WEBINAR TAKEAWAYS:
HIPAA PRIVACY & SECURITY RULES

COMPLIANCE LUNCHBOX
UNPACKING YOUR COMPLIANCE OBLIGATIONS

Key Terms

HIPAA Privacy Rule: Gives an individual certain rights over how their health information may be **used** or **disclosed** by organizations that are subject to the Privacy Rule and protects the **unauthorized use or disclosure** of certain individually identifiable information known as protected health information.

HIPAA Security Rule: Addresses various **physical, technical, and administrative safeguards** that must be implemented by organizations subject to the Security Rule and their Business Associates for protection of the confidentiality, integrity and availability of electronic protected health information.

Protected Health Information (PHI): **Individually identifiable health information** that is held or transmitted by a **Covered Entity** or its **business associate**, in any form or media, whether electronic, paper, or oral.

Covered Entity: This includes an employer-sponsored health plan

What Makes it PHI?

Individually Identifiable

Examples:

- Name
- Address
- Phone Number
- Birth Date
- Social Security Number
- Email Address

+

Health Plan Info

Examples:

- Medical, Dental, Vision Coverage
- Health FSA
- Health Reimbursement Arrangement
- Long-term Care
- Wellness Plan w/ health risk assessment or screening

Key Points

ePHI: PHI in electronic format

Privacy Rule: Applies to all PHI & ePHI

Security Rule: Applies only to ePHI

Health Plans subject to HIPAA Privacy & Security include: Health FSA, HRA, and Wellness plans that include health assessments or screenings

Written policies & procedures: Required for ePHI

Risk Assessment: MUST be performed for ePHI

Risk Management: MUST be documented for ePHI

Business Associate Agreement: MUST be in place for any third-party services that my receive PHI to provide services to your health plan

Notice of Privacy Practices: Required by HIPAA Privacy Rule to make this available

Civil Penalties: Apply to HIPAA Privacy & Security breaches

De-identified PHI: All info that could be used to identify an individual has been removed (no longer considered PHI)

HIPAA Privacy Rule Plan Requirements

(Except for non-retaliation, these do not apply to fully-insured health plans if the employer does not receive any PHI other than enrollment.)

Health Plan Must:

- **Designate a privacy official:** develops & implements policies & procedures
- **Provide a complaint process:** Plan can't retaliate against a person who makes a complaint
- **Provide an assurance of rights:** Plan can't require someone to waive rights to receive benefits
- **Protect the privacy of PHI:** Appropriate administrative, technical & physical safeguards
- **Provide reasonable policies & procedures:** Designed to ensure compliance with Privacy Rule
- **Mitigate harm:** If data is breached, must be mitigated to a practicable or feasible extent
- **Provide workforce training:** Train employees & impose sanctions if failure to comply
- **Provide Notice of Privacy Practices:** Must be available to anyone who asks for it
- **Provide Security Breach Notification:** Without unreasonable delay / Within 60 days of breach
- **Secure Business Associate Agreements:** Imposes specific obligations on third-parties

HIPAA Security Rule Plan Requirements

Covered Entities Must Ensure:

- **Confidentiality:** ePHI protected from unauthorized individuals
- **Integrity:** Valid data is protected against unauthorized modification, insertion, deletion
- **Availability:** Accessible & useable upon demand by authorized entity
- **Administrative, Physical & Technical Safeguards:**
  - **Risk Assessment:** Detailed regimen on how to make decisions about protections
  - **Risk Management system:** How & when to deal with ePHI threats and vulnerabilities

Compliance dashboard®

Information covered in this webinar series is a compilation of generally published information by the Department of Labor and other public agencies regulating employee benefit plans and employee benefit issues. It is not legal advice, and should not be construed as legal advice. If legal advice or other professional assistance is or may be required with regard to any issues referenced in the webinar, the services of a competent legal professional should be sought. This flyer is intended to communicate discussion points from the webinar and is not intended to communicate ERISA in its entirety.

©2018 **Compliance**dashboard®, LLC