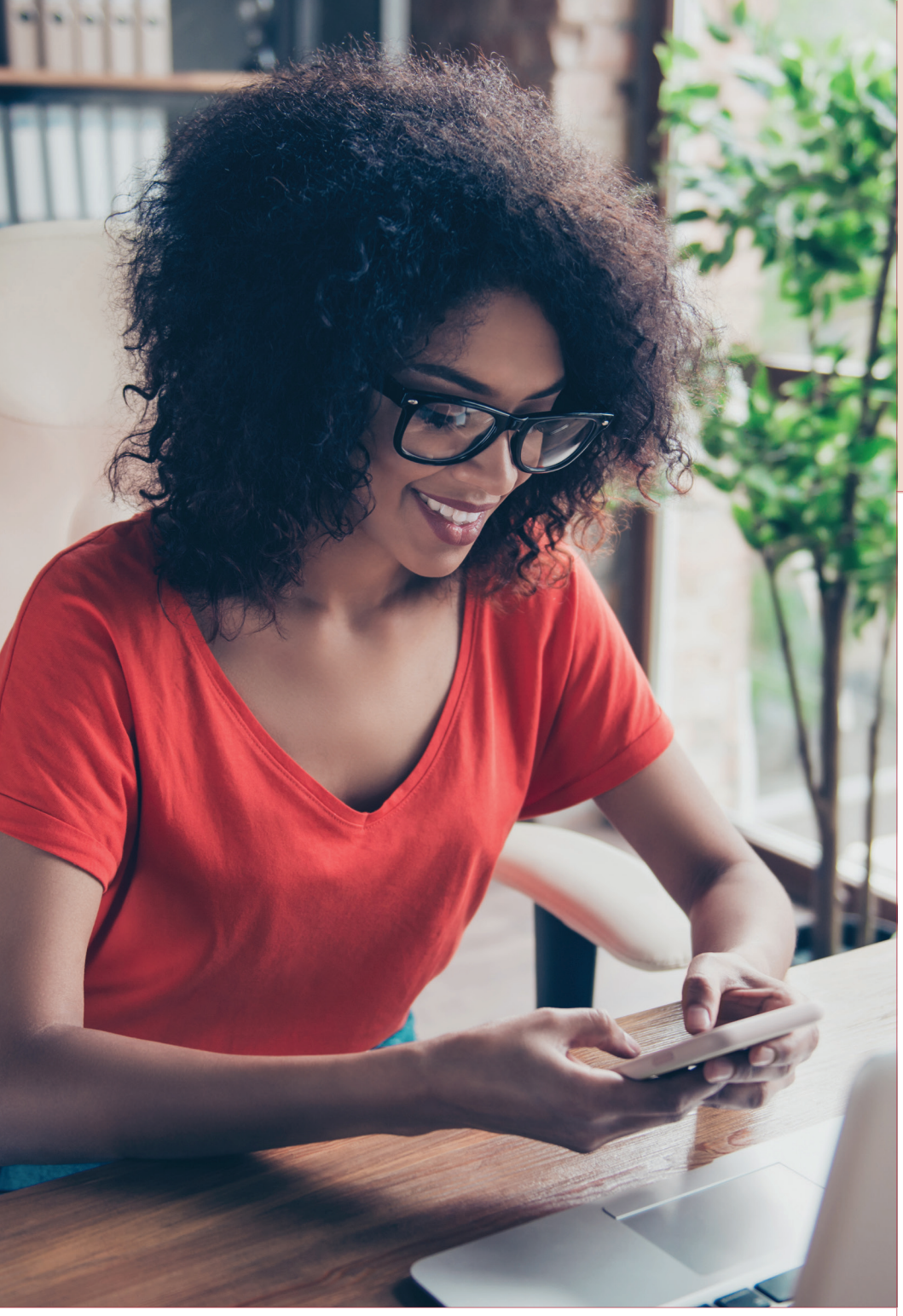

Record Storage Best Practices

Always Designing for People®

Always Designing for People®

Organizing Your Files

Knowing where to store employee records is essential to proper recordkeeping. Certain information, such as medical information, must be kept separate and secure from other employee records. As a best practice, employers should maintain a personnel file for each employee. Personnel files should contain data related to employment. Personnel files should not contain medical information and certain other types of information. Medical information should be stored in separate and confidential medical files.

What belongs in the personnel file?

The test of what belongs in a personnel file is that it be job-related. Examples of job-related information that belong in a personnel file include:

- Resume
- Employment application
- Offer letter
- Job description
- List of company-issued property
- Handbook acknowledgment
- Licenses/certifications
- Attendance records
- Direct deposit authorization
- Salary history
- Records of promotions, demotions, transfers
- Performance goals
- Performance review forms
- Training records
- Discipline notices
- Exit interview form
- Resignation letter

Although an employee's personnel file should contain all significant job-related data (including documents and other electronic information), exercise caution on the information that you place in the file. In many states, employees have the right to review their personnel files. Plus, lawyers will always ask for the production of the personnel file if you ever find yourself in a lawsuit with an employee.

