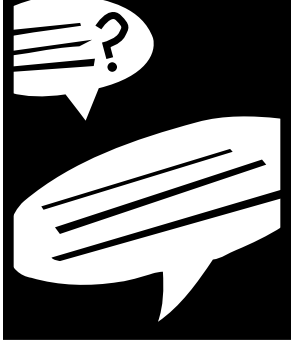

Seven Steps to Privacy Protection

What's the best way to protect your clients' privacy?

Q: I work for a social-service agency. Some of our clients have expressed concern about security and confidentiality in the information age. Is there a difference between security and confidentiality? Are there special problems we should be aware of when we use computers? How can we best address our clients' concerns? Can you give us some steps to follow?

A: People who receive social services have legitimate concerns about privacy. Client information could be embarrassing and damaging in the wrong hands. It is crucial that you treat client information with extreme care.

Perhaps the best way to look at it is this: Treat every client's file as if it were your own. Safeguard the security and the confidentiality of the information appropriately.

Yes, there is a difference between security and confidentiality. Security speaks to how easy it is to *access* information. Confidentiality has to do with *sharing* information.

When privacy is breached, it's often due to a security problem. Information wasn't secured properly and someone was able to see it. An example would be if you left your office with the door unlocked and a file on your desk. Anyone walking in would have access to the information.

A breach of confidentiality usually involves discussing clients without their permission. It could be an innocent comment overheard in a hallway. Or it could be an attempt to get more services for your clients without asking them if you may speak to the agency to which you're referring them. Either way, unless you have a client's permission or are within specific legal guidelines, you shouldn't discuss client information with others.

Technology doesn't pose any unique threats to privacy. What technology does is to magnify a breach in confidentiality by speeding up the dissemination of information.

Nor is security more of a problem with computerized records than with written ones. Many security measures have been developed to safeguard database information. In many cases, putting information into a database with good log-in and password procedures is more secure than traditional methods. When's the last time a file cabinet asked you for a password before you opened the drawer?

A critical element in safeguarding confidentiality is the people with access to the information. In a recent fiasco, a health clinic employee saved HIV test results onto a computer disk and offered it for sale in a Florida bar. The result was a flurry of regulations governing access to sen-

When's the last time a file cabinet asked you for a password?

sitive data. None of those regulations, however, would prevent the same thing from happening. The computer disk didn't violate anyone's confidentiality; the person who stole the information did.

Information age or not, here are rules to follow:

1. Hire the right people. Be sure they share your organization's values, including the value of clients' privacy. You can't teach someone values.

2. Create a confidentiality policy with a client consent form as its cornerstone. Specify what information will be shared, with whom, and for how long the consent form will be in effect. You can get sample consent forms from national associations in your sector or fellow service providers.

3. Implement good, solid procedures that reduce the risk of inadvertent sharing of information. This includes getting consent forms signed.

4. Train everyone in the procedures. Make sure they understand how even innocent conversations or actions intended only in the client's best interests may actually violate that person's privacy.

5. Remember the two biggest technology culprits in the information age—not databases and computers but phones and fax machines. If you call another agency to discuss a client, you need a signed consent form that covers that communication. If you fax a referral form to another agency on behalf of a client, make sure the appropriate person knows it's coming and gets it off the machine right away. These are two situations in which nonprofits frequently compromise confidentiality.

You can't teach someone values.

6. Be sure that all your information systems—paper or electronic—are as secure as they can be. Security protocols for databases include firewalls, user identification numbers, passwords, encryption, and data compression. Paper-file storage relies on more physical security measures, such as locked doors and sign-out sheets.

7. Check the laws in your state. Privacy is mostly a state issue, although there are some specific federal statutes you need to follow as well, especially as they relate to HIV, AIDS, mental health, and substance abuse. Check the Federal Code of Regulations and your state's regulations on client information. Have an attorney from your state doublecheck your policies and procedures. Your local Legal Aid Society may have guidelines or attorneys who specialize in this issue.

Human Services Technologies, Inc.
988 Woodcock Road, Suite 101
Orlando, Florida 32803
www.humanservices.net

Nonprofit World • Volume 19, Number 2 March/April 2001
Published by the Society for Nonprofit Organizations
6314 Odana Road, Suite 1, Madison, WI 53719 • (608) 274-9777
www.danenet.org/snpo