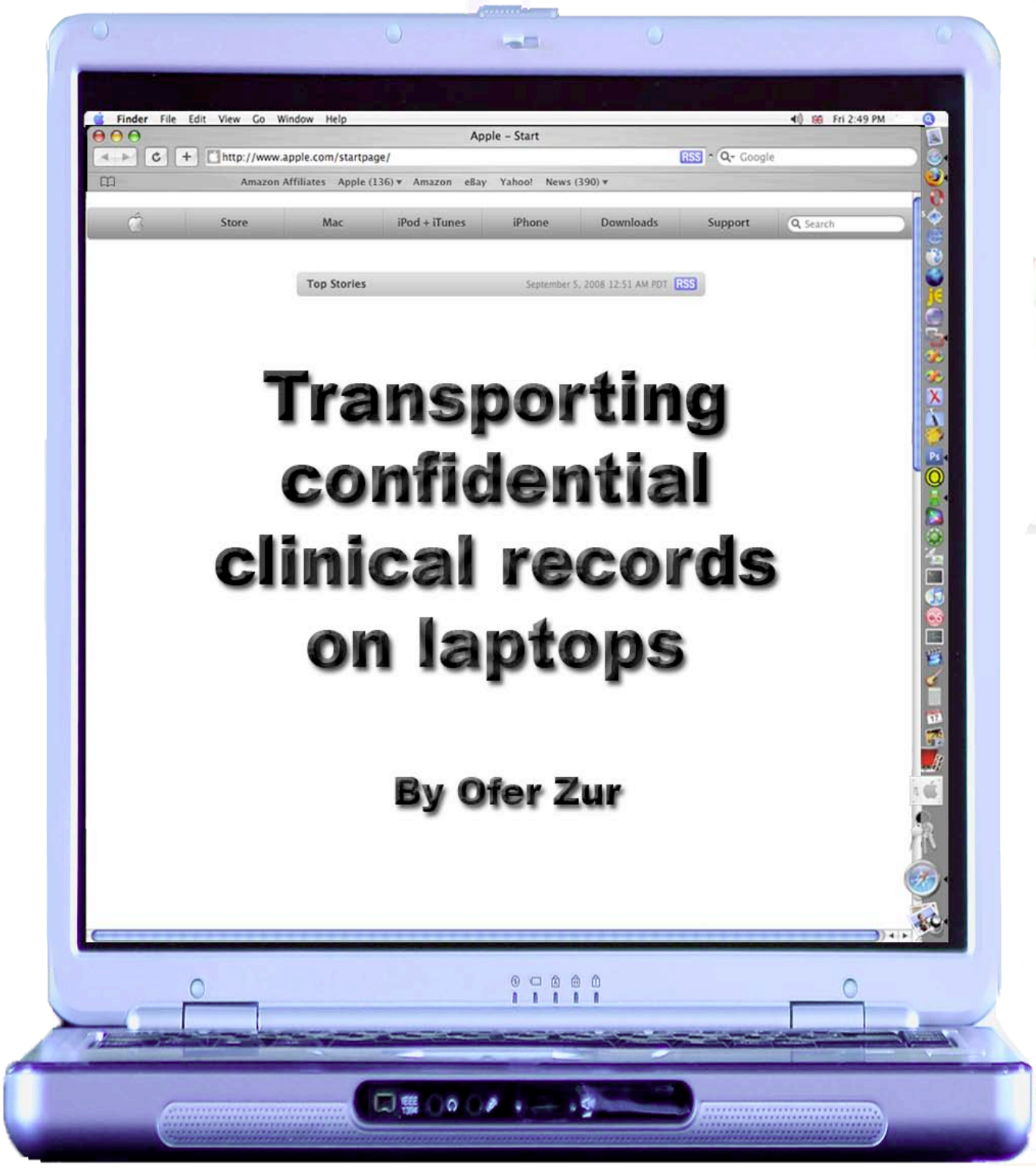

Finder File Edit View Go Window Help
Fri 2:49 PM
Apple – Start
http://www.apple.com/startpage/
Google
Amazon Affiliates Apple (136) Amazon eBay Yahoo! News (390)
Store Mac iPod + iTunes iPhone Downloads Support
Search
Top Stories
September 5, 2008 12:51 AM PDT
Transporting confidential clinical records on laptops
By Ofer Zur

Stolen laptop computers that contain clients' confidential information seem to become weekly news in the media. Administrators, programmers, psychotherapists, and researchers often travel with a laptop. Clinicians who work in multiple offices often find it especially helpful or even mandatory to use a laptop to transport clients' records with them. Inevitably, some laptops are stolen, and inevitably there are breaches of confidentiality. This short article will help psychotherapists, counselors, administrators, and directors strategize how to do their best to prevent laptop theft and what to do when laptops are stolen.

