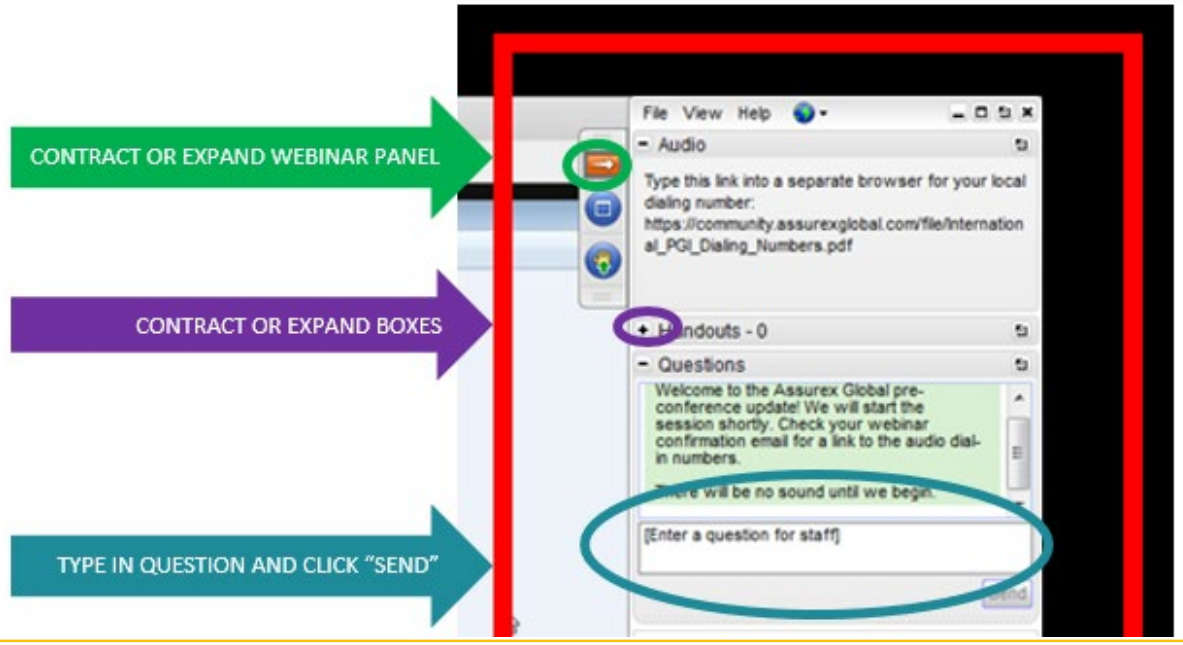
February 2019

HIPAA Privacy and Security Mistakes Employers Make

Benefit Comply, LLC

Compliance Issues Related to Emerging Employee Benefit Strategies

- 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
- Foa & Son
- Gillis, Ellis & Baker, Inc.
- The Graham Co.
- Haylor, Freyer & Coon, Inc.
- Henderson Brothers, Inc.
- The Horton Group
- The IMA Financial Group
- INSURICA
- Kapnick Insurance Group
- Lanier Upshaw, Inc.
- Lipscomb & Pitts Insurance
- LMC Insurance & Risk Management
- Lyons Companies
- The Mahoney Group
- MJ Insurance
- Oswald Companies
- Parker, Smith & Feek, Inc.
- PayneWest Insurance
- Pritchard & Jerden
- R&R/The Knowledge Brokers
- RCM&D
- The Rowley Agency
- Starkweather & Shepley Insurance Brokerage
- Sterling Seacrest Partners
- Woodruff Sawyer

Agenda

- Background
- Employer responsibilities
- Common mistakes (and best practices!)
- Conclusion

Some Background

- HIPAA refers to the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations
- A major part of HIPAA concerns the privacy and security of Protected Health Information (PHI)
  - For our purposes, PHI refers to individually identifiable health information that is related to an employer's health plan
- HIPAA was amended by the Health Information for Clinical and Economic Health Act of 2009 (HITECH)
- Final set of rules (4 of them!) was issued in 2013 – referred to as the "omnibus rule"
  - Included revised Privacy Rule, Security Rule, Enforcement Rule, and new Breach Notification Rule
- HIPAA is enforced by the Office for Civil Rights (OCR) – a division of HHS

Some Background (Cont.)

