

## JUST HOW SAFE IS YOUR CLIENT'S INFORMATION?

By Diane L. Drain, attorney, computer nerd and neurotic (1998)

With the advent of computers information is no longer kept in a form that we can see and touch. Instead, information is now kept in a form that is as understandable as paintings by Picasso or Dali. That information is now being stored in a method called an electronic format. This form of storage is the future, but we must understand what this means to us as lawyers. Confidentiality is our sword and security our shield. In order for both confidentiality and security to be honored as in the past we must train both our staff and ourselves what the words "erased" and "deleted" really mean in the electronic format vernacular. We have seen some prime examples of attorneys not understanding these terms in many of the lawsuits that have reached national acclaim. The ongoing investigation by the Office of the Independent Counsel of the President and other individuals is currently the best-known example of this little understood issue and could become a nightmare.

If you have read the Starr report you will see several references to "document recovered", "e-mail retrieved" and "deleted file recovered from...". In each case I would hazard a guess that either the writer or the recipient had assumed that their message was erased or deleted when they so instructed their computer. Unfortunately, what the users did not understand was that a computer never truly erases or deletes a document (file). Instead, it just changes the marker at the beginning of the file and removes it from the indexing system in the computer. The document still exists in its original form, but now is exposed to being written over, whenever the computer happens to load more information in that same location. Even writing over the top of an old document may not completely erase it. There are still ghosts or reflections of the original document, which can be lifted using software specifically designed for that purpose.

Another problem is e-mail. Just as our traditional mail can be intercepted, so can our electronic mail. When that e-mail is downloaded to our computer it is stored. Again, even if we delete the letter or memo it still exists on the computer. What are the discovery issues related to e-mail inadvertently sent to the wrong company? More litigation to come.

You say that you do not receive the type of information that would put you into the spotlight of our law enforcement agencies. What about sensitive information that your clients fail to properly control? What about situations that happen every day which cause for privileged or sensitive information to be shared with others? Users in a computer network access private files. E-mail that is accidentally left on the server, or even deleted, but still accessible. Computer literate janitors who are bored late at night. Outsiders who accidentally find their way into a computer network. Children playing with a laptop or home computer. Two situations that happen very regularly are: (1) returning a faulty hard drive or exchanging it for an upgraded; or (2) junking of old computers with hard-drives still in place.

Last year a woman in Nevada bought a used computer that had the names, addresses, social security numbers and prescription information for 2,000 people, including those being treated for AIDS, alcoholism and mental illnesses. That really perked the attention of you PI lawyers -- does that sound like a valid cause of action?

Solutions can be found in the form of encryption. Encryption is a form of secret encoding. The more sophisticated the encoding the less change of it being broken by anyone other than its intended user. E-mail can be encrypted and should be in the case of confidential information. There are several software packages that will assist in this process. RSA SECURPC (by Security Dynamics Technologies) is designed to make documents almost impenetrable. Another package is called PGP ([www.pgp.com](http://www.pgp.com)). The government has even gotten into the picture arguing that some of this software is so secure that it may become a national security issue. There have been some rumors of the government demanding that all software providers provide a backdoor through each of these programs. That also opens up some interested litigation issues.

Simple procedures that should be adopted by every law office (and our clients too) is to password on several levels. Each computer should have its own password to start the computer (also there are locks on all computers – use them). Access to the network should have another password, and access to vital information (client documents or bookkeeping information) should have additional passwords. In truth each of these passwords can be broken by a computer tech-head, but how many tech-heads do you really believe want into your computer? The passwords are really there to protect you from an accidental invasion or noisy person. But these passwords are only as good as those that use them. If you or your staff become lazy then all your security plans are for naught. If you fail to change the passwords when an employee or technician leaves the firm, then your computer system is exposed to possible sabotage or invasion. If you do not password your laptop and it is stolen at the airport – is that malpractice? .

It is best that you and your staff understand the steps that must be taken to make certain that all documents, both privileged and otherwise, are exposed only on design. These problems are very real and will only get worse as we become more comfortable with storing information in an electronic format. Plan ahead, implement office procedures and train everyone to understand and to follow these procedures without exception.