Laptops or notebooks are not just expensive pieces of hardware—they often also contain the owners' personal information, confidential office documents, a log of websites that have been visited recently, and clients' confidential information, such as clinical notes, diagnose, treatment plans, test results, billing records, reports, testimonies, and much more. Obviously, a theft or even an accidental loss could put psychotherapy clients or patients and clinics and organizations, as well as the therapists themselves, at some serious risk.

Laptop theft is not a rare phenomenon. 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. While theft of laptops cannot always be prevented, it is the duty of the psychotherapists, administrators and directors to do their best to prevent breach of confidential information and, when such a breach occurs, to handle it appropriately.

"Laptop theft is not a rare phenomenon. Some estimates suggest that a laptop is stolen every minute and most of them are never recovered."

In one of the few enforcements of the Health Insurance Portability and Accountability Act (HIPAA) by Health and Human Services (HSS), 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 to assess whether or not the stolen laptop only contains confidential clinical information or also includes billing information, which may provide data (e.g., Social security numbers) for someone to steal the identity of any and all patients. Most psychotherapists are more likely to be concerned about their clinical notes and how they can affect or embarrass their clients and not realize that it is the patient who is potentially in serious danger of identity theft.

While the APA, ACA, CAMFT, NASW and most other professional organizations' codes of ethics attend to the general issues of confidentiality, they do not specifically address the issue of laptops or electronically transporting clinical records. However, the professional codes of almost all professional associations apply to all professional activities regardless of the role and regardless of the medium. The use of laptops in psychotherapists' professional roles, like the use of the internet, falls under the requirements of these codes of ethics.

While laptops are here to stay and theft cannot be always avoided there are a several things that psychotherapists, counsellors, and administrators should consider and implement.

General information and practice guidelines: 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 couselling client's confidentiality. This includes methods used to prevent unauthorized access to one's laptop at home, at work, or elsewhere.

There are several ways that therapists may inform their clients and help them provide 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. (For over 50 Clinical Forms, including Office Policies: go to:

http://www.zurinstitute.com/forms.html

Following is a sample paragraph that may be included:

E-MAILS, CELL PHONES, COMPUTERS AND FAXES:

> It is very important to be aware that computers and e-mail and cell phone communication can be relatively easily accessed by unauthorized people and hence can compromise the privacy and confidentiality of such communication. E-mails, in particular, are vulnerable to such unauthorized access due to the fact that servers have unlimited and direct access to all e-mails that go through them. Additionally, Dr. X's e-mails and data on his/her computers are not encrypted. It is always a possibility that faxes can be sent erroneously to the wrong address and computers, including laptops, may be stolen. Dr. X's computers are equipped with a firewall, virus protection and passwords, and he/she also backs up all confidential information from his computers on to CDs (stored off-site) on a regular basis. Please notify Dr. X if you decide to avoid or limit, in any way, the use of e-mails, cell phones or faxes, or storage of confidential information on computers. If you communicate confidential or private information via e-mail, Dr. X will assume that you have made an informed decision, will view it as your agreement to take the risk that such communication may be intercepted, and s/he will honor your desire to communicate on such matters via

e-mail. Please do not use e-mail or faxes for emergencies. Due to computer or network problems, e-mails may not be deliverable, and Dr. X may not check her/his e-mails or faxes daily.

- 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 very hard. For details go to:

  http://www.zurinstitute.com/hipaa.html

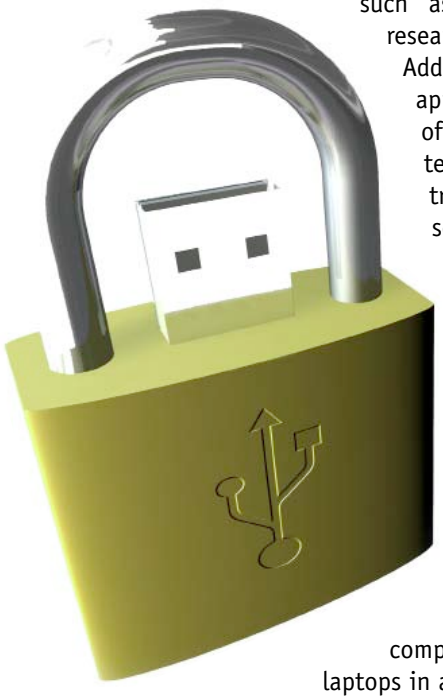
- Make sure that the laptop has a security password installed. Do not make your password something others can easily figure out, such as your pet's name, your birth date, your child's name, or your nickname. Periodically change your passwords.
- Backup, backup and backup. Automatic periodic backups are 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 in a different structure or different location from the computer.
- Use virus protection and a firewall on all your computers, including your laptop. 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. Of course, keep back-ups of these files on your main computer, disc, flash-drive, etc.

