

Technologies

Is Your Personal Digital Assistant Secure?

Harry Karlinsky, MD, MSc, FRCPC

*Clinical Professor and Director, Continuing Medical Education and Professional Development, Department of Psychiatry, University of British Columbia; Faculty Associate, Office for Faculty Development and Educational Support, Faculty of Medicine, University of British Columbia, Vancouver, British Columbia
harryk@telus.net*

Abstract: Protecting confidential patient information on personal digital assistants has become an important risk-management issue. Fortunately, several security-enhancing strategies can now be employed, including the use of passwords, data encryption and virus protection software, identification and frequent backups.

Résumé : Votre assistant numérique est-il sûr?

La nécessité de protéger l'information confidentielle des patients enregistrée sur les assistants numériques est devenue une importante question de gestion des risques. Heureusement, on peut désormais recourir à plusieurs stratégies d'amélioration de la sécurité, y compris l'utilisation de mots de passe, les logiciels de cryptage de données et de protection antivirus, l'identification et des copies de sauvegarde fréquentes.

Key Words: personal digital assistants, security, passwords, encryption, viruses

Recent reviews have highlighted the increasing popularity of personal digital assistants (PDAs) among physicians and other health-care professionals. The rationale seems straightforward. With a wide and increasing range of medical software to choose from—including general medical references, drug databases, downloadable educational content, medical calculators, patient-tracking programs and billing and coding software—PDAs can potentially allow physicians to practise medicine more efficiently and safely (1,2). In this issue, Dr. Warren Steiner (3) describes how PDAs have enhanced point-of-care access to information relevant to the home and community-based care of psychiatric outpatients of the Montreal General Hospital. However, Dr. Steiner's article also highlights a significant concern related to using PDAs in clinical practice: because PDAs can easily be lost, stolen, broken and (or) used fraudulently, the need to protect confidential patient information has emerged as a key risk-management issue. The following overview offers some practical suggestions for managing that risk.

Locking your PDA with a password is the first essential step to enhancing PDA security. The process is as follows: To select a password, first tap on the "security" icon (now preinstalled on virtually all current PDA models). Next, tap on the "assign password" option. After you

enter (that is, key in) a password, you can then select the option to automatically lock the PDA, either on "power off," at a preset time, or after a preset delay. The applications and data within the PDA will subsequently be inaccessible unless the correct password is provided. This password can also be used in a more circumscribed manner to hide sensitive entries in specific programs. For example, after entering a patient's name and appointment time within "date book," tap "details," and then tap the box labelled "private." If you have also selected "hide or mask records" as a "current privacy" option within the security application, this patient's appointment entry (and all entries marked private) will be password-protected.

Unfortunately, the basic security steps referred to above have several limitations. On a mundane—but extremely practical—level, it is cumbersome to constantly enter a text password, particularly if the PDA is frequently turned on and off in the course of a busy clinical day.

Fortunately, third-party applications now exist that address and overcome this concern. One solution is to install software that allows a password to be provided more rapidly. An imaginative example is OneTouchPass (<http://www.onetouchpass.com>), which allows the user to define a password as a point or points on a provided image. When the OneTouchPass-protected PDA is turned on, a picture appears on the screen. To further access applications and data, simply tap the picture at the pre-selected point or points.

Alternatively, some users may prefer to store all sensitive data within a single program—so-called "crypt" or "vault" programs such as Secret! (see <http://linkesoft.com/secret>). Although a password is still required to access sensitive data, crypt programs at least avoid the tiresome input of a password every time the PDA is used.

On a slightly more ominous note, passwords can be guessed—especially simple ones selected by well-intentioned but password-fatigued users. Even more menacing, unauthorized users may have tools to decipher passwords and to read unprotected, sensitive data on stolen or lost PDAs. A potential solution against such fraudulent use is security software that depends upon biometric recognition; that is, behavioural or anatomic

characteristics unique to the user. For example, the software PDALok (see <http://www.pdalok.com>) restricts unauthorized user access unless a live signature from the rightful owner is provided. Although such programs are still in their infancy, it is more than likely that biometric recognition (for example, programs depending upon fingerprint or iris scans) will eventually become a routine security solution.

