Making the leap to electronic records: 4 legal considerations

Given the low cost and the easy accessibility of electronic records storage, many employers are making the digital leap to “paperless” HR. These days, most records are created and maintained electronically, and some never even make their way to paper.

Most paper records can be scanned into electronic form, reducing storage costs and allowing users to preserve and access vast databases of records with the click of a mouse.

But despite the many benefits of going paperless, a host of legal problems could derail even the best-intentioned digital records plan.

Carefully consider these legal issues when transitioning to an electronic personnel records system:

1. Employees *can* review their records, paper or electronic

The obligation to produce an employee’s personnel record extends to all covered records, including electronic data. Comply by allowing the employee to review the record during business hours in the presence of a company official or producing a copy of the personnel record without charge upon an employee’s request.

2. Records must be accessible

Store electronic personnel records in an accessible, organized manner so you can timely produce a personnel record upon a lawful request. Unless your electronic storage system is well-organized and accessible, you might not have enough time to produce a personnel record.

Quick access to all necessary files, searchability and the ability to cull records are essential elements of an effective electronic storage system.

3. Keep e-records confidential

Personnel records often include information that employers must keep confidential, such as employee medical records, drug testing records, Social Security numbers and credit reports. Employee files may also include sensitive information that should be maintained confidentially, such as pay records, leave requests and performance or termination data.

When dealing with physical documents, employers can safeguard files by keeping them in locked cabinets in a locked office and providing keys only to authorized individuals.

Employers must take similar virtual measures in the electronic realm—such as limiting access with security settings, password protection and data encryption—to ensure that electronic records can be viewed only by authorized individuals. Security measures are vital where storage is in “the cloud”—accessible on the web and hosted on a remote server not maintained by the employer on its premises.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002

As in the case of paper records, employers must ensure that their electronic storage system follows the rules that apply to particularly sensitive information, such as medical data or drug testing results. By law, those documents must be stored confidentially in a file that is separate from an employee's personnel file.

For various legal reasons, I-9 forms should also be maintained separately from personnel records.

4. Plan retention, destruction

Think carefully about how long to preserve personnel records and when to destroy them.

Even though maintaining electronic files costs very little, storing electronic records indefinitely can be counterproductive—for example, in cases where a court orders an employer to produce damaging electronic personnel records that it could have lawfully destroyed at an earlier date.

Many businesses implement document retention and destruction policies that set minimum retention periods, while providing for the eventual destruction of unnecessary documents. If you're trying to develop a records retention and destruction policy, make sure you comply with all applicable laws.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002