Personal Digital Assistants: the Healthcare Matter at Hand

Save to myBoK

By Cheryl L. Berthelsen, PhD, RHIA

With everyone from executives to college students using personal digital assistants (PDAs), it was only a matter of time before the devices invaded healthcare. Physicians are embracing PDAs to order prescriptions, make progress notes, and order tests faster and more easily. What's the down side? The data kept on PDAs isn't entirely secure. Here's what you need to know about PDAs and how to prepare your facility for them.

Personal digital assistants (PDAs, also known as hand-held computers) are revolutionizing the way people organize their business and personal lives. These miniature computers provide instant access to important information with just a few taps of a stylus on a pressure-sensitive screen. They fit conveniently in a lab coat pocket or purse or can be attached to the user's belt for quick access. Their popularity is due primarily to ease of use and the large amounts of data and information that can be stored in an easily transportable device.

Doctors and other healthcare providers are joining the ranks of individuals who rely on PDAs, thanks to the hundreds of medical applications available.[1] More than 15 percent of US physicians currently use hand-held computers for reference purposes.[2] Analysts predict that by 2004 the number of clinicians using handhelds for e-prescribing, ordering and checking lab tests, capturing charges, and dictating notes will have reached 20 percent.

Personally-owned PDA use in healthcare is both exciting and disconcerting. As wireless technology becomes the standard for use at the point of care, there are inherent security risks to consider. Most users don't know how unsafe the private data on their handhelds really is. HIM professionals and clinicians need to explore the solutions available to enable secure use of PDAs, as well as how large information systems and networks can be adapted to incorporate PDAs as a primary mode of information interchange.

Information in an Instant

PDAs provide instant access to information for the provision of quality healthcare. Applications with data about prescription drugs, indications and contraindications, side effects, and the average cost of the drug are already available. Other applications allow the physician to check for drug-drug and drug-herb interactions or add data on which drugs are in the hospital's formulary and identify drugs that are not covered by various health plans. Numerous scholarly reference documents are available with information on the latest diagnostic and treatment standards by subspecialty or for general practice.

Beyond references and managing appointments, physicians are drawn to applications that allow them to manage information about their hospitalized patients. With PDAs, physicians can jot progress notes or field emergency calls from the nursing staff without having access to the record. PDA databases can also store results of diagnostic tests and medications for each patient. If another physician is covering calls over the weekend or holiday, the patients' data can be simply "beamed" via infrared light to the covering physician's PDA using the built-in infrared port. Data on the PDA can be synchronized with applications on a personal computer by placing the device in a docking station. Data are exchanged between the handheld and the PC so that both have the same concurrent information.

PDAs can also function as wireless Web browsers. By attaching the PDA to a small modem and an appropriate digital cell phone or by using a PDA that has built-in wireless access, a user just about anywhere in the world can log into hospital, medical library, or private practice computer systems that have Web-based client servers. Data can be downloaded to update information on the PDA and notes can be uploaded to the system. This enables physicians to perform order entry and report authentication and write progress notes without coming near an on-site terminal.

The most popular PDA is currently the Palm Pilot, and 90 percent of existing medical applications for PDAs run on the Palm operating system platform.[3] Palm Pilot dominates the healthcare industry because of active marketing by pharmaceutical companies, which have provided many free Palm Pilots to physicians along with access to free prescription-writing applications and drug and medical knowledge databases in exchange for the right to sponsor advertising and other health-related information on the devices.[4] Physicians have found the devices easy to use, and most have moved beyond storing drug and reference information to managing patient data with their PDAs.

So What's the Problem?

PDAs have great potential for improving the quality of patient care, but there are significant risks involved with using wireless technology. For example, security problems with the Palm Pilot prompted NASA to issue a Palm PDA user security notice because meetings, agendas, notes, address book, and memo pad entries and data marked "private" can be transferred to other Palm PDA units without protection.[5] In May 2000, the Lawrence Livermore National Laboratory banned the Palm VII from the lab as a security threat because it violated the Department of Energy's Technical Surveillance Countermeasures directives by using radio frequencies to transmit data from Web services.[6]

The PDA's size is no aid to security: it's easily stolen or lost. In fact, Denver International Airport estimates it collected 20 to 30 such devices in its lost-and-found bin over the Christmas 2000 weekend.[7] More worrisome, however, are the many PDA owners who believe that the standard password protection installed on the Palm Pilot provides adequate security for the patient data stored in it if lost or stolen. Recent news releases alerted users of the Palm operating system that their PDA is essentially an open book to anyone finding or stealing it. Software code provided within the operating system as a developer's tool allows anyone to bypass the password system and access anything stored on the device by placing it in a "hotsync cradle" attached to a PC and entering the debug mode with a simple graffiti "stroke."[8] (See glossary.) Even a Palm protected by encryption software could be compromised by using the operating system back door to load a software program that records all passwords as they are entered.[9]

Security is further compromised by users storing their passwords and user IDs for computer systems and networks on their PDAs. They may even have auto-dial macros installed to log on to systems via modem and cell phone. These are the "keys to the front door" to all those computer systems for any unwanted user, forming a very real threat to network security.[10] Wireless networks are also easy targets for unauthorized access if not protected appropriately. A recent article in *CIO* described an incident where the writer's wireless local area network (LAN) adapter card accessed a corporate LAN while he was walking through Boston's financial district with an open laptop.[11]

PDAs enjoy no immunity to viruses, either. The very first virus targeted directly at PDAs, Phage, was discovered in September 2000. Phage can spread from one PDA to another if infected files are shared through infrared beaming or installed using a hotsync dock.[12] The proliferation of wireless devices provides the motivation for the development of destructive viruses that could cripple a company depending on a wireless network. Fortunately, many freeware, shareware, and commercial virus protection programs are already available for most types of PDAs.