Data encryption software can also significantly enhance security. In brief, encryption is the conversion of data into a form that cannot be easily understood by unauthorized individuals, while decryption is the process of converting encrypted data back into its original form (4). Encryption–decryption is particularly important in wireless communication; in the United States it is a Health Insurance Portability and Accountability Act (HIPPA) security rule that all data traveling over a public network, which has been interpreted to include a wireless local area network in a health-care setting, be encrypted (5). Fortunately, there are several encryption packages available for PDAs; these can quickly and transparently encrypt new data as it is stored and decrypt it as it is accessed. For example, Dr. Warren Steiner (3) describes the selection of PDA Defense (see <http://www.pdadefense.com/>) as the encryption solution adopted by the Montreal General Hospital’s psychiatric outreach program.

What does one do about virus protection? Although viruses have not yet attacked the broad base of PDA users, a range of antivirus solutions has now been developed. The most sophisticated of these applications reside on the PDA, automatically obtain updated virus definitions with PC synchronization, and protect against every possible entry point—for example, when beaming data and applications through a PDA’s infrared port; downloading files, e-mail or Web pages through a wireless connection; or synchronizing information with a PC. With only a limited number of viruses currently in existence, most experts feel that purchasing an antivirus program (see <http://www.mcafee.com/> or <http://www.kaspersky.com/>) is premature. Nevertheless, as PDAs grow in popularity, malicious viruses will no doubt become more common.

Finally, there are other common-sense ways to protect the data on a PDA:

- Limit access. Although access by administrative support staff may be an allowed exception, in general no one other than the primary user should have access to a PDA that contains patient information.
- Perform a backup frequently. In particular, important patient information stored on a PDA should also be

saved elsewhere, so that the PDA is not the only source of that information. Further, although HotSync synchronizes all data for preinstalled applications, additional installed applications and data files are not necessarily backed up to the desktop computer. Users who want added protection can ensure that data synchronization for these additional applications and data files occurs by installing more sophisticated backup software, such as Backup Buddy (see <http://www.backupbuddy.com/>).

- Ensure that your PDA can be identified. Surprisingly, someone finding a lost PDA may want to return it. To facilitate this, tape a business card to the back of the PDA. A more sophisticated option includes entering one’s name and phone number (and preferably, a “reward if found” notation) under the “owner” tab within the “preferences” icon. If the PDA is also locked, these identifying details will appear whenever the PDA is subsequently turned on. For those who wish to remain more anonymous, tags or strips with confidential code numbers can be purchased and attached to the back of the PDA (for example, <http://www.idstrip.com>). If such a PDA is found, a good Samaritan can call the toll-free number imprinted on the strip. A third-party operator then facilitates return of the PDA.

In closing, it seems inevitable that PDAs and other mobile devices will increasingly become the primary points of clinical communication within health-care environments. The resulting benefits could be considerable. However, implementing and managing effective security for these mobile devices and networks—both by physician users and by information technology specialists—will be crucial to ensuring that their significant benefits outweigh the equally significant security risks and challenges (5).

References

1. Adatia F, Bedard PL. “Palm reading”: 1. Handheld hardware and operating systems. *CMAJ* 2002;167:775–80.
2. Adatia F, Bedard PL. “Palm reading”: 2. Handheld software for physicians. *CMAJ* 2003;168:727–34.
3. Steiner W. Handheld computer use in a psychiatric outreach program. *CPA Bulletin* 2003;35(5):30–32.
4. SearchSecurity.com. Glossary. http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci212062,00.html. Accessed July 20, 2003.
5. Sims B. Deploying secure, reliable wireless LANs in the healthcare environment. *Health Management Technology* 2003;April:24–9.