"It is very important to be aware that computers and e-mail and cell phone communication can be relatively easily accessed by unauthorized people and hence can compromise the privacy and confidentiality of such communication."

- You may consider using additional password protection for the actual clinical files or folders on your computer.
- Consult with computer experts to ensure you utilize proper and appropriate available security procedures and techniques.
- 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 used by psychotherapists in private practices, small clinics, or agencies. The main users of encryption have been those who do their billing online, health insurance companies who have online billing services, and those in certain industries with concerns about industrial espionage. Encryption software programs are increasingly more readily available and are likely to be more commonly used by psychotherapists in the future.
- 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.
  - When in your hotel room or even when in the office, consider securing it to an object that is not easily movable, such as a desk or dresser. Most laptops have a hole on the side that is used to lock in place a cable with a combination lock. This may be used in your office, hotel, etc. when the laptop is left unattended. Remember, it only takes a minute for a laptop (or wallet) to be stolen.
  - Physically secure your laptop with a locking cable whenever you are not personally carrying it.
  - Never leave it unattended such as in the overhead bin in an airplane when you go to the restroom or in your car when you run into a store for 'just a few seconds.' The same applies to external hard drives, flash drives, and the like.
- Never grant another person 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 which includes a statement about confidentiality of electronic records.
- Therapists who use billing programs, such as Therapist Helper, might want to contact the software company to see if they have any helpful hints regarding security for their product, 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.
- Strictly follow all security procedures each and every day. It just takes one minute away from your laptop, putting it down unattended for 30 seconds, not backing up data just one time, failing to use password protection one time, or letting virus protection software lapse one day to violate clients' trust and our responsibilities to them to protect and preserve their privacy in every reasonably available way.
- More diligent methods for protecting your laptop and data have been suggested by technically sophisticated experts.

Following is a list of extra, not commonly used, available measures obtained from buzzle.com:

- 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. It won't fool hardened thieves but most will opt for a less secure laptop. For example, you can use a product like STOP. This system works by attaching a specially made security plate to your laptop. This plate is bar-coded and registered. It also carries a warning label letting would-be cyber thieves know that the ownership of your laptop is permanently monitored.
- 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. Keeping track of your laptop's serial number is also a good idea and have this number stored in a different place than on your laptop.
- If you place important information on your laptop, have a remotely controlled self-destruct solution in place. Then your highly sensitive information can be deleted remotely after your laptop is stolen.



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

- Notify the clients who may be affected by such breach of confidentiality, 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 them.
- Assess whether, besides the clinical-confidential information, the lost computer may also contain personal information, such as Social security numbers or identity numbers, that can readily lead to identity theft.
- Notify any other people (non-clients) who may be significantly affected with such 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 their advice and suggestions as well.
- Therapists who use billing programs might want to contact the software company to see what they might recommend.

Review and update your security procedures to help ensure that such a breach cannot happen again. Learn from your mistake.

Codes of Ethics

While the APA, ACA, CAMFT, NASW and most other professional organizations' Codes of Ethics attend to the general issues of confidentiality, they do not address, specifically, the issue of transporting clinical records. However, the APA Ethics Code (APA, 2002), for example, clearly states in the Introduction and Applicability section that the standards of the Ethics Code apply to all professional activities of psychologists, such as the provision of clinical services, research, teaching, supervision, and others. Additionally, it states "The Ethics Code applies to these activities across a variety of contexts, such as in person, postal, telephone, Internet, and other electronic transmissions" (p. 1061). Thus, it can be seen that the APA Ethics Code applies to all professional activities of psychologists regardless of the role and regardless of the medium. The use of computers in psychologists' professional roles (and the use of the Internet) falls under the requirements of the Ethics Code. Relevant standards of importance to laptop computer and Internet use include:

2.03 Maintaining competence:

Be sure to develop all needed competencies (knowledge and skills) to use laptops in a safe and appropriate manner.

3.04 Avoiding harm:

Failure to secure one's laptop, allowing unauthorized individuals access, or allowing breaches of confidential information all may result in harm to clients who are trusting us to protect and preserve their privacy.