- HIPAA privacy and security requirements apply to:
  - Covered Entities
  - Business Associates
- Covered Entities include:
  - Insurance Carriers/HMOs
  - Providers
  - **Employer-sponsored health plans (fully-insured and self-funded)**
- The **health plan** is the covered entity (i.e., the legal entity subject to HIPAA)
  - But the employer, as plan sponsor, is responsible for ensuring that its health plans (the covered entities) comply

What do Employers Need to Do?

- High-Level Employer Checklist
  - Identify where PHI is located and limit access
  - Identify Employees responsible for Plan Administration
  - Make sure Plan Document contains necessary HIPAA language
  - Establish & implement safeguards to protect PHI
  - Develop **written** Policies & Procedures
  - Appoint Privacy and Security Officials
  - Develop/Maintain/Distribute Notice of Privacy Practices
  - Conduct Security Risk Assessment
  - Identify/Enter into contracts with Business Associates
  - Conduct Training (Privacy and Security)
- Compliance obligations may differ for some fully-insured plans
  - If employer, as plan sponsor, only has access to summary health information and enrollment information from its fully-insured health plan, may rely on the insurance carrier (also a covered entity) for many compliance obligations
  - Plan Sponsors with access to detailed PHI from fully-insured plan, and plan sponsors of ALL self-funded plans, must comply with all of HIPAA's requirements

Common Mistake: Not Considering ALL Plans

- It's common to think about HIPAA in terms of a medical plan only
- In fact, HIPAA applies to a variety of different health plans, including: Dental, Vision, Prescription Drug, Health FSA, Health HRA, Long Term Care, and many EAPs and Wellness Programs
- If an employer fails to consider compliance for each of these plans, it may miss a crucial requirement
  - The employer may fail to apply appropriate safeguards to PHI from some of its plans if it isn't aware that those plans are subject to HIPAA
  - The employer may assume their compliance obligations are limited if they don't receive detailed PHI from their fully-insured medical plan. But if that employer also sponsors a self-funded plan (e.g., an FSA or HRA), then additional requirements will apply

Best Practices for Evaluating Plans

- Review each plan sponsored and determine whether it is a “health plan” subject to HIPAA privacy and security requirements
- All health plans subject to HIPAA must be addressed in the employer’s compliance efforts
- For administrative ease, the employer may designate its various plans an “Organized Health Care Arrangement,” or OHCA. This means:
  - A single set of policies and procedures for all plans
  - A single Notice of Privacy Practices for all plans
  - A single Privacy Official and Security Official for all plans
  - Etc.

Common Mistake: Just Doing One Piece

- It is not enough to JUST:
  - Send a Notice of Privacy Practices
  - Conduct Training
  - Name a Privacy Official
  - Develop Policies and Procedures
  - Etc.

- HIPAA compliance consists of multiple steps and ongoing efforts. Each requirement is one piece of a larger whole.

Ensuring Total Compliance

- High-Level Employer Checklist
  - Identify where PHI is located and limit access
  - Identify Employees responsible for Plan Administration
  - Make sure Plan Document contains necessary HIPAA language
  - Appoint Privacy and Security Officials
  - Establish & implement safeguards to protect PHI
  - Develop **written** Policies & Procedures
  - Develop/Maintain/Distribute Notice of Privacy Practices
  - Conduct Security Risk Assessment
  - Identify/Enter into contracts with Business Associates
  - Conduct Training (Privacy and Security)
- Review OCR Audit Protocol for guidance on compliance requirements

Common Mistake: Relying Solely on TPA for Compliance

- TPAs are Business Associates, and therefore have an obligation to comply with HIPAA
- Business Associates are also contractually obligated to adhere to the terms of the Business Associate Agreement
- The Plan Sponsor may delegate certain responsibilities to the Business Associate
- But the Plan Sponsor is STILL RESPONSIBLE for ensuring that its plan complies with HIPAA, and must undertake many compliance obligations itself

