Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Using an Employee's Protected Health Information for Employment Decisions

Publication — 12/18/2017

Employers must beware HIPAA when using an employee's protected health information to make employment-related decisions. HIPAA problems generally arise in two situations:

- **The employer is a healthcare provider who renders treatment to the employee.** For example, a hospital employee may receive treatment or lab work at the hospital; a physician in a group practice may see an employee as a patient; or a nurse employed by the employer may provide drug tests, employment-related physicals, or other healthcare to employees. In such cases, the employer is both an employer and a treating provider. If the provider engages in certain electronic transactions, HIPAA will apply to the health information it obtains or maintains in its capacity as a healthcare provider.
- **The employer receives employee health information through its employee benefit plan.** HIPAA applies to employee benefit plans that have 50 or more employees or that are administered by a third party. In such cases, the employee benefit plan generally may not disclose protected health information concerning plan participants to the employer who sponsors the plan, and the employer-sponsor may not use such information for employment-related decisions, unless HIPAA rules are satisfied.

Whether HIPAA applies to the health information depends on the capacity in which the healthcare provider/employer obtained or received the health information: did it obtain or generate the information in its capacity as a HIPAA covered entity (*i.e.*, a healthcare provider or employee group health plan), or solely in its capacity as an employer?

In What Capacity Was the Information Obtained? The HIPAA Privacy Rule only applies to "protected health information";

> *Protected health information* excludes individually identifiable health information in …
> [e]mployment records held by a covered entity in its role as employer.

(45 CFR § 164.501, definition of "protected health information"). Thus, the HIPAA Privacy Rule does not apply to employment records held by a hospital or other healthcare provider solely in its capacity as an employer. "For example, information in hospital personnel files about a nurse's sick leave is not protected health information under this rule." (65 FR 82612). On the other hand, "[i]ndividually identifiable health information maintained or transmitted by a covered entity in its health care capacity [will] continue to be treated as protected health information" under HIPAA. (67 FR

53191). HHS explained the distinction as follows:

> drug screening test results will be protected health information when the provider administers the test to the employee, but will not be protected health information when, pursuant to the employee's authorization, the test results are provided to the provider acting as employer and placed in the employee's employment record. Similarly, the results of a fitness for duty exam will be protected health information when the provider administers the test to one of its employees, but will not be protected health information when the results of the fitness for duty exam are turned over to the provider as employer pursuant to the employee's authorization.

(67 FR 53192). HHS commentary that accompanied the final HIPAA Privacy Rule contains a fairly extensive discussion of the issue. (*See* 67 FR 53192). Among other things, HHS warned:

> The Department is sensitive to the concerns of commenters that a covered entity not abuse its access to an employee's individually identifiable health information which it has created or maintains in its health care, not its employer, capacity….
>
> To address these concerns, the Department clarifies that a covered entity must remain cognizant of its dual roles as an employer and as a health care provider [or] health plan…. Individually identifiable health information created, received, or maintained by a covered entity in its health care capacity is protected health information. It does not matter if the individual is a member of the covered entity's workforce or not. Thus, the medical record of a hospital employee who is receiving treatment at the hospital is protected health information and is covered by the [HIPAA Privacy] Rule, just as the medical record of any other patient of that hospital is protected health information and covered by the Rule. The hospital may use that information only as permitted by the Privacy Rule, and in most cases will need the employee's authorization to access or use the medical information for employment purposes. When the individual gives his or her medical information to the covered entity as the employer, such as when submitting a doctor's statement to document sick leave, or when the covered entity as employer obtains the employee's written authorization for disclosure of protected health information, such as an authorization to disclose the results of a fitness for duty examination, that medical information becomes part of the employment record, and, as such, is no longer protected health information. The covered entity as employer, however, may be subject to other laws and regulations applicable to the use or disclosure of information in an employee's employment record. (67 FR 53192).

More recently, in its commentary to the Omnibus Rule, HHS explained:

> An entity that maintains an on-site clinic to provide health care to one or more employees may be a HIPAA covered provider to the

> extent the clinic performs one or more covered transactions electronically, such as billing a health plan for the services provided. If covered, the entity need not become a hybrid entity so as to avoid applying the Privacy Rule to health information the entity holds in its role as employer, such as sick leave requests of its employees. Such information is already excluded from the definition of "protected health information" as employment records and thus, the Privacy Rule does not apply to this information. However, the identifiable health information the entity holds as a covered health care provider (e.g., the information the clinic holds about employees who have received treatment) is protected health information and generally may not be shared with the employer for employment purposes without the individual's authorization.

