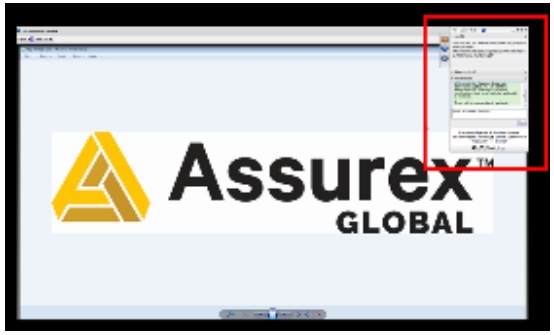
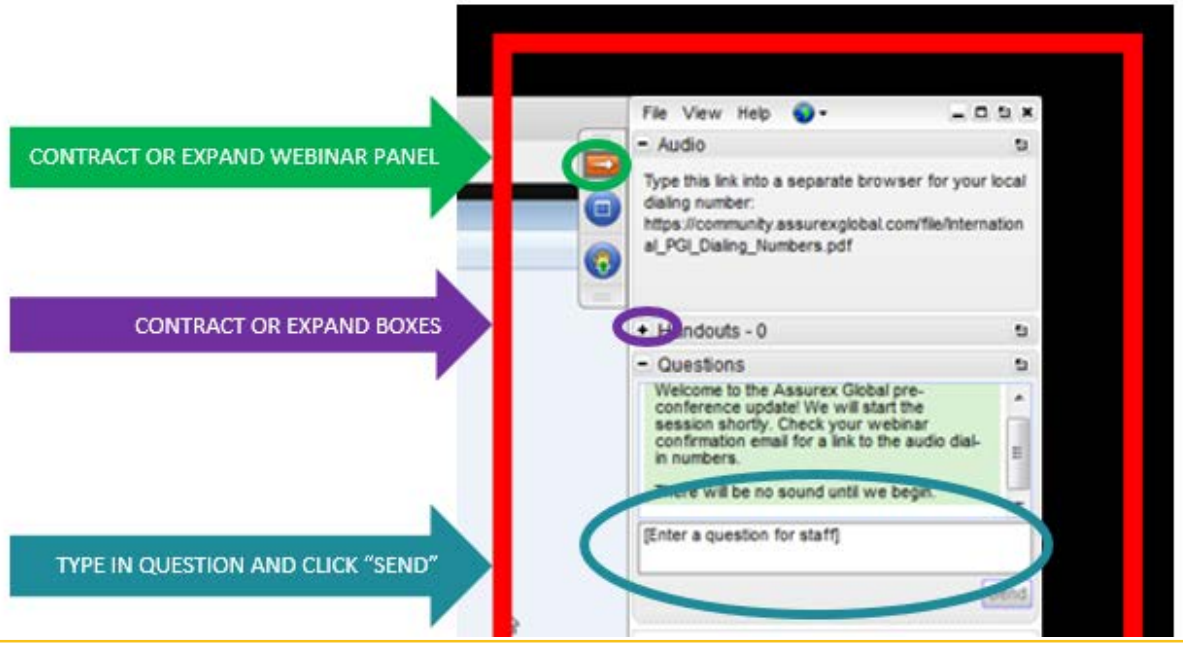
March 29, 2018

Key Principles in HIPAA Compliance

Presented by Benefit Comply

- 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” or “Chat” 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

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

Agenda

- HIPAA Background/Overview
- Key Privacy Requirements
- Use and Disclosure of PHI Issues
- Key Security Requirements
- Breach Notification Rule
- HIPAA Enforcement
- OCR Audit Activities

HIPAA Background/Overview

- Underlying Laws
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - Established key administrative simplification provisions
  - Health Information Technology for Clinical and Economic Health Act of 2009 (HITECH)
    - Modified existing law to increase oversight and enforcement, and strengthened breach reporting requirements

- Key Regulations
  - Privacy & Security Rules (2000 and 2003)
    - Issued pursuant to 1996 law
  - Omnibus Final Rule (2013)
    - Issued pursuant to HITECH– includes updated Privacy and Security Rules, Breach Notification Rule, and HIPAA Enforcement Rule

Who does HIPAA apply to?