Best Practices for TPAs

- A Plan Sponsor may delegate certain plan administration functions to its TPAs – e.g., claims processing, assistance with claims/eligibility questions, etc.
- A Plan Sponsor should clearly delineate between the obligations it assumes, and the obligations it delegates to its TPA
- Duties delegated to the TPA should be clearly outlined in the Business Associate Agreement
- Before entering into a Business Associate Agreement, a Plan Sponsor should exercise reasonable due diligence to ensure the TPA can reliably carry out these duties
- The Plan Sponsor should conduct periodic oversight of its TPA to ensure that the TPA is adhering to the terms of the BAA

Common Mistake: Not Conducting Risk Analysis

- A Security Risk Analysis is an exercise that reviews an organization's existing security controls and compares them to the requirements of the HIPAA Security Rule
- Conducting a Risk Analysis is **required** by the Security Rule
- Having security policies and procedures in place is not enough
- In fact, security policies and procedures should be developed based on the results of a risk analysis – not vice versa!
- Failing to conduct an adequate risk analysis can increase the risk of a breach, exposing an employer to significant civil penalties

Risk Analysis Best Practices

- There is no prescribed method for a Risk Analysis, but a typical process will involve the following:
  - A review of all systems/applications/files that are used to store, transmit, or maintain electronic Protected Health Information (ePHI)
  - A review of each security standard/implementation requirement under the Security Rule
  - A comparison of the organization's security controls with HIPAA's security standards
  - A determination of risk to the organization's ePHI based on its existing security controls, taking into account the following:
    - The likelihood that a threat could exploit an existing vulnerability
    - The impact (cost, reputation, etc.) to the organization if a vulnerability were exploited
  - Development of a mitigation plan to address issues identified as having a higher risk
- Security Official should review the risk analysis periodically to ensure controls remain sufficient as operations/infrastructure/laws change

Common Mistake: Misidentifying PHI

- Definition of PHI:
  - Individually identifiable health information
  - In practical terms, this means any individually-identifiable information that is part of the employer's health plan's records
- PHI does NOT include employer data
- PHI does NOT include individually identifiable information related to non-health plan programs (e.g., life insurance, worker's comp, disability)
- Any individually identifiable information (e.g., name, date of birth, etc.) can be PHI if it's related to the health plan
- Two common mistakes:
  - Employer definition of PHI is too broad (i.e., including employment data, worker's comp information, FMLA, disability, etc. as PHI)
  - Employer definition of PHI is too narrow (i.e., only Diagnosis or detailed information constitutes PHI)

PHI Best Practice

- Understand which information is and is not PHI
- Apply HIPAA Privacy and Security safeguards to information that **is** PHI
  - Access controls
  - Use and disclosure policies and procedures
  - Security controls
  - Etc.
- (And remember that other privacy/confidentiality laws might apply to other types of sensitive information, even if HIPAA does not apply)

Common Mistake: Failing to Identify BAs

- What a Business Associate IS: A Person or Entity who performs plan administration functions on behalf of the covered entity, and who accesses PHI in performing those functions
  - Common Business Associates: TPAs, Brokers, Payroll Vendors
  - A compliant BAA **must be in place** before an PHI is shared!
- What a Business Associate is NOT: A person or entity who is not providing plan administration, and/or who does not need to access PHI as part of its contractual obligations
  - Entities Who Aren't Business Associates: Janitorial Service Providers, Other entities that access sensitive corporate information (if not acting on behalf of the health plan)
  - An NDA is always a good idea – but a BAA is not necessary!
- Commonly Missed Business Associates:
  - Shredding Vendors (Paper and Electronic Media)
  - Cloud Services Providers (including email providers)
  - Attorneys/Employment Advisors

Business Associate Best Practices

- Review all contractual agreements to determine scope of services for each contractor/vendor
- If a vendor is providing any type of plan administration that involves the use of PHI (e.g., claims processing, SaaS for systems that store/transmit/maintain PHI, IT support, assistance with benefit/enrollment/claims issues), then ensure that a valid Business Associate Agreement is in Place
- BAA must contain certain regulatory provisions, including:
  - Scope of the Business Associate's services
  - Permissible Uses and Disclosures of PHI by the Business Associate
  - Requirements for reporting/responding to known and suspected breaches of PHI
- Understand what duties are delegated to Business Associate, and monitor contractual compliance with those provisions

