

BLOGS

Archive; Privacy & Information Security; Workplace Policies

Just How Much Information Should You Have?

Okay – technology has done some wonderful things for all of us, including giving us the ability to store lots and lots of information. But, do you really want to do that?

Many employers are looking at ways to be more efficient by using technology to gather and store information about employees and applicants. Employers store everything from names to social security numbers to discipline data on electronic systems.

You may say, well that's just being efficient. I'm all for efficiency, but employers need to be aware that they have to balance their need for information with the employees rights relating to the personal information that is being gathered. We've all heard about companies that have been hacked and companies that inadvertently release protected information about employees or customers. Both federal and state governments have reacted to those events by enacting laws relating to how you may use and store certain types of information. Here are some of the restrictions employers gathering information need to think about:

1. Under 325E.61 of the Minnesota Statutes, if employers do not encrypt personal information (first name or initial together with last name and social security number, drivers license number or account numbers), they must notify all affected person of any unauthorized disclosure of the information.
2. The Federal Fair Credit Report Act requires that information obtained from credit reporting agencies be managed and disposed of properly.
3. The Federal Trade Commission (FTC) has entered into consent decrees with employers regarding their handling of employment records. In a matter involving the Rite Aid corporation, the FTC filed a complaint against Rite Aid for, among other things, improper disposal of employment applications. [Rite Aids settlement with the FTC](#) requires independent audits for twenty years, implementation of a comprehensive security program, and on site examinations by the FTC.

So, how should employers deal with this information? Here are some guidelines:

1. Only acquire information you use. Don't acquire information simply because you always have. Focus on current business need.
2. Restrict access to information so that only those with a documented business need can get it or pass it on.
3. Adopt appropriate written policies regarding data security and retention, including:
 - Assigning responsibility for security of records



- Training staff
- Defining appropriate uses of information
- Risk management
- Response programs in the event of a breach