HIPAA FOR HUMAN RESOURCE EXECUTIVES

Stuart Miller, Esq.

Gerry Hinkley, Esq.

Davis Wright Tremaine LLP

COVERED ENTITY ANALYSIS

- Determine if employer is a Covered Entity (health care provider, health plan or healthcare clearinghouse)
- Most employers, themselves, won’t be deemed to be a covered entity
- Self-administered plans with fewer than 50 participants are exempt

PLAN SPONSOR

- Determine if employer is a “plan sponsor” under HIPAA
- Even if employer is not a covered entity, it has substantial obligations under HIPAA if it is a plan sponsor

PLAN SPONSOR DEFINITION

- ERISA defines a plan sponsor as:
  - **The employer if plan established or maintained by single employer**
  - **An employee organization if plan established or maintained by employee organization; or**
  - **An association or board that establishes or maintains a multi-employer plan or joint employer/employee plan**

PLAN SPONSOR OBLIGATIONS

- If the employer is a plan sponsor under HIPAA, a group health plan may not disclose PHI to the plan sponsor, or permit a health insurance issuer or HMO to do so, unless the group health plan ensures that the plan documents restrict uses and disclosures of PHI by the plan sponsor as required by HIPAA

PLAN SPONSOR OBLIGATIONS

- The plan documents must be amended to establish the permitted and required uses and disclosures of PHI by the plan sponsor
- Group health plan may not disclose PHI to plan sponsor unless sponsor certifies that plan documents have been amended so that plan sponsor agrees to the following:

PLAN SPONSOR OBLIGATIONS

- **Sponsor agrees not to use/disclose PHI except as permitted/required by plan documents/law;**
- **Sponsor ensures that agents who receive PHI from sponsor agree to these same restrictions and conditions;**
- **Sponsor agrees not to use or disclose PHI for "employment-related actions and decisions or in connection with any other benefit or employee benefit plan ….**"

PLAN SPONSOR OBLIGATIONS

- Must report to the group health plan any use or disclosure of PHI “that is inconsistent with the uses or disclosures provided for of which it becomes aware.”

PLAN SPONSOR OBLIGATIONS

- Must, “if feasible, return or destroy all PHI received from the group health plan … when no longer needed for the purpose for which disclosure was made.”
- If not feasible, “limit further uses and disclosures to those purposes what make the return or destruction of the PHI infeasible.”

PLAN SPONSOR OBLIGATIONS

- Must ensure “adequate separation” between the group health plan and the sponsor, including describing in plan documents the persons who have access to the PHI, and restricting such access and use to the administration of the plan

EMPLOYER HIPAA ACTION PLAN

- Conduct a covered entity analysis and plan sponsor analysis
- Conduct an information flow assessment
- Perform a gap analysis
- Develop a remediation plan

ROLE OF HR EXECUTIVE UNDER HIPAA

- Involvement in designation of a Privacy Official
  - **Privacy Official responsible for developing and implementing policies and procedures necessary to comply with HIPAA privacy regulations**
  - **Includes responsibility for implementing training**

ROLE OF HR EXECUTIVE UNDER HIPAA

- Who should serve as Privacy Official?
  - **Regulations don't specify**
  - **Choice varies with size of organization**
  - **Is covered entity able to home grow the Privacy Official?**
  - **Immediate selection and training of a Privacy Official is critical**

ROLE OF HR EXECUTIVE UNDER HIPAA

- Create a HIPAA Compliance Team consisting of Privacy Official, HR executive, other HR managers with relevant expertise, the Information Systems manager and other relevant managers
- Each participant should become fully educated about HIPAA

ROLE OF HR EXECUTIVE UNDER HIPAA

- Compliance Team should promptly:
  - **Prepare a budget**
  - **Develop set of requirements for each department to comply with the regulations**
  - **Assign responsibilities and develop a timeline for implementing those requirements and measuring progress toward implementation**
  - **Monitor and measure each dept's progress**

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- Training required for “workforce”, including employees, volunteers, trainees and other persons under the direct control of the covered entity, whether or not compensated

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- HR exec, together with Privacy Official and Compliance team, should develop privacy and security training standards for workforce members
- The training must be job specific
- Regulations allow flexibility in establishing methods of training

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- Training must be provided to each member of covered entity's workforce before April 14, 2003; earlier implementation is wise
- New workforce members must be trained "within a reasonable period of time after the person joins the … workforce."

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- Workforce members must receive added training if job functions are impacted by a material change in HIPAA requirements or in covered entity's policies/procedures required by the regs.
- Written acknowledgements of training
- Document all training; retain for 6 years

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- "Appropriate Sanctions"
  - **Develop and implement systems for monitoring and evaluating compliance**
  - **Develop system for investigating suspected violations while maintaining confidentiality**
  - **Apply sanctions consistently**
  - **Thoroughly document investigations**
  - **No retaliation**

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- Training requirements under proposed HIPAA security regulations
  - **Security awareness training should include password maintenance, incident reporting and viruses/malicious software**
  - **All employees, agents and contractors must participate**
  - **Customized education programs based on job responsibilities**

ROLE OF HR EXECUTIVE FOR TRAINING UNDER HIPAA

- Training requirements under proposed HIPAA security regulations
  - **“Periodic security reminders” for employees, agents and contractors**
  - **User education re virus protection, log-in success/failure and password management**

IMPACT OF "MINIMUM NECESSARY" STANDARD ON HR

- Verification of request for reasonable accommodation under the ADA or for paid sick leave
- The privacy regs apply to oral communications
- Not all health information is PHI under HIPAA; must be created or received by a covered entity. Other privacy laws, ADA, constitutional requirements may apply.

AUTHORIZATION FOR PRE-EMPLOYMENT PHYSICAL EXAM

- HIPAA doesn’t prohibit conditioning employment on obtaining consent to take a drug test, medical exam or fitness-to-work exam but other laws including ADA impose limitations

DISCLOSURES RELATING TO WORKPLACE INJURIES

- Privacy regs state that “A covered entity may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers’ compensation ….”