Vol. 03, No. 8 / August 2004

Are your electronic patient records secure?

Protect your computer network with passwords, anti-intrusion measures.

John Luo, MD
Assistant clinical professor Department of psychiatry University of California Los Angeles

Is your office computer system-and the confidential patient records it contains-safe from hackers?

Maintaining office computer security isn't just good practice-it's the law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires physicians to ensure that patient records are kept confidential.[1] Although the same physical security issues apply to paper records, ease of transmission makes electronic records a higher security risk.

You can easily and inexpensively prevent security breaches by restricting access to the office network, updating your operating system (OS), and installing an anti-intrusion program.

WAYS TO RESTRICT ACCESS

Passwords are fairly basic and easy to implement, but they:

- must not be too easy to guess
- should never be in plain view, such as on a sticky note on the monitor.

If you must write the password down, store it safely in another location.

Passwords should be changed every 3 months and should never be shared, so that a disgruntled ex-employee cannot access electronic patient files or other data after he or she leaves the practice. Microsoft offers suggestions for creating secure passwords, such as using a combination of eight characters.[2]

BIOS/Open firmware passwords further restrict access by preventing unauthorized users from turning your computer on. A Windows OS-based computer BIOS program essentially starts the computer and manages data flow between the OS and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer. Open Firmware is the Mac OS equivalent to BIOS.[3]

For information on setting a BIOS password, click here.

Hardware tokens are pocket-size devices that, when connected to the computer, allow access by entering the proper password. Hardware tokens are suitable for managing off-site remote access and add another layer of security for local access.

Medical records programs. Most software programs allow administrators to restrict access to medical records by setting up levels of ability to access and modifying electronic records for different users. Each user should have a unique password for authentication. The software also should have an audit trail capability, so that each user's activity with electronic patient records can be reviewed.

SECURITY BREACHES

An Internet connection-however brief-can invite security breaches that allow hackers to access patient information, delete

programs, steal passwords, disrupt other Internet-connected computers, and erase the hard drive. Avoiding Internet connections altogether would increase security, but this is not feasible.

- **Viruses** reproduce using the host computer, most commonly by infiltrating the e-mail program and making it hard to detect corrupted files.

- **Worms** are similar to viruses but are self-contained, whereas a virus must attach to another file.

- **Trojan horse** programs, usually disguised within seemingly legitimate Internet programs, are less common than viruses or worms. They do not replicate but are equally dangerous. You unknowingly start the Trojan horse after downloading what looks like a useful program. The Trojan horse then self-installs silently, giving the hacker who created it access to your computer.

- **Port attacks** are malicious attempts to connect and eventually take over another computer. A 'port' is a software 'location' where a program on another computer can connect to a host computer.

  Common-sense measures. To reduce the chances of a security breach:

- **NEVER** open e-mails from unfamiliar sources. Viruses are commonly sent as attachments, which you should never open unless you know they are safe.

  An e-mail from a familiar source containing an odd attachment or an unusual or strangely spelled subject may be a virus that has infected your colleague's computer.

- **Turn off your computer** or disconnect from the Internet when not in use.

- **Back up your data** regularly. Put patient files in one folder or directory, then copy them to a backup medium such as CD-ROM, zip drive, or portable hard drive. Of course, keep the disks in a secure place.

ANTI-INTRUSION PROGRAMS

Antivirus programs can check for the latest viruses and their variants and remove them. To do this, automatically update the program with new virus signature files- files created by antivirus program vendors to help the software identify viruses. Most antivirus programs will automatically check the vendor's Web site for updated files if the computer is connected to the Internet.

Virus signature files should be updated daily to provide maximum protection. Most companies provide a 1-year subscription to the updates, which must be renewed upon expiration for new virus definition files.

Manual updating is acceptable but may be too time-consuming for a busy office.

Well-known antivirus programs include Norton AntiVirus, VirusScan, PC-cillin, and Panda AntiVirus, which cost between $40 and $60. Most antivirus programs also check for worms and hybrid worm-viruses.

Programs that guard against Trojan horses, such as Emisoft A [2], Anti-Trojan Shield, and XoftSpy, are available for between $30 and $40.

Patches, or OS updates, can protect patient files from intrusion via the Internet at no charge. Patches fix other problems, but most patches provide security updates when OS flaws are found.

Patches should be installed as soon as they become available. Visit http://windowsupdate.microsoft.com for information on Microsoft Windows OS updates, or http://www.apple.com/support/ for Mac OS updates.

Firewalls. Updates close most susceptible OS ports from attack, but other ports are opened when programs that require Internet access are installed. A 'firewall' is necessary to monitor port activity and prevent intrusion.

Office computers linked to a network that shares an Internet DSL or cable modem with another network typically are connected via a router. Such computers usually have built-in firewalls (See " Wireless Internet 101," Psyber Psychiatry, December 2003)

If your computer is connected directly to the DSL or cable modem or a telephone line, you probably need a firewall. The most recent Microsoft Windows XP and Mac OS X versions each include a software firewall, which should be activated upon installation.

Windows-compatible firewall programs include ZoneAlarm, Sygate Personal Firewall, Symantec Norton Personal Firewall, and Tiny Software Personal. Mac OS-compatible firewalls include Intego NetBarrier, Sustainable SoftworksIPNetSentryX, and Norton Personal Firewall.

Once your firewall is installed, check it to verify that all ports are protected. Gibson Research Corp. has two excellent (and free) security checks: ShieldsUP! and LeakTest. Run these tests, then follow the listed suggestions to secure your computer.

Disclosure

Dr. Luo reports no financial relationship with any company whose products are mentioned in this article. The opinions expressed by Dr. Luo in this column are his own and do not necessarily reflect those of CURRENT PSYCHIATRY.

REFERENCES (ALL ACCESSED JULY 13, 2004)

1. U. S. Department of Health and Human Services, Centers for Medicare and Medicaid Services. HIPAA administrative simplification - security. http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp
2. Microsoft: Creating stronger passwords. http://www.microsoft.com/security/articles/password.asp
3. SecureMac.com. Open firmware password protection. http://www.securemac.com/openfirmwarepasswordprotection.php