Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The Oft-Forgotten Covered Entity: HIPAA Compliance for Group Health Plans

---

Rebecca L. Williams, RN, JD
Partner,
Co-Chair Health Information Practice
Davis Wright Tremaine LLP

Don't Forget

- Covered Entities and Business Associates have direct HIPAA compliance obligations
- But, most Employers have Health Plans with their own HIPAA compliance obligations
- Sometimes Group Health Plans are forgotten… or at least are not a high priority

Agenda

- Who is covered by HIPAA in the Group Health Plan Setting?
- How can information flow?
- HIPAA obligations for Group Health Plans
- Compliance considerations

What is a Covered Health Plan?

- Individual or group plan, private or governmental, that provides or pays for medical care
- Employer-sponsored Group Health Plans/ ERISA plans
- Includes self insured and insured plans

Small Group Health Plan Exception

- Small group health plans
  - Fewer than 50 employees eligible to participate
- Self-administered
- Self-insured

Examples of Covered Health Plans?

- Self Funded and Fully Insured Group Health Plans/Medical Plans
- Vision Care Plans
- Dental Plans
- Health Care Flexible Spending Accounts (FSA)
- Health Reimbursement Arrangements (HRA)
- Health Savings Accts (HSA)
- Prescription Drug (Rx)Plans
- Long-Term Care Plans
- Some Employee Assistance Plans
- Many Wellness Plans

What is Not a Covered Health Plan?

- Workers' Compensation
- Group Universal Life insurance
- Dependent Life
- Basic Life/AD&D
- Short-Term/Long-Term Disability Plans
- Stop Loss/Reinsurance
- Other Property/Casualty Insurance
- Dependent Care Flexible Spending Account
- Severance Pay Plan
- Auto Insurance

Business Associates Group Health Plans

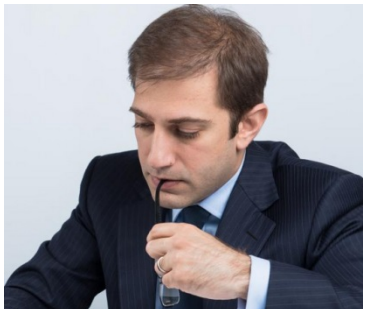
- Perform designated activities, functions, or services
- On behalf of the Health Plan – not solely the Employer
- Create, receive, maintain, or transmit Plan Protected Health Information (PHI)
- In addition to typical Business Associate Agreement requirements, Plans often need to designate responsibilities

Examples of Business Associates

- Typical Business Associates of Health Plans include:
  - Third-party administrators
  - Claims administrators
  - IT vendors
  - Attorneys, accountants, auditors, consultants, actuaries,
  - Document shredding, offsite storage, copier repair vendors, etc.
  - Cloud service providers, computer systems support vendors, data backup storage vendors
  - Some insurance brokers

What about Employers?

- Employers are not Covered Entities or Business Associates simply because of their status as Employers
- Employers may have unique responsibilities
  - As the fiduciary of a Group Health Plan
  - As a Plan Sponsor

