

Introduction

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, non-job-related or confidential information, and the payroll records are usually maintained separately by the payroll administrator(s). I-9 files should always be maintained separately. Additional files may be necessary to maintain your hiring records, investigations, drug test results, etc. Employers must give special consideration to where and how they maintain these files, limiting access to those with a need-to-know only and protecting applicants and employees from discrimination, identity theft, breach of privacy, and HIPAA violations.

Checklist

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?

- Documents that include medical information, SSNs or other protected class information such as age, race, gender, national origin, disability, marital status, religious beliefs etc. should NOT be 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?

- 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, etc.)

Is there a policy or consistent practice regarding employee access to personnel files?

- Is this policy/practice compliant with any **relevant state laws**?

See below for a template form to use when auditing each individual personnel file.

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"?

- Supervisors usually do not have a “need-to-know” unless there is an accommodation requirement, in which case only the information they need to assess accommodation needs should be released to them.
- Only a few people should have access to these records to keep them maintained appropriately.

Separate files

Hiring records

- These records should include any job requisitions and job postings, interview notes, reference checks, other hiring records such as applications and resumes (however, hired employee’s application and resume should be moved to personnel or employee’s medical/confidential file).
- These records can be accessed by the hiring manager as well as HR, so they should NOT include ANY records that have information irrelevant to the job or the hiring decision. Therefore, no protected class information, arrest records, SSNs, etc., should be part of these records.

Drug tests and background checks/credit checks

- These records should be kept separate from any records a supervisor has access to.
- The hiring manager should be told whether an applicant or employee passes these tests, but not provided a copy of the record. Reports often include some irrelevant and/or protected information.
- Once an employee is hired, you need to decide whether to place these reports in his or her medical/confidential file or keep them 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 locked cabinet or secured electronic database. Hiring managers should not have access.

EEO records

- Any EEO data collection should be maintained separate from personnel files and used only for reporting purposes such as AAP, 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 locked cabinet or secured electronic database. Hiring managers should not have access.

Payroll files

- Contents will include W-4s, state withhold forms, garnishments, pay information, wage deduction acknowledgements and time keeping records.

Investigation files

- For harassment and other grievance complaints, maintain the files separate from any

- personnel file since it usually affects more than one person and has witness accounts.
- Only relevant disciplinary action or individualized memos/letters should go in an employee's personnel file.
- Access is highly restricted. Keep in locked cabinet. Hiring managers should not have access.

Some employers also maintain their Worker's Compensation and/or FMLA files separate 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, it may make sense to keep these files together. If it is a separate administrator, these files should be maintained separately, at least until they are closed.

Manager desk files

- There is debate over whether manager desk files should be permitted. It really may depend on how close the personnel files are maintained. Often, when personnel records are kept at HQ, then 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.

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 lawsuit maintained by legal counsel or in some other way marked to be exempted from any disposal process until after the suit is closed?

- 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?