Laptops threaten confidentiality

By Ofer Zur, Ph.D.
and Jeffrey Barnett, Psy.D., ABPP

Laptop theft is very common. Some estimates suggest that a laptop is stolen every minute and most of them are never recovered.

Laptops are stolen from cars, offices and homes. They are mistakenly left behind in cabs, coffee houses, hotel rooms and restrooms. Missing laptop computers that contain clients' confidential information seem to be becoming weekly news in the media.

Administrators, programmers, psychologists and researchers often travel with a laptop. Psychologists who work in multiple offices often find it especially helpful or even mandatory to utilize a laptop to transport clients' records with them. Inevitably, some laptops are stolen and inevitably there are breaches of confidentiality.

Laptops or notebooks often contain the owners' personal information, confidential office documents, clients' confidential information, such as clinical notes, diagnosis, treatment plans, test results, billing records, reports, testimonies and much more.

Obviously, a theft or an accidental loss could put psychotherapy clients or patients and clinics and organizations, as well as the therapists themselves, at some serious risk.

Theft of desktop computers is almost as prevalent and many of the considerations here are highly relevant to desktop office computers as well. While theft of laptops cannot always be prevented, it is the duty of the psychologists and administrators to do their best to prevent breach of confidential information and, when such breach occurs, handle it appropriately.

In one of the few enforcements of HIPAA by Health and Human Services (HHS), a Seattle company that provides home health care services was forced in mid 2008 to pay a $100,000 settlement because laptops, disks and tapes containing individuals' health records were taken from company employees' cars on five occasions in 2005 and 2006.

The agreement seems to signal that HHS is finally taking a tougher stance toward violations. This may have started a shift from the education approach they have taken so far to an enforcement mode. This HIPAA enforcement action suggests that psychotherapists who carry patient records with them are at risk for security violations and may be held legally and ethically accountable for security and privacy breaches.

Therapists may want also to assess whether or not the stolen laptop contains only confidential clinical information or also includes billing information, which may provide data (e.g., Social Security numbers) for someone to steal the identity of patients.

While laptops are here to stay and theft and breaches of confidentiality cannot be always avoided there are a several things that psychotherapists, counselors and administrators should implement in order to protect their clients and themselves.

Guidelines on how to handle a laptop outside the office:

• The use of laptop computers must be addressed in the informed consent process, and any potential drawbacks or risks involved must be discussed along with all precautions taken to preserve and protect each counseling client's confidentiality.

• There are several ways that therapists may inform their clients and help them make informed consent regarding electronic records and laptops. When appropriate, therapists may inform or discuss the issue in person. More commonly, Office Policies, which clients receive prior to treatment or in the first session, may include a section on keeping and transporting electronic records.

• Generally, if you keep electronic clinical records, it means that you are a "Covered Entity" under HIPAA and must be HIPAA compliant.

Becoming HIPAA compliant is not hard:

• Make sure that the laptop has a security password installed. Do not make your password something others can easily figure out, such as your pet's name, your birth date, your child's name, or your nickname. Periodically change your passwords.

• Backup and more backup. Automatic periodic backups are very simple to install and use. If you do not have an automatic backup system, download all materials from your laptop onto a computer disk on a daily basis. Store all disks apart from the laptop in a locked storage cabinet, preferably off site.

• Use virus protection and a firewall on all computers, including laptops. Make sure you have automatic or other means to update your virus protection and firewall.

• Delete all confidential files from your laptop that you will not need to access when going on a vacation or to a conference.

• Consider using additional password protection for the actual clinical files or folders on your computer.

• HIPAA guidelines are "technologically neutral." They do not mandate any specific technology or method, they just focus on how to maintain confidentiality in the best and most appropriate and relevant ways.

• Encryption is often recommended but so far is rarely, if ever, used by psychotherapists in private practices, small clinics or agencies.

• Treat the laptop like the cash in your wallet and never leave it unattended, even when you are leaving the car for a few minutes or just taking a short break to use the restroom or the coffee vending machine.

While traveling or attending a conference with your laptop:

• The easiest option to secure your laptop against theft is to put it in its carrying case and keep it on your shoulder at all times.

• Never grant other persons access to your laptop computer if you store confidential client information on it unless they are part of your clinical operation and need to have access to your laptop or to confidential information, are HIPAA trained and have a written contract that includes a statement about confidentiality of electronic records.

• Therapists who use billing programs, such as Therapist Helper, might want to contact the software companies to see if they have any helpful hints regarding security for their products and what they might recommend if the laptop gets stolen.

• When using your laptop computer to store confidential client information as well as to administer psychological tests and assessments, always closely supervise the use of the laptop. Never leave it unattended or unsupervised during testing.

• When deleting confidential records from your laptop, special software to wipe the hard drive must be used. Otherwise, even though you hit the delete button, others may be able to recover the materials from your hard drive. If you are not familiar with this special software, hire a techie to install it.

More diligent and extreme, however rarely used, methods for protecting your laptop and data have been suggested by technically sophisticated experts:

* Physically secure your laptop with a locking cable whenever you are not personally carrying it.

* Don't use an obvious laptop bag. Carry your laptop in regular luggage that doesn't look like it has a laptop. Don't advertise your laptop to any would-be thieves.

* Encrypt data on your laptop.

* Use visual locks and restraints to secure your laptop and to act as a deterrent.

* Use anti-theft software that can track and locate your laptop or computer through the IP address once the stolen laptop is used to access the Internet.

* Use invisible ultraviolet markings so that any recovered stolen laptops will be clearly marked as yours to the police.

* Have a remotely controlled self-destruct solution in place.

When records are stolen and/or patients' confidential information is compromised or potentially compromised:

• Notify the clients who may be affected, unless there are (rare) compelling reasons not to do so. Examples of such situations would be when a client is suicidal or in crisis. If you choose not to notify a client, document your reasons in your records and outline a plan as to when you will tell.

• Assess if beside the clinical/confidential information, the lost computer may also contain personal information, such as Social Security numbers, that can readily lead to identity theft.

• Notify any other people (non-clients) who may be significantly affected with such a breach, unless there are reasons not to do so.

• File a report with police and with other agencies if necessary or required.

• Consult with your state or national ethics committee to discuss the matter and learn what additional steps or actions they may recommend.

• Consult with your malpractice insurer's risk management experts for advice and suggestions as well.

• Therapists who use billing programs might want to contact the software companies to see what they recommend.

• Review and update your security procedures to help ensure that such a breach cannot happen again. Learn from your mistakes. **CE**

Ofer Zur, Ph.D. is a psychologist, author, lecturer, forensic expert and director of the Zur Institute, LLC (www.zurinstitute.com), which offers more than 90 online courses for CE credits. His e-mail address is: drozur@drzur.com

Jeffrey E. Barnett, Psy.D., ABPP, is a licensed psychologist in Arnold, Md., and is a professor on the affiliate faculty in the Department of Psychology at Loyola College. He is a regular columnist for The National Psychologist *on ethics.. His e-mail address is drjbarnett1@comcast.net*