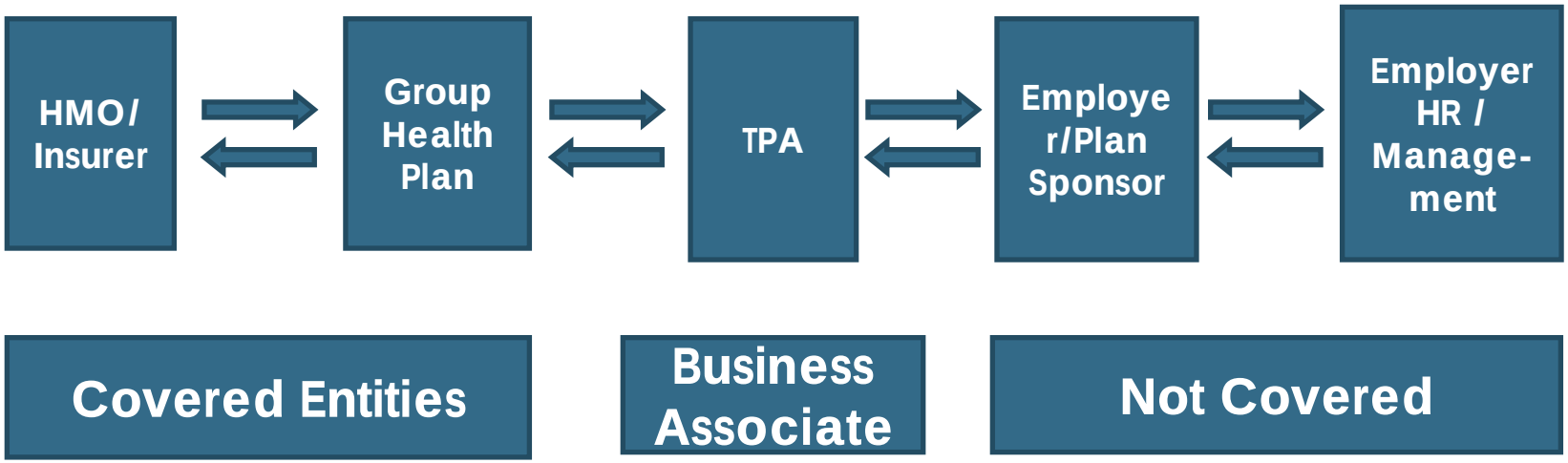


Administrators

How Does HIPAA Affect Employers/Plan Sponsors

- HIPAA applies to the Health Plans sponsored by the Employers/Plan Sponsors
- HIPAA burden depends on Plan Sponsor's role

Who is Covered: Tag You're It

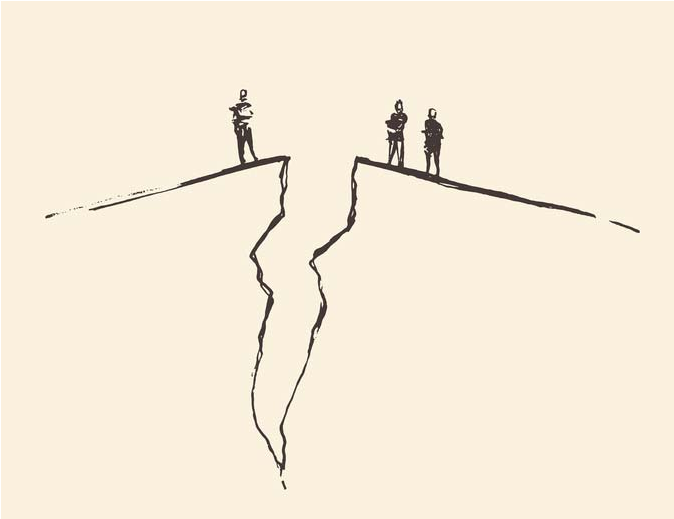


Agenda

- Who is covered by HIPAA in the Group Health Plan Setting?
- How can information flow?
- Obligations for Group Health Plans
- Compliance considerations

Health Plans are Separate

- Health Plans are separate legal entities from the Employer/Plan Sponsors



PHI in the Health Plan Context

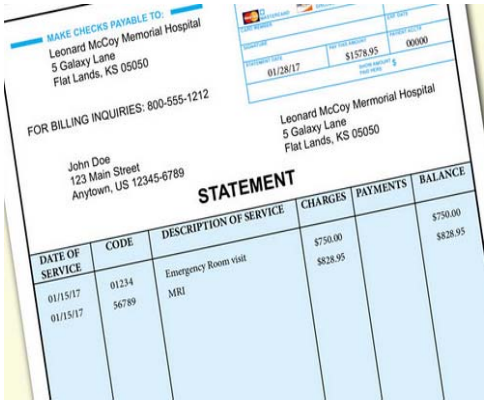
Medical Certification for Sick Leave

Provider treating Patient

PHI

Medical certification to justify leave

Not PHI



Claim for Treatment to Plan

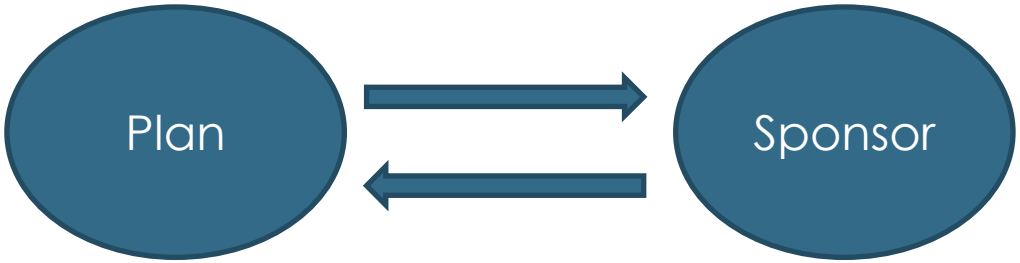
PHI

What Hat are you Wearing?

