Audit: Personnel Files: Employment (Personnel) Records Audit Checklist (Including Form to Audit Individual Employee Personnel Files)

Aug 19, 2014

Note to Employers:

Each employer may have its own unique employment record maintenance practices. Personnel records can be maintained in paper form, scanned, or completed and maintained electronically. No matter what format is used, the maintenance, security and retention requirements are the same.

Most employers have at least three or four different employment record filing systems. The main personnel file that contains employee performance information; the medical/confidential file that contains protected, nonjob-related or confidential information; and the payroll records are usually maintained separately by the payroll administrator(s). Form I-9 files should always be maintained separately. Additional files may be necessary to maintain hiring records, investigations, drug test results and other documents. Employers must give special consideration to where and how they maintain these files, limiting access to only those with a need to know and protecting applicants and employees from discrimination, identity theft, breach of privacy, and Health Insurance Portability and Accountability Act (HIPAA) violations.

Questionnaire

Electronic files (skip this section unless your personnel records are maintained electronically)

- Do you have a good document management system?
- Have you established clear parameters around which employees have access to which files?
- Have you implemented proven security and password protections to ensure access is provided only to those with a need to know?
- Do you have a backup system in place to ensure data are not lost?
- Do you have a secondary backup system in the event both the software and its backup are destroyed?
- Have you provided training to end users on how to properly use and protect information in the document management system?

Personnel files

- Are the personnel files maintained in a locked and secure cabinet, or have proper electronic security features been developed?
    - Have all documents that contain protected information been removed from the personnel file? (Note: Documents that include medical information, Social Security numbers or other protected class information such as age, race, gender, national origin, disability, marital status and religious beliefs should not be kept in the personnel files. Supervisors should have access or be able to request access to personnel files to assist them in making employment decisions.)
- Are personnel files organized in a logical manner so that information is easy to find? Note: How to organize the files is up to the company. The two most common practices are to maintain files in chronological order or to have files with different sections for different types of documents (e.g., performance, training, employment).
- Is there a policy or consistent practice regarding employee access to personnel files?
- Is this policy/practice compliant with any relevant state laws?

Medical and confidential files

- Are medical/confidential files maintained in a locked and secured cabinet?
- Do you restrict access to only those with a need to know? (Note: Supervisors usually do not have a need to know unless there is an accommodation requirement, in which case only the information they require to assess accommodation needs should be released to them. Only a few people should have access to these records to keep them maintained appropriately.)

Terminated Employee Files

- Are terminated files locked and secured with limited access?
- Does your company have a regular (weekly, monthly or quarterly) disposal plan for documents that have exceeded record retention guidelines?
- Are employment records that have met or exceeded record retention requirements disposed of via shredding, burning or fully destroying these records prior to disposal? (Note: Relevant state and federal record retention guidelines.)

- Are files related to a current or potential lawsuits maintained by legal counsel or in some other way marked to be exempted from any disposal process until after the suit is closed? (Note: Under discovery and e-discovery laws, it is illegal to destroy documents related to a current or potential lawsuit.)
- Does your company have a written record retention and destruction policy and procedure?

Checklist

Separate files

- Hiring records
    - These records should include any job requisitions and job postings, interview notes, reference checks, and other hiring records such as applications and resumes if they contain protected information.
    - These records can be accessed by the hiring manager as well as by HR, so they should not include any information irrelevant to the job or to the hiring decision, such as protected class information, arrest records and Social Security numbers (SSNs).
- Drug tests and background checks/credit checks
    - These records should be kept separately from any records a supervisor has access to.
    - The hiring manager should be told whether an applicant or employee passes these tests, but he or she should not be provided a copy of the record. Reports often include irrelevant or protected information.
    - Once an employee is hired, these reports should be placed in the employee's medical/confidential file or kept in a separate file altogether.
- I-9 files
    - Form I-9 and any relevant documentation should never be left in an employee's personnel file.
    - Access is highly restricted. Keep in a locked cabinet or secured electronic database. Hiring managers should not have access.
- EEO records
    - Any equal employment opportunity (EEO) data collection should be maintained separately from personnel files and used only for reporting purposes such as for an affirmative action program (AAP), the Form EEO-1 and internal diversity tracking.
    - Do not allow EEO records to be attached or kept with other hiring or employment records.
    - Access is highly restricted. Keep in a locked cabinet or secured electronic database. Hiring managers should not have access.
- Payroll files
    - Contents will include W-4s, state withholding forms, garnishments, pay information, wage deduction acknowledgements and time-keeping records.
    - Investigation files
        - For harassment and other grievance complaints, maintain the files separately from any personnel file because they usually contain information affecting more than one person and include witness accounts.
        - Only relevant disciplinary action or individualized memos/letters should go in an employee's personnel file.
        - Access is highly restricted. Keep in a locked cabinet. Hiring managers should not have access.
- Manager desk files
    - There is debate over whether manager desk files should be permitted. It may depend on how closely the personnel files are maintained. Often, when personnel records are kept at headquarters, managers at other locations may find it helpful to maintain copies of records in the personnel file.
    - If manager desk files are maintained, make sure they are locked in a cabinet or secured if electronic.
    - Ensure all original documents are placed in the personnel file and managers keep only copies.
    - Managers should be trained on proper documentation procedures to ensure that notes in their files are not discriminatory or illegal.
    - Be aware that manager desk files are discoverable in the event of a lawsuit.

Note: Some employers also maintain their worker's compensation and Family and Medical Leave Act (FMLA) files separately from the medical files. It is up to the company whether to keep these records in the medical file or separately. It often depends on who is responsible for administration of these benefits. If it is the same person who maintains the medical/confidential files, keeping these files together may make sense. If it is a separate administrator, these files should be maintained separately, at least until they are closed.