Common Mistake: Not Tailoring the NPP

- The Notice of Privacy Practices describes the plan sponsor's obligations with respect to an individual's PHI, and it describes the individual's rights with respect to their own PHI
- Many plan sponsors of self-funded plans will rely on a generic model notice
  - Generic model notices will meet the minimum content requirements, but may not accurately describe a plan sponsor's actual practices
- Many plan sponsors of fully-insured plans will rely on a carrier's NPP
  - A plan sponsor is only allowed to rely on the carrier's NPP if the plan sponsor is limited to receiving summary health information and enrollment information
  - A carrier's NPP will rarely be tailored to accurately describe a plan sponsor's plan/practices
  - If a plan sponsor has any self-funded plans, the carrier's NPP won't suffice for those plans

Best Practice for NPPs

- Examine all plans offered
- Ensure that all plans subject to HIPAA are addressed by the NPP (Remember the OHCA option!)
- Work with legal counsel to ensure that the NPP accurately describes the plan's practices/operations
- If all plans are fully-insured, and the plan sponsor wishes to rely upon the carrier's NPP, then the plan sponsor should review the NPP to ensure it is comfortable with how the plan is described

Common Mistake: Privacy Training Only

- HIPAA requires that covered entities and business associates provide the following trainings:
  - Training on basic HIPAA Privacy Principles, and the Organization's Privacy Policies, to employees who have access to PHI
  - Corporate Security Training to **ALL employees**

- It is not sufficient to provide training focused only on privacy principles, or to only provide security training to staff with access to PHI

HIPAA Training Best Practices

- HIPAA Privacy Training
  - Ensure all staff with access to PHI are appropriately trained on HIPAA privacy principles and the organization's privacy policies and procedures
    - E.g.: Use and Disclosure policies; safeguarding PHI; caller verification requirements; handling individual rights requests
  - Training should be provided within a reasonable time of hire and periodically (e.g., annually) thereafter
- HIPAA Security Training
  - Generally leveraged as part of corporate security training
  - Training must be provided to ALL employees
  - As part of this standard, organization must implement: Password management processes; processes for preventing/detecting malware; and procedures for monitoring log-in attempts and reporting discrepancies
  - Training should be provided on a regular basis (e.g., annually), with general security reminders/updates issued periodically between more formal trainings

Common Mistake: No Mobile Device Encryption

- OCR has made it clear in its recent audit protocol that it expects covered entities and business associates to properly encrypt their data
- Under HIPAA, loss of an unencrypted mobile device that is used to access/store/receive/transmit PHI could be a breach
- Employees have more access than ever to information via company-issued and personal mobile devices (laptops, phones, tablets)

Encryption (and other mobile device) Best Practices

- Evaluate the company's use of mobile devices as part of its Security Risk Analysis
  - Consider all portable devices (phones, tablets, USB drives, laptops, etc.)
  - Address encryption for data stored on and transmitted by device
  - Consider all ways PHI could be accessed (including via email and browsers)
- If devices are not encrypted, Plan Sponsor should be sure that they are not used to access PHI, and/or can't be removed from the facilities
- Remember: ePHI on a properly encrypted device that is lost/stolen/compromised is considered "secure"
- Also consider:
  - Prohibitions on using public Wi-Fi networks to access data
  - Password requirements for mobile devices
  - Prohibitions on storing data on devices using unapproved applications

Conclusion

- HIPAA compliance involves several steps
- It is important to understand how all of the pieces fit together to ensure that all compliance obligations are met
- Use the following as a starting point:
  - Identify where PHI is located and limit access
  - Identify Employees responsible for Plan Administration
  - Make sure Plan Document contains necessary HIPAA language
  - Appoint Privacy and Security Officials
  - Establish & implement safeguards to protect PHI
  - Develop **written** Policies & Procedures
  - Develop/Maintain/Distribute Notice of Privacy Practices
  - Conduct Security Risk Assessment
  - Identify/Enter into contracts with Business Associates
  - Conduct Training (Privacy and Security)

February 2019

Benefit Comply, LLC

Assurex GLOBAL

assurexglobal.com