- Health Insurance Plans (HMOs, Individual Plans)
- Providers (Doctors, Hospitals)
- Health Care Clearinghouses
- Employer-Sponsored Group Health Plans (Self-Funded and Fully-Insured)
  - The GROUP HEALTH PLAN is the covered entity. Not the employer! (But the employer is responsible for ensuring that each plan complies!)
  - Group health plans include: Medical, dental, vision, prescription drug, health FSAs, HRAs, some EAPs, most wellness programs, and LTC plans.
  - Exception: Plans with fewer than 50 participants that are **self-administered** by the employer (i.e., no TPA).
- Business Associates
  - After HITECH, Business Associates became directly subject to HIPAA privacy and security requirements (prior to HITECH, they were only contractually liable through agreements with covered entities).

HIPAA and Plan Funding

- Yes, HIPAA applies to fully-insured plans!
  - If the plan sponsor has limited access to the plan's protected health information (i.e., only accesses enrollment/disenrollment information and summary health information), then only limited privacy and security obligations apply.
  - If the plan sponsor has access to information beyond enrollment information and summary health information (e.g., claims information), then it is subject to all privacy and security requirements.
- If a plan is self-funded, all of HIPAA's privacy and security requirements apply
- Remember to look at ALL plans offered!
  - Medical plan may be fully-insured, but if employer also offers a health FSA or HRA, these are self-funded plans and therefore subject to all of HIPAA's requirements!

Defining Terms – Protected Health Information (PHI)

- What does “PHI” refer to?
  - Individually identifiable health information.
  - “Health Information” relates to the past, present, or future treatment of an individual.
  - Coverage by a group health plan is considered health information.
  - Therefore, any piece of individually identifiable information that is connected to a group health plan (e.g., name, address, date of birth, etc.) is considered PHI.
  - PHI does NOT just refer to claims, treatment, or diagnostic information.
- What is NOT Considered PHI?
  - Payroll information maintained by the employer in its capacity as employer.
  - Health information gathered by the plan sponsor in its role as employer (e.g., results of drug tests as part of hiring process).
  - Health information related to FMLA or Worker’s Comp claims.
  - Enrollment information gathered by the employer **before** it is transmitted to the health plan (enrollment information obtained from health plan records IS considered PHI).

Key Privacy Requirements

- Assign a Privacy Official
- Determine which employees will administer plan
- Put plan amendment in place to permit access to PHI
- Develop Notice of Privacy Practices
- Develop written policies and procedures
- Train workforce members

Assign a Privacy Official

- Usually an individual in the Human Resources or Benefits Department.
- Responsibilities include:
  - Implementation of HIPAA policies and procedures/compliance oversight;
  - Responding to disclosure of PHI requests;
  - Coordinating breach responses/notifications;
  - Managing/coordinating responses to individual requests with respect to their PHI; and
  - Developing/overseeing Notice of Privacy Practices.
- Privacy Official may delegate certain responsibilities to other staff (but still maintains responsibility for oversight).

Determine Employees Responsible for Plan Administration

- In general, a select number of employees will have actual plan administration responsibilities. These could include:
  - Enrollment assistance
  - Assistance with claims questions
  - Coordinating payment activities with a TPA
- Only those employees who have plan administration responsibilities should have access to PHI.
- These employees MUST be trained on HIPAA privacy!
- A plan amendment must be in place before any employees are permitted to access PHI.

Group Health Plan Amendment

- Remember: the group health plan (not the employer) is the covered entity!
- Therefore, in order for the group health plan to release PHI to the employer, a plan amendment must be put in place.
- There are specific content requirements for the plan amendment. It must:
  - Identify the employees (or classes of employees) who require access to PHI for plan administration;
  - Establish the permitted uses and disclosures of PHI by the plan sponsor, and the plan sponsor's responsibilities with respect to PHI;
  - Require the plan sponsor to:
    - Establish a firewall between employees authorized to access PHI and those who are not;
    - Ensure agents/subcontractors that carry out plan administration functions agree to the same protections for PHI (e.g., via a BAA);
    - Report to the plan any unauthorized use of PHI;
    - Provide a sanctions process for non-compliance with the provisions of the amendment;
    - Make PHI available as necessary to respond to individuals' access rights;
    - Make books and records available for oversight functions; and
    - Provide written certification of compliance.
  - Separate security provisions for a plan amendment (more on these later).

