Health Insurance Portability and Accountability Act (HIPAA) in the Workplace

This WorkCare Fact Sheet describes key provisions of HIPAA and its association with workers’ compensation and workplace wellness programs.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) offers protections to millions of American workers. Its basic function is to improve the continuity of health insurance coverage, prevent discrimination, and ensure privacy and security in the handling of electronically transmitted personal health information.

The federal legislation:

• Provides opportunities for employees to enroll in group health plan coverage when they lose other health care coverage, get married or add a dependent.
• Prohibits discrimination in enrollment and premiums charged to employees and their dependents based on any health factors.
• Preserves the role of states in regulating health insurance, including the authority to provide greater protections than those available under federal law.

Employees and their family members cannot be denied eligibility or benefits based on certain health factors. They also cannot be charged more than similarly situated individuals. Health factors include medical conditions, claims experience and genetic information.

HIPAA rules apply only to covered entities and their business associates. Covered entities include health care providers who transmit personal health information in an electronic form, health plans including insurers and health maintenance organizations, and health care clearinghouses such as billing and repricing companies. While an employer is not a covered entity under HIPAA, a group health plan sponsored by an employer is a covered entity. A business associate is a person or entity performing functions for or providing services to a covered entity.

Privacy and Security

HIPAA uses administrative, technical and physical security safeguards to ensure the integrity, availability and confidentiality of protected health information (PHI), also referred to as “individually identifiable health information,” that is held or transmitted by a covered entity or business associate in any form or media, whether electronic, paper or oral.
Individually identifiable health information relates to an individual’s past, present or future physical or mental health or condition; the provision of health care to the individual; and the past, present or future payment for the provision of health care to the individual. It includes common identifiers such as name, address, birth date and Social Security number.

The HIPAA privacy rule establishes protective safeguards and sets limits and conditions on uses and disclosures of PHI that may be made to employers and others without employee authorization. The rule also upholds individual rights to obtain copies of health records and request corrections. Refer to 45 CFR Part 160 and Subparts A and E of Part 164.

The HIPAA security rule establishes national security standards for protecting health information that is held or transferred in electronic form. The security rule operationalizes the protections contained in the privacy rule by addressing technical and non-technical safeguards that covered entities must put in place to secure individuals’ PHI. Refer to 45 CFR Part 160 and Subparts A and C of Part 164.

Within the U.S. Department of Health and Human Services, the Office for Civil Rights is responsible for enforcing HIPAA privacy and security rules through voluntary compliance, corrective action and civil monetary penalties of up to $50,000 for each violation and up to $1.5 million in a calendar year for repeated violations of the same provision.

The HIPAA breach notification rule requires covered entities and their business associates to notify the Labor Secretary, individuals and in some cases, the media, about use or disclosure that compromises the security or privacy of PHI.

Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The HITECH Act gives the government authority to establish programs to improve health care quality, safety and efficiency through the promotion of health information technology.

**PHI in the Workplace**

The following guidance applies:

- Documentation containing PHI must be stored in accordance with OSHA regulations (29 CFR, Access to Employee Exposure and Medical Records) and the HIPAA privacy rule.
• Medical records cannot be released to an unauthorized party without an employee’s express written consent and authorization, except under certain circumstances that must be explained.

• When an employee or designated representative requests access to a record, the employer must ensure that access is provided in a reasonable time, place and manner. If the employer cannot reasonably provide access to the record within 15 working days, the employer must advise the requestor about the reason for the delay and the earliest date when the record can be made available.

• Coordination of health care services – including health care management of an individual through medical surveillance, case management, disability review and onsite medical evaluation – is considered treatment under HIPAA regulations.

In addition, security safeguards must be in place for processes that are administrative, technical and physical in nature. Electronic transmissions of medical information (fax or email) are confidential. A cover sheet or privacy notice should be used to identify the information contained in a transmission as confidential and remind the recipient that there may be serious legal consequences if information is mishandled.

Privacy rules require covered entities to make reasonable efforts to limit the amount of PHI that a physician or other medical professional uses or discloses to the minimum amount necessary to accomplish the purpose of the use or disclosure. This requirement does not apply when a physician discloses information to another provider or when a physician requests information from another provider for treatment purposes. Accordingly, the minimum necessary standard should not interfere with a qualified medical provider’s ability to provide appropriate treatment. The minimum necessary standard also does not apply when a physician releases information: a) directly to a patient; b) pursuant to a patient’s authorization; or c) for disclosures that are required by law or are necessary to comply with privacy rules.

