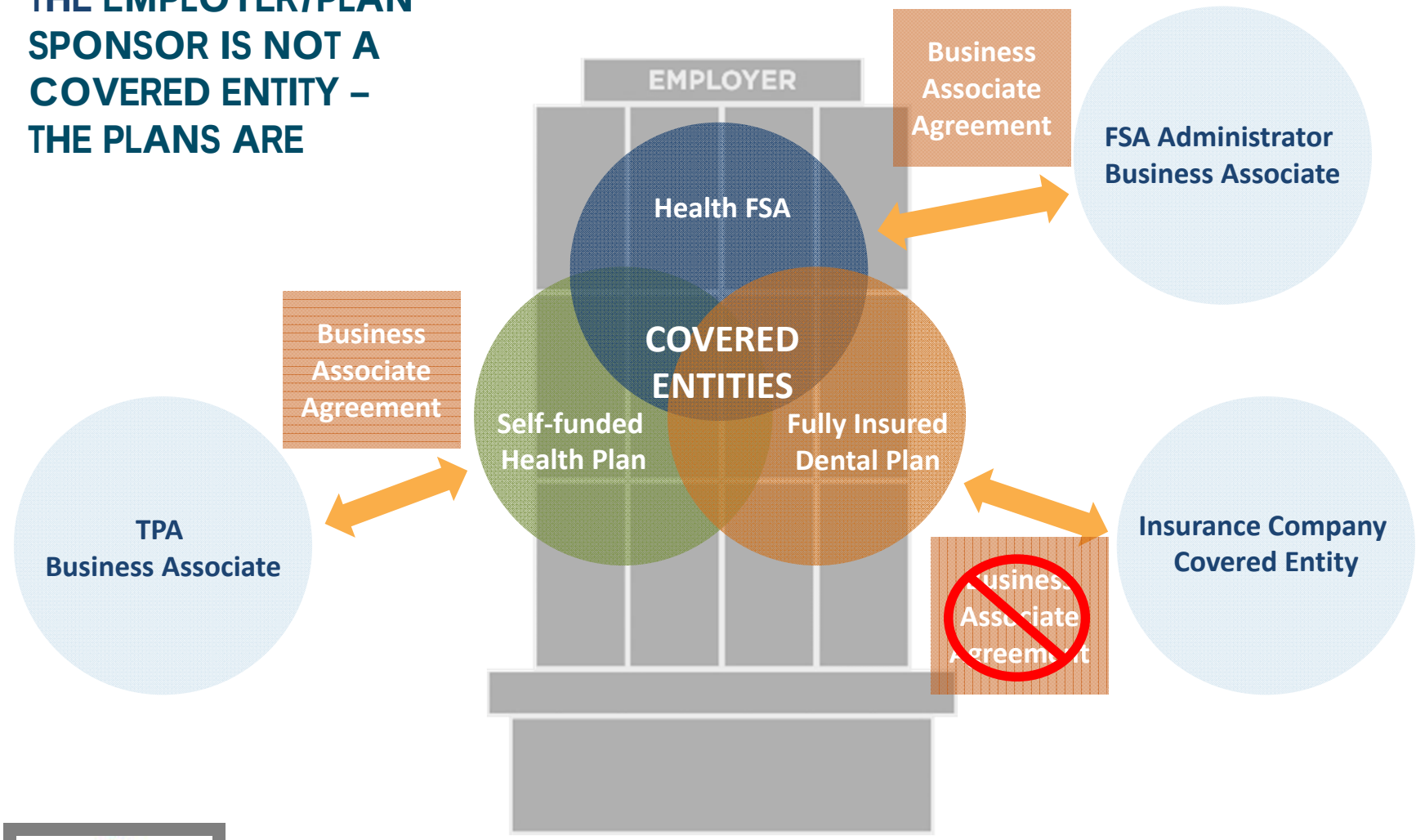
- Employers with Fully Insured Plans
  - "Level 1" Employers
    - Access only "Summary Health Information" & Enrollment Data
    - Summary Health Information is health plan information which contains no individually identifiable information
    - Limited compliance obligations
  - "Level 2" Employer
    - Have access to individually identifiable information
    - Must certify HIPAA compliance to carrier before carrier can release individually identifiable information
    - Subject to similar requirements related to PHI as self-funded employers

Business Associates

- Business Associates (BA)
  - Perform a function on behalf of the covered entity involving the use of PHI
    - CE 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 vendor (some)
    - Law firm (maybe)
    - IT consulting firm depending on what they do with PHI
    - Other vendors

EMPLOYERS & HIPAA

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



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 have access to PHI

HIPAA Privacy and Security Basics

Audio trouble? Dial 1-719-867-1571 Access Code 265313
Copies of this presentation are available through your benefits advisor.

What is PHI?

- Protected Health Information (PHI)
  - Individually identifiable information
  - Related to health or condition of an individual, or the provision or payment for health care
  - Is created or received or maintained by a covered entity
- Electronic PHI (ePHI)
  - PHI that is transmitted electronically or maintained in electronic media

What is PHI?