(78 FR 5589).

In short, healthcare providers or plans must still protect health information they obtain in their role as a healthcare provider or plan. The OCR website reports the following sanctions related to an entity that improperly used employee information:

> A hospital employee's supervisor accessed, examined, and disclosed an employee's medical record. OCR's investigation confirmed that the use and disclosure of protected health information by the supervisor was not authorized by the employee and was not otherwise permitted by the Privacy Rule. An employee's medical record is protected by the Privacy Rule, even though employment records held by a covered entity in its role as employer are not. Among other corrective actions to resolve the specific issues in the case, a letter of reprimand was placed in the supervisor's personnel file and the supervisor received additional training about the Privacy Rule. Further, the covered entity counseled the supervisor about appropriate use of the medical information of a subordinate.

(*See* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html).

So What's an Employer to Do? If the employer obtains health information in its capacity as a healthcare provider or plan, then it must protect the information consistent with the HIPAA Privacy Rule. To access, use or disclose protected health information for employment-related decisions, the provider or plan generally needs one of the following:

1. The Employee/Patient's HIPAA-Compliant Authorization. An employer may request the employee's written authorization to access, use or disclose the information. HIPAA authorizations must contain certain elements and statements described in 45 CFR § 164.508, including a description of the intended use and disclosure. For more information about the requirements for valid authorizations, *see* https://www.hollandhart.com/valid-hipaa-authorizations-a-checklist. In most cases, a healthcare provider may not condition treatment on the provision of the authorization; however, if the purpose of the treatment is to obtain

information for disclosure to the employer (*e.g.*, employee drug tests, fitness for duty exams, etc.), the provider may condition the test or treatment on the authorization, *i.e.*, the provider may refuse to conduct the test or exam unless the authorization is given. (45 CFR § 164.508(b)(4)(iii); 65 FR 82516 and 82658). For more information about disclosing test results to employers, *see* https://www.hollandhart.com/hipaa-disclosing-exam-results-to-employers. Employers should consult their attorney before taking adverse employment action against an employee based on the employee's refusal to authorize the disclosure of protected health information.

2. The Employee/Patient's Written Request to Disclose the Information. The HIPAA Omnibus Rule created a new way for patients or plan participants to authorize disclosure: a covered entity may (in fact, must) disclose information to third party if the patient requests the disclosure in writing. (45 CFR § 164.524(c)(3)(ii)). Such a request need not contain the elements of a formal HIPAA authorization, and may be combined with another document. For more information about such requests to release information, *see* https://www.hollandhart.com/hipaa-releases-of-information-per-request-or-authorization. Although we do not have any authoritative commentary on the issue, it may be possible for an employer to incorporate such a release into its employment documentation, thereby allowing disclosures. Employers should consult with their attorney before attempting to do so.

3. A HIPAA Exception that Allows Disclosure without Authorization. HIPAA contains several exceptions that may allow disclosure to or use of protected health information by an employer without the employee/patient's authorization in limited situations. For example:

- A covered entity may use or disclose protected health information for certain specified healthcare operations, including quality assessment and improve activities, reviewing the competence of or qualifications of health care professionals, evaluating practitioner performance, credentialing and peer review, management activities, resolution of internal grievances, etc. (45 CFR §§ 164.506 and 164.501, definition of "health care operations").
- A covered entity may use or disclose protected health information to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. (45 CFR § 164.512(j)).
- A covered entity may use or disclose protected health information to the extent required by law. (45 CFR § 164.512(a)(1)).
- A covered entity may use or disclose protected health information for certain public health activities, including disclosures to employers for medical surveillance or reporting work-related injuries as required by OSHA, MSHA, or similar state laws. (45 CFR § 164.512(b)(v)).
- A covered entity may use or disclose protected health information as authorized by and to the extent necessary to comply with workers compensation laws. (45 CFR § 164.512(l)).

Each of these exceptions carry specific conditions; covered entities should

carefully review the regulations and circumstances to confirm whether they apply in a given situation.

Remember Other Laws. The foregoing only addresses relevant HIPAA concerns. The use or disclosure of health information for employment-related decisions may implicate other laws, including but not limited to the Americans with Disabilities Act ("ADA"), Family and Medical Leave Act ("FMLA"), Genetic Information Nondiscrimination Act ("GINA"), and other state and federal laws. For example, once the healthcare employer receives employee health information in its capacity as an employer, it must retain that information in a confidential, secure employee medical file, apart from other personnel records, to comply with the ADA and FMLA. Employers should carefully consider and consult with their attorney when navigating these issues.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913