- Some Workforce may act on behalf of both the Employer and the Plan
- Each Workforce Member needs to know:
  - Acting on behalf of Employer?
  - Acting for the Plan
- Training

Permitted PHI Sharing: Group Health Plan with Plan Sponsor

- Enrollment/ Disenrollment information
- Summary Health Information: Summarize claims history, expenses, or types of claims
  - Upon request
  - For obtaining bids or modifying plan
- With Participant authorization



Information Sharing : Plan Administration

- If the Plan/Plan Sponsor jumps through HIPAA Hoops
- Then Plan may disclose PHI to Plan Sponsor
  - Limited to Plan administrative functions
- Hoop 1: Plan Document Amendment

- Establish permitted uses and disclosures, consistent with HIPAA
- Permit disclosures to Sponsor only with Sponsor certification
- Provide for adequate separation

HIPAA Hoops

- Hoop 2: Plan Sponsor Certification
  - Agree to plan document restrictions
  - Facilitate individual rights
  - Process for resolving issues of non-compliance
  - Subcontractors agree to same restrictions
  - Destroy PHI when no longer needed
- Hoop 3: Firewalls
  - Describe class of workforce with access to PHI
  - Restrict access for ONLY Plan administration – NOT employment purposes
  - Security safeguards
  - Reporting

Plan PHI Cannot Be Used for Employment Purposes

- Employer may **not** access PHI in a health plan for employment purposes

- Examples
  - Considering a leave of absence
  - Disciplinary action
  - Assessing job performance
  - Considering a promotion

Agenda

- Who is covered by HIPAA in the Group Health Plan Setting?
- How can information flow?
- HIPAA obligations for Group Health Plans
- Compliance considerations

Putting this in Perspective

Insured plans	☐ Hands-On PHI ☒ Hands-Off PHI
Self-insured plans	
Regardless of the type of plan	• Be prepared to deal with sensitive information

HIPAA Obligations: Fully Insured/ Hands- On PHI

- Full compliance with Privacy, Security, and Breach Notification Rules
  - Lessened Notice of Privacy Practices obligation
  - Must have one and provide to any participant who requests it
- HIPAA Hoops for sharing Plan PHI with Plan Sponsor (amend plan documents, certification, firewall)
- Business Associate
  - Allocate responsibilities between Plan/Plan Sponsor workforce and third party service providers (e.g., notice of privacy practices, individual rights, administrative responsibilities)

HIPAA Obligations: Fully Insured/ "Hands- Off" PHI

- Only limited HIPAA compliance required
- Still need
  - Prohibitions against retaliatory acts
  - No requirements of waiver of rights
  - Policies
  - Security Rule requirements
  - Breach/incident response
- Consider
  - Hands- off policy
- Insurer must comply with HIPAA

HIPAA Obligations: Self- Insured

- Cannot be "hands-off"
  - Even if a Business Associate is handling all PHI
- Full compliance with
- Privacy Rule
- Security Rule
- Breach Notification Rule

- Don't forget Business Associate requirements
  - Allocate responsibilities between Plan/Plan Sponsor/third party service providers (e.g., notice of privacy practices, individual rights, administrative responsibilities)

Agenda

- Who is covered by HIPAA in the Group Health Plan Setting?
- How can information flow?
- Applying HIPAA obligations to Group Health Plans
- Compliance considerations

General Health Plan Compliance Considerations

- Whether each plan/ benefit is covered by HIPAA
- How many Plans
- Whether/ how the Plan is using or disclosing PHI
  - Map where the PHI "lives" and "flows"
- Whether the Plan is insured or self- insured
  - If insured, determine whether the Plan is hands-on or hands-off PHI

Compliance Considerations

- Jump through HIPAA Hoops as needed
  - Verify firewall between Employer and Plan activities
  - Training
- Identify all Business Associates of Plan
  - Could include TPA, COBRA administrator, legal, accounting, consulting
  - Are services provided to the Employer or the Plan
  - Verify updated BAA is in place

HIPAA Enforcement & Health Plans

- Failure to have a business associate agreement ($3.5m)
- Unencrypted laptop containing Plan PHI stolen from vehicle ($250K)
- Failure to erase a hard drive of a leased photocopier prior to return ($1.2m)

Questions?

Becky Williams
beckywilliams@dwt.com
206-757-8171