Published on *The National Law Review* https://natlawreview.com

What All Employers Need to Know About Protecting Employee Health Information

Article By:

Kelly S. Riggs

Employers obtain employee health information in a number of ways—most commonly, in relation to a work-related injury or when an employee requests medical leave or a disability accommodation. Most employers understand that such information is “confidential,” but may not fully understand what that means or what they should do to protect it.

HIPAA Generally Does Not Apply to Employers

It is a common misconception that the Health Insurance Portability and Accountability Act (HIPAA) applies to employee health information. In fact, HIPAA generally does not apply to employee health information maintained by an employer.

HIPAA applies only to “covered entities,” which are defined as: (1) health plans; (2) healthcare clearinghouses; and (3) healthcare providers that electronically transmit certain health information (and certain “business associates” of covered entities). If an employer does not fall into one of those categories, HIPAA does not apply to it at all. Indeed, even if an employer is a “covered entity,” HIPAA still does not apply to health information contained “in employment records held by a covered entity in its role as an employer.” So even for those employers, although HIPAA may apply to health information they acquire in their capacities as covered entities, it does not apply to health information they acquire in their roles as employers.

Employers should not forget, however, that HIPAA does apply to an *employer’s* request for health information from a covered entity. A covered entity may not disclose protected health information to an employer without the employee’s authorization or as otherwise allowed by law. This is true even where the employee is also a patient or member of the covered entity; information maintained in that capacity may not be shared with human resources or an employee’s managers, except as expressly authorized by the employee or applicable law.

Protecting Employee Health Information

Even when HIPAA does not apply, employers still have other legal obligations to protect the confidentiality of employee health information in their possession.

For example, the Americans with Disabilities Act (ADA) requires employers that obtain disability-related medical information about an employee to maintain it in a confidential medical file that is kept *separate* from the employee's personnel file. Such information may be disclosed *only* in limited situations and to individuals specifically outlined in the regulations:

- supervisors and managers who need to know about necessary work restrictions or accommodations;
- first aid and safety personnel, if a disability might require emergency treatment; and
- government officials investigating compliance with the ADA.

Similarly, the Genetic Information Nondiscrimination Act (GINA) requires employers that acquire an employee's genetic information (although they generally should not request it) to treat it as a confidential medical record in a separate medical file. It can be maintained in the same confidential medical file as disability-related information. However, different rules regarding when and to whom genetic information may be disclosed apply—which do not include supervisors, managers, or first aid or safety personnel, but do include others not on the list for disclosure of disability-related information.

Oregon medical records privacy law is generally consistent with HIPAA; it expands the definition of "covered entities" to include "health insurers," but does not provide broader protections to employee health information. The Oregon Consumer Identity Theft Protection Act, however, includes additional protections for personal identifying information and medical information in an employer's possession, including requiring businesses in Oregon to implement and maintain certain safeguards to protect the security and confidentiality of protected personal information, and to report certain data breaches.

Accordingly, in order to ensure compliance with these privacy requirements, employers in Oregon should maintain *all* employee health information in separate, confidential medical files with restricted access, and should implement clear policies, safeguards, and training to help employees understand and comply with the requirements.

Requests for Employee Health Information

Notwithstanding the above, employers may disclose employee health information with an employee's express authorization (which should be in writing). Employers also may, if certain legal requirements are met, disclose such information in response to subpoenas, court orders, or other legally authorized requests, but should examine such requests closely and limit disclosure of health information only to the extent specifically requested and authorized by the employee or applicable law.

National Law Review, Volume VIII, Number 79