Notice of Privacy Practices (NPP)

- An NPP describes the plan's uses and disclosures of PHI; the individual's rights with respect to their PHI; and the plan's legal duties with respect to PHI.
- The NPP must be provided:
  - To new participants (in enrollment materials);
  - Within 60 days of any revision; and
  - To anyone (participant or non-participant) who requests it.
- A reminder of the NPP must be sent to participants every 3 years.
- Delivery Requirements
  - Must be posted on any benefits/customer service website maintained by the plan (note – this does NOT mean it must be posted on the company's corporate website).
  - Must be delivered to the individual entitled to the notice (OK to combine with other written materials, but can't just be posted centrally).
  - May be provided by email if the recipient has agreed and the agreement hasn't been withdrawn. (If the plan knows the email transmission has failed, it must provide a paper copy of the notice.)

Written Policies and Procedures

- Set of written documents that describe the ways in which the plan complies with the Privacy Rule
- Key items policies should address:
  - Procedures for using and disclosing PHI;
  - Processes for entering into Business Associate relationships;
  - Sanctions processes;
  - Training requirements;
  - Administrative, technical, and physical safeguards;
  - Processes for responding to individuals' requests regarding their PHI;
  - Processes for receiving and responding to complaints; and
  - Breach notification processes.

Privacy Training

- Any workforce member responsible for plan administration who has access to PHI should receive HIPAA training.
- There is no prescribed format in the HIPAA Privacy Rules.
- Typical training covers:
  - Definition of PHI
  - Appropriate uses and disclosures of PHI
  - Processes for safeguarding PHI
  - Sanctions policy
- Training should be provided prior to granting access to PHI, and periodically (e.g., annually) thereafter.

Using and Disclosing PHI

- HIPAA restricts the use of PHI
  - To certain uses allowed by the law; and
  - 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.
- In almost every other case, an individual's written authorization is needed before their PHI can be used or disclosed.

Use and Disclosure of PHI Issues

- Common Employer Use & Disclosure Issues
  - Use of PHI for employment purposes prohibited without written authorization from the individual.
    - FMLA
    - Health related work rules (e.g., drug testing)
  - Spouse or adult children
    - Restrictions on what can be disclosed to spouse or parent of adult child.
      - Limited to that individual's own information unless there is an authorization
    - Limited information may be disclosed to subscriber/policyholder.
      - Falls under "TPO" exception
      - Limited to what is contained on Explanation of Benefits (EOBs)

Key Security Requirements

- Assign a Security Official
- Conduct a Risk Analysis
- Put plan amendment in place to permit access to ePHI
- Develop written policies and procedures
- Develop corporate security training

Assign a Security Official

- Security Official responsibilities include:
  - Performing initial and periodic risk analyses to ensure the confidentiality, integrity, and availability of ePHI;
  - Implementing necessary security controls to safeguard the security of ePHI;
  - Implementing and overseeing the organization's risk management program;
  - Developing process for identifying and responding to known or suspected security incidents;
  - Working with Privacy Official and Legal to identify and respond appropriately to breaches of unsecured ePHI; and
  - Developing and overseeing implementation of written HIPAA security policies and procedures.

Risk Analysis

- What is a Risk Analysis?
  - A Risk Analysis is an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the plan.
  - Looks at where ePHI is housed, and what potential threats/vulnerabilities exist with respect to that data
  - Typically review: **Likelihood** of a threat; **Impact** of a successful threat; and **Cost** of mitigating the threat through additional controls.
  - Results of Risk Analysis help drive implementation of any necessary additional controls to safeguard ePHI
- Typically conducted by Security Official and stakeholders from IT and HR.
- No prescribed frequency for conducting Risk Analysis, but should ideally be performed at least every 3 years or sooner if there are major organizational or regulatory changes.

