Medical records: Do's and don'ts

Medical records are among the most sensitive documents employers maintain in personnel files. They must be afforded the utmost protection, so no transgressions arise regarding the Americans with Disabilities Act (ADA), the Health Insurance Portability and Accountability Act (HIPAA), the Family and Medical Leave Act (FMLA), and other similar medically-sensitive federal and state regulations.

FAQs

1. How long must employers preserve and maintain each employee's medical records?

Not everyone realizes this, but OSHA regulations require that general medical records be maintained for an employee's length of employment plus 30 years.

Specifically, OSHA regs define the term "medical records" as "...a record concerning the health status of an employee which is made or maintained by a physician, nurse, or other health care personnel or technician," including medical and employment questionnaires and histories (including job description and occupational exposures); the results of medical examinations (pre-employment, pre-assignment, periodic, or episodic) and laboratory tests (including chest and other X-ray examinations taken for the purpose of establishing a baseline or detecting occupational illnesses and all biological monitoring not defined as an "employee exposure record"); medical opinions, diagnoses, progress notes, and recommendations; first-aid records; descriptions of treatments and prescriptions; and employee medical complaints.

There are certain exceptions to this requirement. Health insurance claims records maintained separately from the employer's medical records, first-aid records for one-time treatment, and the medical records of employees who have been employed for less than one year provided the records are offered to the employee upon termination need not be maintained for 30 years after termination.

2. Do HIPAA's privacy regs apply to all medical records?

Some employers mistakenly believe that HIPAA's privacy regs apply to any and all medical information that makes its way into the workplace. That's simply not true. HIPAA applies to information received through the group health plan; it does not apply where an employer collects health information for employment purposes, including:

- pre-employment physicals, drug tests, and fitness-for-duty exams;
- medical information used to carry out obligations under the FMLA, the ADA, and similar laws;
- employment files or records, such as sick leave requests and workplace medical or safety records.

Employers that most need to concern themselves with HIPAA's privacy rules are those that offer a self-funded health plan. That's because a fully insured group health plan only has access to limited medical information about participants and beneficiaries and can rely on insurance issuers to comply with HIPAA's privacy regs. Employers with self-funded plans, on the other hand, have access to a variety of non-employment related medical information, including types of health claims filed, medical diagnoses, treatment codes, medical costs, physicians visited, lab work, etc. It's this information that HIPAA privacy regs work to protect.