3.10 Informed consent

All possible limits to confidentiality should be reviewed with clients at the outset. If a laptop computer will be used, the client should be informed of this in advance. All steps taken to protect each client's privacy should be reviewed, and clients should be informed that they would be notified immediately if any security breaches occur.

4.01 Maintaining confidentiality

"Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium…" (p. 1067). We each must use all reasonably available technologies and practices to protect and preserve each client's confidential information.

4.02 Discussing limits of confidentiality

As part of the informed consent process, we must ensure that clients understand all "risks to privacy and limits of confidentiality" (p. 1067) that come with the use of laptop computers.

4.05 Disclosures

Unless authorized by the client or mandated/permitted by law, psychologists do not disclose confidential client information, even unintentionally, such as through avoidable security breaches.

6.01 Documentation of professional and scientific work and maintenance of records

We are required to "maintain…store, retain, …records and data relating to [our] professional and scientific work…" (p. 1069). Clearly, these records may be stored and maintained, and retained on one's laptop computer.

6.02 Maintenance, dissemination, and disposal of confidential records of professional and scientific work

We must take all reasonable steps to ensure that records under our responsibility are maintained in a manner that protects and preserves each client's confidentiality "whether written, automated, or in any other medium" (p. 1069). Further, "If confidential information concerning recipients of psychological services is entered into databases or systems of records available to persons whose access has not been consented to by the recipient, psychologists use coding or other techniques to avoid the inclusion of personal identifiers" (p. 1069).

8.02 Informed consent to research

All research participants must be fully informed of all "limits to confidentiality" and "reasonably foreseeable factors that may be expected to influence their willingness to participate, such as potential risks…" (p. 1070).

9.03 Informed consent in assessments

The informed consent process for assessments includes an open discussion of "the limits of confidentiality" (p. 1073). Assessment materials and reports should be preserved and protected on laptop computers just as all confidential materials should.

9.11 Maintaining test security

Psychological tests may be administered through laptop computers. In fact, some test may only be given using a computer, such as continuous performance tests. Others may be more easily administered and scored using computer software. "Psychologists make reasonable efforts to maintain the integrity and security of test materials and other assessment techniques" (p. 1074) regardless of the medium with which they are stored.

10.01 Informed consent to therapy

As has been highlighted, all reasonably anticipated limits to confidentiality should be included and openly discussed in the informed consent process. Further, just sharing this information is insufficient. To ensure that informed consent is valid, we must ensure each client's understanding of the information provided.

Similar guidance is found in the ACA Ethics Code (ACA, 2005), which includes standards on informed consent, confidentiality, avoiding harm, research, assessment security, and competence as highlighted above. For example, in Section B: Confidentiality, Privileged Communication, and Privacy, Standard B.1.d. Explanation of Limitations, it states: "At initiation and throughout the couselling process, counselors inform clients of the limitations of confidentiality and seek to identify foreseeable situations in which confidentiality [may] be breached" (p. 7).

Further, Standard B.3.e. Transmitting Confidential Information is relevant to the storage and maintenance of client information on laptop computers, as well. It states: "Counselors take precautions to ensure the confidentiality of information transmitted through the use of computers, electronic mail, facsimile machines, telephones, voicemail, answering machines, and other electronic or computer technology." (p. 8).

At initiation and throughout the counselling process, counselors inform clients of the limitations of confidentiality and seek to identify foreseeable situations in which confidentiality may be breached.

Further, the ACA Ethics Code additionally includes Standard A.12, Technology Applications, which includes:

A.12.a. Benefits and limitations

"Counselors inform clients of the benefits and limitations of using information technology applications in the counselling process and in business/billing procedures. Such technologies include but are not limited to computer hardware and software, telephones, the World Wide Web, the Internet, online assessment instruments, and other communication devices" (p. 6).

A.12.g. Technology and informed consent

- "Address issues related to the difficulty of maintaining the confidentiality of [laptop computers]" (p. 6).
- "Inform clients of all colleagues, supervisors, and employees, such as Informational Technology (IT) administrators, who might have authorized or unauthorized access to [laptop computers]" (p. 6).
- "Urge clients to be aware of all authorized or unauthorized users including family members and fellow employees who have access to any technology clients may use in the counselling process" (pp. 6-7).

This article can be found on the Zur Institute website: http://www.zurinstitute.com at http://www.zurinstitute.com/onlinedisclosure.html and reported here by kind permission of Ofer Zur.

Earlier versions of this article was published in the Independent Practitioner, V. 28/2, pp 83-85, 2008 and in the National Psychologist journal pp, 22, 2008.