EIGHT COMMON HIPAA MISCONCEPTIONS BY EMPLOYERS

1. **HIPAA regulates employers.**

   An employer in and of itself is not a covered entity under HIPAA. HIPAA governs the privacy and security of protected health information (PHI), which is individually identifiable health information that is created, received, or maintained by a HIPAA covered entity or business associate (e.g., TPA or broker), and that relates to an individual's past, present, or future physical or mental health or condition. HIPAA covered entities include (1) health care providers that conduct electronic transactions, (2) health care clearinghouses, and (3) group health plans.

2. **All Health information received by an employer is covered by HIPAA.**

   A common misconception is that all health information received by an employer is subject to HIPAA. For HIPAA compliance purposes, the key distinction is whether the information is created, received, or maintained in connection with an employer's group health plan. Health information received by employers in their capacity as "employer" is generally not PHI (e.g., health information related to sick leave, FMLA, or STD). Also, health information contained in employment records is not PHI.

3. **Health information received from an employee's health care provider is PHI in relation to a medical inquiry or ADA accommodation.**

   HIPAA's privacy rule does in fact prohibits health care providers from disclosing PHI to employers without an individual's explicit, written authorization. Therefore, PHI that the employer received from an employee's health care provider will generally have been properly released. Accordingly, that information no longer maintains its HIPAA protections. Also, because employers are typically requesting this type of information for employment-related reasons (i.e., with their employer "hats" on), this information will not constitute PHI once in the employer's possession.

4. **Health information received from an employee's health care provider is PHI (e.g., in relation to a medical inquiry or ADA accommodation).**

   HIPAA's privacy rule prohibits health care providers from disclosing PHI to employers without an individual's explicit, written authorization. Thus, PHI received from an employee's health care provider will generally have been released, and no longer maintains its HIPAA protections. Also, because employers are typically requesting this type of information for employment-related reasons (i.e., with their employer "hats" on), this information will not constitute PHI once in the employer's possession.

5. **I don't have to comply with HIPAA because we have fully-insured medical coverage.**

   Employers with fully-insured medical coverage are only excepted from HIPAA's privacy rule requirements (e.g., maintaining privacy policies and procedures, breach notification requirements, and distributing notices of privacy practices) if the employer maintains a "hands off" approach with respect to the administration of its fully-insured plan. A hands off approach requires that the employer have no access to the plan's PHI, though employers may receive summary health information and enrollment/disenrollment information for certain purposes. If an employer does not maintain a hands off approach, for example, by assisting employees with claims without obtaining a HIPAA release, the employer will be subject to HIPAA's privacy rules. Self-funded plans like health flexible spending accounts (health FSAs) and health reimbursement arrangements (HRAs) cannot maintain a hands-off approach and will be subject to HIPAA's privacy requirements.

6. **Employees' health information cannot be provided in relation to worker's compensation claims.**

   HIPAA allows a covered entity to disclose PHI as necessary to comply with workers' compensation laws. Under one of HIPAA's public health exceptions, health care providers that are providing services at the request of an employer relating to worksite injuries or workplace-related medical surveillance may disclose to the employer limited information that the employer needs to comply with occupational safety and health laws as well as mine safety and health laws, or similar state laws, so long as certain requirements (e.g., providing notice of the disclosure) are satisfied.

7. **HIPAA preempts state privacy laws.**

   HIPAA is a federal law that provides a uniform standard for creating, maintaining, and disclosing PHI. HIPAA specifically provides that if state law is "contrary" to HIPAA, then HIPAA preempts the state law and is controlling. However, if state law is "more stringent" than HIPAA, then in essence the federal and state laws are complementary and both will apply.

8. **My employees can sue me for a HIPAA violation.**

   Although legal actions may be available under other state and federal laws if an employee is victim to an egregious violation of the HIPAA rules, HIPAA does not give people the right to sue. Instead, individuals must file a written complaint with the Secretary of HHS via the Office for Civil Rights. It is then within the Secretary's discretion to investigate the complaint and issue penalties (if appropriate).

For more information, contact the Chelsea Deppert at CDeppert@fisherphillips.com or 404.240.4268.