Key Point: Flexibility of Security Rule

- The Security Rule recognizes that not all organizations are the same
- While all the same security requirements must be addressed, organizations have some flexibility with respect to how they implement controls based on the size, complexity, mission, and capabilities of the organization.
  - For example the Security Rule requires that covered entities have a "contingency plan" in place in the event of a disaster or emergency that ensures the safeguarding and continued availability of ePHI. A hospital's contingency plan will look very different from that of a small employer sponsoring a health plan (the employer's contingency plan might be to call its TPA!).
  - The Security Rule requires things like having a password policy in place, and anti-virus controls in place. But there are no complexity requirements or dictates to use specific antivirus software. Organizations have a lot of flexibility to implement the controls that make most sense for their culture/infrastructure!

Plan Amendment

- Like the Privacy Rule, the Security Rule requires that a plan amendment be in place in order to share ePHI with the plan sponsor.
- Provisions must require the plan sponsor to:
  - Implement administration, physical and technical safeguards to protect the confidentiality, integrity and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan;
  - Ensure that the “firewall” between the plan and the employer is supported by reasonable and appropriate security measures;
  - Ensure that agents and subcontractors to whom the sponsor provides ePHI agree to implement reasonable and appropriate security measures to protect the information; and
  - Report security incidents to the group health plan.

Written Security Policies and Procedures

- Organizations must have written policies and procedures that describe the administrative, technical, and physical procedures in place for complying with the required security controls.
- Key items that must be included:
  - Access controls
  - System activity review, Auditing, and Integrity controls
  - Periodic technical and nontechnical evaluation of security controls
  - Encryption policies
  - Password policies
  - Sanctions policies
  - Workstation use requirements (e.g., Acceptable Use Policy)
  - Security training procedures
  - Security incident response
  - Contingency planning
  - Business Associate requirements
  - Breach identification and notification

Corporate Security Training

- The Security Rule requires that ALL Workforce Members be trained on general security awareness and principles
- Normally, companies can leverage existing corporate training materials for this purpose
- Training should be accompanied by “periodic security reminders” (i.e., security training is an ongoing effort)!
- Three specific items must be addressed:
  - Password Management Procedures
  - Login Monitoring
  - Protection from Malicious Software (Viruses, Phishing, Social Engineering, etc.)

Breach Notification Requirements

- If there has been a “Breach” of PHI
  - Must notify individuals within 60 days.
  - Must log all breaches and submit annual log to HHS.
  - If breach involves more than 500 individuals must notify media and HHS within 60 days.
- Definition of Breach
  - …“the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI.”
  - Must constitute a violation of the Privacy Rule.
  - Exceptions apply for unintentional acquisition, access, or use by employees; certain inadvertent disclosures; and when the covered entity or business associate has good reason to believe the unauthorized recipient would not be able to retain the information.

Breach Notification Requirements

- Breach is assumed to have occurred unless plan can demonstrate a low probability that PHI has been compromised using Four-Factor analysis:
  - Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification;
  - Unauthorized person to whom unauthorized disclosure was made;
  - Whether the PHI was actually viewed or accessed; and
  - Extent to which risk to PHI has been mitigated.

HIPAA Enforcement

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

Privacy and Security Penalties

HIPAA Violations	Penalties	
Civil Penalties	**Each Violation**	**All violations of an identical provision in a calendar year**
Due to unknowing violation	$112 - $55,910	$1,677,299
Due to reasonable cause but not willful neglect	$1,118 - $55,910	$1,677,299
Due to willful neglect that is timely corrected	$11,182 - $55,910	$1,677,299
Due to willful neglect not timely corrected	$55,910 -$1,677,299	$1,677,299
Criminal Penalties	**Fines**	**Imprisonment**
Clearly applicable to individual employees (not just the entity) – for "knowing misuse"	$50,000 - $250,000	1-10 years

OCR Audit Detail

- OCR Audits Phase I
  - 2011 – 2012 pilot audit program
  - 115 Covered Entities audited
- OCR Audits Phase II
  - Broad rage of CEs selected and send an 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 were selected for Desk audit. Some audits to include follow up on-site audits

OCR Audit Detail

- OCR Audits Phase II (cont'd.)
  - 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"*

Assurex Global Partners

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

March 29, 2018

Key Principles in HIPAA Compliance

Presented by Benefit Comply