

## Keep Personnel Information Under Lock And Key

In a recent case, a large nonprofit association paid more than six figures to correct the credit of 100 of its highest paid employees. The reason, a security breach occurred when the organization changed life insurance policies. It hand delivered to its new broker paper documents containing all the necessary information – names, birth dates, addresses and social security numbers. A temporary worker for the insurance broker proceeded to photocopy and sell the information. The breach wasn't discovered until employees began receiving credit card bills for hundreds of dollars in items they hadn't purchased.

Worse than the financial and administrative burdens was the cost to morale. Seven of the association's senior employees quit as a result of the security breach.

What precipitated this security breach nightmare and subsequent damage to organizational morale? Is unauthorized access to personnel files difficult to obtain?

### Unauthorized access – the biggest risk

The following situation is all too real. Paper files are left on the desk by an employee who has access to employee records, another employee who may or may not have access comes and looks at them. The employee is looking at the record to see salary information or performance appraisals with the intention of harassing or stalking them.

While identity theft may be the biggest risk of unauthorized access, most breaches of personnel records involve one employee obtaining information on another, violating their privacy for clandestine motives, usually by looking at paper files.

Most authorities say that one of the best protections against someone lifting a paper personnel file is to have as little on paper as possible. The following are some recommended policies and procedures to maintain the tightest security of personnel information:

- Appoint someone to be in charge of personnel security, preferably the HR director.
- Keep the file drawers locked when not in use.
- Assign employee numbers, rather than using social security numbers.
- Shred documents after you are no longer required to keep them or they are not needed.

Congress has passed several laws in recent years that regulate how employers should guard personnel information. There are laws that govern how long you should keep certain personnel records and when you should dispose of them. For a full listing of these requirements, go to [www.dol.gov/esa](http://www.dol.gov/esa).

### What This Means For Counties

When files meet the terms of the disposal laws, they should be shredded. It is imperative that counties have a system of destroying files. With possible liability for any breach that violates employee privacy, counties will want to implement the suggestions in this update if they have not already done so.

For more information, contact CTSI at 303-861-0507.