- What IS PHI?
  - Health insurance enrollment application
  - Report that shows who enrolled in what plan
  - A staff person mentioning to another staff that the plan paid a claim to Burnsville Family Physicians for Bob Radecki
  - A claim report from a dental insurance carrier that contains I.D. numbers
  - An email from an employee that contains details about a health plan claim payment
- What is NOT PHI
  - FMLA medical certification
  - Results from employee drug testing
  - Workers' compensation information
  - Life insurance application

HIPAA Privacy Rules 101

Audio trouble? Dial 1-719-867-1571 Access Code 265313
Copies of this presentation are available through your benefits advisor.

HIPAA Privacy Rules

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

Use and Disclosure of PHI

- HIPAA restricts the use of an individual's PHI
  - To certain uses allowed by the law
  - To times when the individual gives a valid authorization to use the information
- Uses allowed without an individual's authorization
  - Treatment, Payment & Health Care Operations (TPO)
  - Disclosures to a Business Associate
  - Other (i.e. required by law, public health, etc.)

Employer Specific Issues

- 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

Employer Specific Issues

- Employers Use of PHI for Other Purposes
  - PHI may not be used by employer for employment related activities unless the individual specifically authorizes the use
    - Job related physicals
    - FMLA
    - ADA
  - Employers must be careful about disclosures involving spouses and adult children
- Access to PHI
  - Limiting other employee access to PHI
  - Does the CFO need identity specific health information???

HIPAA Administrative Rules

- The Privacy Notice
  - Plans must send notice of privacy practices (NPP) to individuals upon enrollment
    - One notice to participating employee satisfies requirement for covered family members
    - Many employers depend on carrier to send NPP for fully-insured plans – however you should review carrier's NPP
    - Carrier NPP may not be applicable to employer's plan
  - A reminder that the NPP is available must be sent at least every 3 years
- The Business Associate Agreement (BAA)
  - Who are the plans Business Associates?
  - Does the plan have a BAA in place with the BA?
  - Did the plan create its own BAA or use one provided by the BA
  - Specific BAA language important to handling of breaches (more later!)

HIPAA Security Rules 101

Audio trouble? Dial 1-719-867-1571 Access Code 265313
Copies of this presentation are available through your benefits advisor.

HIPAA Security Rules

- Security Standards and Implementation Specifications
  - The Security Rule contains a number of standards that must be addressed
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
    - Organizational Policies and Procedures and Documentation Requirements
- 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)

Security Compliance Road Map

- Perform risk analysis (required by HIPAA security rules)
- Assign a security official
- Amend Business Associate Agreements
- Implement reasonable steps and develop policies and procedures to address HIPAA security standards
- Train appropriate staff

Breach Notification Rules

Breach Notification

- HITECH Breach Notification Requirements
  - First effective September 2009
- Definition of Breach
  - "the acquisition, access, use, or disclosure of PHI in a manner
    - Not permitted under HIPAA
    - Compromises the security or privacy of the PHI
  - Breach excludes inadvertent, unintentional, or unable to retain PHI
  - When there has been an "incident", a breach is assumed unless it can be shown there is a "low probability" of harm to individual

Breach Notification

- The Act defines “unsecured PHI” as
  - PHI that is not secured through the use of a technology or methodology specified by HHS
    - HHS has specified encryption and destruction for rendering PHI unusable
    - Safe harbor for secured PHI
      - Loss of this type of “secure” PHI would not require a breach notification

Breach Notification

- If there has been a “breach of PHI”
  - Notification to individuals
    - Without unreasonable delay and in no case later than 60 calendar days
  - Notification to the HHS
    - 500+ individuals: employer to notify HHS immediately
    - Less than 500 individuals: employer maintain a log and annually submit to HHS
    - All breaches of more than 500 are posted on HHS breach website
  - Notification to the media
    - Breach of more than 500 residents of a State

