When Do the HIPAA Privacy Rules Apply to Individually Identifiable Health Information Received by Our HR Department?

EBIA Weekly (September 4, 2025)

QUESTION: Our HR department often receives individually identifiable health information from employees, health care providers, or health plans in connection with an employee's request for leave (e.g., sick leave or FMLA leave) or a reasonable accommodation under the Americans with Disabilities Act (ADA). The department also assists employees with claims under our health plan and may receive individually identifiable health information for this purpose. Is any of this information subject to the HIPAA privacy rules?

ANSWER: The answer depends upon where the information came from, who has it now, and why they have it. The privacy rules only apply to "covered entities"—that is, health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with any of the transactions covered by the HIPAA administrative simplification regulations. Employers are not covered entities under those regulations. However, sometimes an employer performs administration functions on behalf of its health plan; information that an employer uses or discloses in performing plan administration functions is affected by the privacy rules.

Information that an employee turns over to an employer for employment-related functions, such as responding to leave or accommodation requests, is not subject to the privacy rules. (Other laws, such as the ADA, may apply—we address only HIPAA's requirements in this answer.) However, the same information is subject to the privacy rules in the hands of covered entities. Accordingly, if the employer wants to obtain the information directly from a covered entity (such as a provider or plan), rather than from the employee, the provider or plan must comply with the privacy rules before making disclosure. The provider or plan generally will not disclose information to the employer without an authorization satisfying HIPAA's requirements. (The privacy rules permit a covered entity to disclose information as authorized by and to the extent necessary to comply with workers' compensation laws, but the HIPAA provision is permissive only and some providers and plans will still want a HIPAA-compliant authorization.) Once an employer receives information from a provider or plan for employment-related functions, however, the employer has no HIPAA privacy obligations as to that information.

For information disclosed to an employer for use in assisting an employee with a health plan claim, the source of the information is important, as is the employer's characterization of the assistance as an employment-related function or a plan administration function. An employer may receive information directly from an employee to assist with a claim without any HIPAA obligations attached to that information. And if the employer seeks information from a covered entity provider, the provider will probably require a HIPAA-compliant authorization from the employee or other patients. But what if the employer seeks information from the plan? If the employer renders assistance to the employee as an employment-related function (rather than as a plan administration function), the same rules discussed above for such functions would apply (i.e., the plan would need an authorization from the individual).

However, an employer that has amended its plan to permit the employer to receive information from the plan for plan administration functions (specifying in the amendment that assisting employees with claims is a plan administration function) might also take the position that it can receive information about a claim without an authorization. For a self-insured plan, because HHS has not issued formal guidance on whether the plan administration functions that may be performed by a plan sponsor include assisting employees with claims (and because informal comments by HHS representatives have differed), plans may need authorization. And for a fully insured plan, an employer that is taking the “hands-off PHI” approach will always need an authorization to obtain PHI from the plan. An employer that does not carefully follow this rule may inadvertently make itself “hands-on” and subject to more onerous privacy and security requirements. For more information, see EBIA’s HIPAA Portability, Privacy & Security manual at Sections XXIII.C (“Sharing PHI and Electronic PHI With Plan Sponsors”), XXIII.D (“Many Common Employer Functions Require Authorization”), and XXIII.F (“Applying the HIPAA Privacy and Security Rules to Group Health Plans and Their Sponsors”).

Contributing Editors: EBIA Staff.