What does not belong in the personnel file?

What does not belong in a personnel file is often determined by who has access to the data. For example, due to the confidential nature of medical information, it must be maintained in a separate confidential medical file. Access to medical records must be severely restricted.

Below are some examples of records that would be appropriate to store in a confidential medical file:

- Doctor's notes and medical certification forms
- Requests for medical leave of absence
- Medical leave information
- OSHA medical exam or exposure records
- Short or long-term disability records
- Workers' compensation records
- Drug and alcohol testing records
- Benefit enrollment forms and claim histories
- Requests for reasonable accommodation

Non-medical confidential information must also be kept separate from the personnel file. This includes information that has the potential to reveal an employee's membership in a protected class (e.g. national origin, disability, religion, or other protected characteristic).

Always Designing for People®

Below are some examples of records that would be appropriate to store in other confidential files:

- EEO records and self-identification forms
- Affirmative action data
- Background check reports (employees)
- Supporting I-9 documentation (e.g. social security card, driver's license, passport)
- Investigation records, including witness statements, evidence, and investigation results
- Litigation documents

In addition to confidential medical files and other confidential files, it is a best practice to separately store certain records so that they can be promptly produced following an official request from a government agency. For example, it is a best practice to store all I-9 forms together in one file because you will have to produce them within 3 days upon official request. Similarly, you may want to store safety training records apart from other personnel records so that they can be produced promptly upon request from the Occupational Safety and Health Administration.

General Company Records

In some cases, you may have records that are not directly related to a particular employee. In addition, non-discrimination laws require you to maintain certain information on nonhires. In these circumstances, it may be appropriate to keep a separate folder to store these types of records.

- Applicant Records
- Applicant records (non-hires) should include:
- Resumes
- Application forms
- Interview notes
- Skill inventories

Confidential Company Records

For confidential applicant or other confidential company information, keep a separate sub-folder. Store documents related to:

- Background check reports (non-hires)
- Pre-employment tests (non-hires)
- Adverse action notices
- Customer/client lists
- Company financials

Record Retention and Destruction

A number of laws, both at the federal and state level, dictate the types of records that need to be retained and for how long. RUN Powered by ADP® (RUN) HR package clients can find more information on federal and state record retention requirements in the resources provided in the HR section of RUN or by contacting the HR HelpDesk.

Develop a Policy

It's extremely important that you maintain records for their full retention period. And, at the conclusion of the retention period, you must properly discard them. Consider developing a record retention and destruction policy that defines what documents must be kept, how long they must be kept, and how they are to be properly discarded. Attach a record retention schedule that is consistent with federal, state, and local law. In the event of legal action against the company, suspend the disposal of any relevant documents or other information.

Document Destruction

Following the conclusion of the retention period, records must be disposed of properly, so they cannot be read or reconstructed. Note: The Fair and Accurate Credit Transactions Act (FACTA) has disposal rules for background check reports. For paper files, shredding is a best practice. For electronic records, you must properly destroy or erase the files so that the information cannot be read or reconstructed.

Always Designing for People®

Electronic Retention

Generally, most laws do not require records to be kept in any particular format (e.g. paper vs. electronic). However, you must be able to retrieve records quickly and produce legible hard copies when necessary. In general, the same record retention and security rules that apply to paper files apply to electronic records. Below are considerations for storing employee records in electronic format:

- **Identify records that can be transferred to electronic format.** Determine the types of records that can be accurately and completely transferred to an electronic system. You must retain hard copies of the records that can't be stored electronically.
- **Separate confidential information.** Separate medical information and other confidential information from the personnel file in the same way you would if you maintained paper files.
- **Ensure authorized access.** Develop protocols to ensure that only authorized user's access electronic files. Change passwords when an authorized user leaves the company or if someone with unauthorized access gains entry into the system. If an unauthorized user gains access to the system (e.g. password was given to someone who should not have access to the system), promptly investigate the situation and document the steps you take to respond.

Clients of the RUN Complete Payroll and HR Plus bundles can use our Doc Vault tool to store these documents securely and safely online for easy access when needed.

Access to Employee Files

Employee files must be kept secure at all times and only accessible to those with a "need to know". The business owner or someone with HR management responsibilities should have ultimate authority over who has access to, and what goes in and out of, employee files.

Supervisor Access

Supervisors should only have access to relevant performance-related records under the direction of someone with recordkeeping authority. Under no circumstances may supervisors have access to employee medical information or other confidential data.

Employee Access

Access to employee personnel files is governed by state law. Many states give employees the right to examine their records, typically within a "reasonable period of time" following a written request. RUN HR package clients can find more information on state laws governing access to employee records in the resources provided in the HR section of RUN or by contacting the HR HelpDesk.

Following an employee's request to view their personnel file, print electronic records stored in an electronic personnel file. Provide the employee with access to their personnel file under the direction of someone with recordkeeping authority.