In emergencies, it may be necessary for medical professionals and others to obtain PHI without following standard permission procedures. This is called “breaking the glass” (as in breaking the glass to pull a fire alarm). Health systems must develop, document, implement and test break-glass procedures that would be used in the event of an emergency requiring access to electronic medical records. These systems must have a clearly stated and widely understood procedure for allowing access via alternate and/or manual methods.
HIPAA and Workers’ Compensation

The HIPAA privacy rule does not apply to workers’ compensation cases, but many employers consider compliance with at least minimal privacy and security standards to be best practice – regardless of the nature of the complaint, delivery setting or circumstances.

The privacy rule recognizes the legitimate need of parties involved in the workers’ compensation system to have access to individuals’ health information as authorized by state or other laws. Insurers, medical providers and employers are allowed to confer on cases without violating employees’ rights as long as the information exchanged involves the work-related injury or illness and care plan. Covered entities are also permitted to disclose PHI in order to obtain payment for health care provided to an injured or ill worker. When a covered entity routinely makes disclosures for workers’ compensation or payment purposes, it may develop standard protocols as part of its minimum necessary policies and procedures.

Awareness of HIPAA privacy and security provisions helps ensure employees’ PHI is adequately protected and that employers do not inappropriately obtain access to information that exceeds the scope of what is necessary to make an informed job placement decision. Employer representatives at the worksite, such as onsite medical providers and safety professionals, must be aware of the context of HIPAA and evaluate the limits and conditions that may be placed on uses and disclosures made with or without employee authorization.

HIPAA and Wellness Programs

The application of HIPAA to workplace wellness programs depends on how the programs are structured. For example, some employers may offer employees certain incentives or rewards related to group health plan benefits, such as reductions in premiums or cost-sharing amounts, in exchange for participation in a wellness program. Other employers may offer workplace wellness programs directly to employees rather than through a group health plan.

When a workplace wellness program is offered as part of a group health plan, HIPAA applies to PHI collected via health risk assessments, biometric screening and other mechanisms. HIPAA does not apply to PHI when a workplace wellness program is offered by an employer directly to employees who agree to participate. However, other federal or state laws may apply and regulate the collection and/or use of information.
According to the Office for Civil Rights, employers who administer a wellness program as part of a group health plan are:

- Prohibited from using or disclosing PHI for employment-related actions or other purposes not permitted by HIPAA (for example, marketing without express authorization).

- Required to establish firewalls or other security measures to ensure information collected as part of plan administration functions is not allowed to be accessed and used for employment functions. For example, PHI cannot be used by a supervisor for a job-related decision.

**HIPAA, ADA and Wellness**

On May 17, 2016, the Equal Employment Opportunity Commission (EEOC) issued a final rule to amend sections of the Americans with Disabilities Act (ADA) that relate to wellness programs: Employers may provide limited financial and other incentives in exchange for an employee answering disability-related questions or taking medical examinations as part of a wellness program, regardless of whether the program is part of a health plan.

The EEOC sought to provide consistency with HIPAA and Patient Protection and Affordable Care Act rules on wellness program incentives while also ensuring that incentives would not be so high as to become coercive or render participation in the program involuntary. The ADA regulates certain aspects of wellness programs that HIPAA and the Affordable Care Act do not.

HIPAA and the Affordable Care Act allow wellness programs that are part of an employer-sponsored group health plan to offer incentives for “health-contingent” wellness programs. These programs offer rewards to employees who perform activities (such as walk 10,000 steps a day) or achieve certain health outcomes (such as lowering their blood pressure), or impose penalties if they do not perform an activity or fail to achieve a particular outcome.

The regulations implementing HIPAA do not impose any incentive limits on “participatory” programs (such as programs that only ask employees to complete a health risk assessment or attend a smoking cessation class). As long as these programs are available to all similarly situated individuals, and incentives are made available regardless of a health factor (e.g., participating employees receive the same incentive regardless of their health status or disability), participatory wellness programs do not violate HIPAA and the Affordable Care Act.
Unlike HIPAA and the Affordable Care Act, the ADA places limits on disability-related inquiries and medical examinations related to wellness programs, regardless of how the information obtained is ultimately used. The EEOC’s final rule specifies that a limit on incentives applies to any wellness program that requires employees to answer disability-related questions or undergo medical examinations (whether it is participatory or health contingent). Like HIPAA and the Affordable Care Act, this rule also makes clear that the term “incentives” includes both financial and in-kind rewards.

The ADA makes no distinction between wellness programs that are part of, or outside of, a group health plan. All wellness programs that obtain medical information from employees must be voluntary.

Additionally, in order to ensure that an employee’s participation is voluntary, an employer must provide a notice that clearly explains what medical information will be obtained, how it will be used, who will receive it and restrictions on disclosure. Finally, an employer must comply with incentive limits as described by the EEOC in its final rule.