Breach Notification

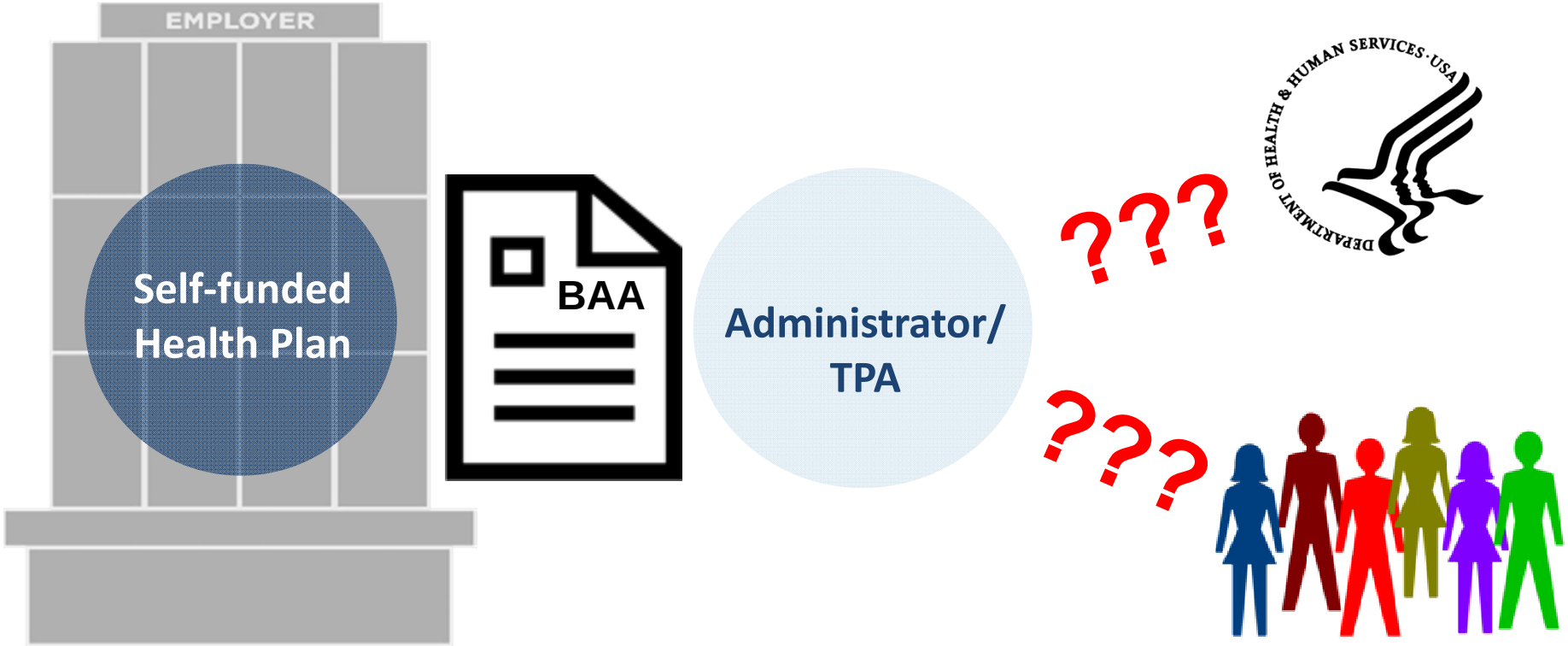
- Who is Responsible for the Breach Notification? - It Depends!
- Fully Insured Plans
  - Breach by carrier – notice is generally the responsibility of the carrier
- Self-funded Plans
  - Breach by administrator/TPA – notice requirements technically fall on the plan (i.e. plan sponsor)
  - However – Business Associate Agreements may assign notice responsibility

Breach Notification

- Who is Responsible for the Breach Notification? - It Depends!
- Fully Insured Plans - Breach by carrier
  - Notice is generally the responsibility of the carrier

Breach Notification

- Self-funded Plans - Breach by TPA
  - Notice is generally the responsibility of the plan (i.e. plan sponsor)
  - However responsibility can be defined in terms of BAA



Breach Notification

- Sample of Breach Language from an Actual BAA
  - Example 1 – Notice Obligations TBD by Covered Entity
    - Business Associate will notify Covered Entity within one (1) business day by telephone or e-mail of any potential HIPAA breach. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the breach, to include…
    - Covered Entity may choose to make any notifications to the Individuals, to the media, and to the Secretary of the U.S. Department of Health and Human Services, or direct Business Associate to make required notices.
    - Business Associate will be responsible for all reasonable costs of all notifications…

Breach Notification

- Sample of Breach Language from Actual BAAs
  - Sample Anthem ASO Breach Language
    - Breach. Business Associate will promptly report to Plan any Breach of Unsecured PHI. Business Associate will cooperate with Plan in investigating the Breach and in meeting the Plan's obligations under the HITECH Act and other applicable Security Breach notification laws. In addition to providing notice to Plan of a Breach, **Business Associate will provide any required notice to individuals and applicable regulators on behalf of Plan, unless Plan is otherwise notified by Business Associate.**

Health Plan ID Number (HPID) Update

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
    - No. 5th, 2014 for large health plans ($5 million in claims)
    - No. 5, 1 or small health plans
- 2015 Certification
  - Self-funded health plans will have to provide attestation to CMS that the plan is correctly processing certain electronic transactions by 12/31/2015

DELAYED

HIPAA Compliance Summary

- 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 handle PHI

Summary

HIPAA Privacy and Security for Employers in the Age of Common Data Breaches

April 30, 2015

Assurex Global Partners:

- Catto & Catto
- Celedinas Insurance Group
- Cottingham & Butler
- Cragin & Pike, Inc.
- The Crichton Group
- Engle-Hambright & Davies
- 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
- Roach Howard Smith & Barton
- The Rowley Agency
- Starkweather & Shepley Insurance Brokerage
- Woodruff-Sawyer & Co.
- Wortham Insurance & Risk Management

Thank you!

Assurex GLOBAL

HIPAA Privacy and Security for Employers in the Age of Common Data Breaches

April 30, 2015

Assurex GLOBAL