Current mobile Web browsing devices use Wireless Application Protocol (WAP) to access the Web. WAP uses Wireless Markup Language (WML) to display Web page content and Wireless Transport Layer Security (WTLS) to enable Secure Socket Layer (SSL) capabilities. To access the Web using a WAP device, PDA users need access to a WAP gateway, which is responsible for translating an HTML (hypertext markup language) Web page to WML and then compiling WML into code that is understood and can be displayed on a WAP device. Most Web servers can provide WAP gateway e-mail access by adding a few MIMEs (multipurpose Internet mail extensions). However, WAP poses a security risk because encrypted messages have to be decrypted, translated, and then encrypted to enable WTLS-SSL sessions, but there is no continuous encrypted datastream between the WAP device and the SSL Web server. WAP only provides a secure communication connection between the WAP device and the WAP gateway.[13]

The medico-legal risks associated with physician use of PDAs also need to be considered. If a physician is using the PDA to store data and results on current hospitalized patients, the most recent lab results and changes in patients' conditions won't be available on the PDA. To have current information, the PDA must either be frequently hotsynced with the hospital's computer system, or the physician must access the system frequently throughout the day to manually update the data in the PDA. Drug interaction databases and virus protection software for the PDA must be updated regularly to provide the intended benefits. Give that many physicians have trouble finding the time to sign the required documentation for paper medical records within 30 days of discharge, it's a legitimate worry whether they will be able to find the time to sync their PDAs four or five times a day. Will they sync the drug and medical knowledge databases regularly or will they be satisfied with using last year's download they obtained from a colleague via infrared beam?

A physician is only protected from malpractice liability to the extent that the care provided is in accordance with the standard of practice for his or her specialty and community. Depending on a PDA to provide medical information for patient care is a huge malpractice liability if the physician has outdated information installed on the PDA. Similarly, physicians could make medical decisions based on outdated or incorrect patient information if relying on another physician to beam the information instead of getting it directly from the medical record. Finally, the PDA may become the basis of treatment decisions, but that information may not become part of the patient's hospital medical record.

Start with Education

The first step in addressing the security and privacy risks is education. Physicians who received PDAs as promotions from a drug company and started using patient tracking software may not know how vulnerable the data is. Experts recommend that PDA owners know the location of the device at all times, keep the device out of the hands of individuals they don't know or can't trust, and practice safe beaming and syncing (that is, don't exchange data with an unknown PDA owner). Hospitals and healthcare facilities should provide guidelines about the use of privately owned PDAs in privacy and security education. Further, security and confidentiality agreements should explain the physician's responsibilities regarding privately owned PDAs, including providing adequate security in case of loss or theft, using current medical reference software, providing current virus protection, and practicing safe syncing and beaming.

The next step is for information systems leaders to take an enabling stance toward wireless technology rather than a prohibitive one. PDAs have accomplished something that hospitals have struggled with for years—getting physicians to use computers. Physicians have been slow to adopt computer use in hospital patient care, but have found that PDAs are easy to use and provide fast and reliable reference information. IS departments should capitalize on the growing enthusiasm for the devices and make efforts to safely incorporate their use within their networks as the demand arises. If exchange of data between the patient computer system and a PDA is not feasible in the near future, consider equipping printers with infrared receivers so the physicians can beam the notes they've written on the PDA and print them for the paper medical record.

One Oklahoma hospital system is piloting a project to offer physicians the ability to download patient data to their Palm Pilots.[14] Physicians will be able to place their Palm in a cradle and download a patient list, demographic information, and test results from the previous 24 hours. The main complaint from the voluntary participants is that they need more cradles on more PCs. Eventually, the system plans to offer wireless access and allow the physicians to upload progress notes. This is the type of progressive, innovative planning that must take place to incorporate wireless technology in the large health enterprise setting.

Better Technology to the Rescue

The well-known problems with Palm Pilot security should be resolved in the near future. For the present, solutions include reverting to version Palm OS 3.1 desktop, disabling the serial port on the Palm, or not using the Palm to store any private information until a patch to the operating system back door is available.[15,16,17] For long-term strategic planning, a recent press release from one provider of high-assurance data security systems announced plans to expand its market and product development of its data security product to Palm PDAs.14 The current products aim to provide security for remote dial-in services to hospital information services, including preventing unauthorized network access, protecting against intercept attacks on data transmissions via public telephone lines and encrypting all sensitive information on a PC's hard drive and removable media.[18] The extension of such technology to Palm PDAs means the healthcare industry will have access to a level of wireless security that meets the requirements of the US Department of Defense.

The "WAP gap," that is, the lack of a continuous encrypted datastream between WAP devices and SSL Web servers, will be more difficult to solve. Hospitals can refuse to provide a WAP gateway for wireless access to the patient computer system. However, any available WAP gateway can enable access, which means the WAP gap occurs outside the hospital's control. A better alternative is for hospitals to plan for wireless access and provide a WAP server (that includes the WAP gateway and WML pages) to exist within the hospital network firewall in their strategic IS planning.

Hospitals should welcome the use of medical reference databases on physicians' PDAs, because they can improve quality of patient care. But the hospital should not be the owner and provider of the devices or the data. If the hospital retains ownership of the devices, it will be responsible for every PDA and all data stored on them—and a list maintained by HIM or IS of delinquent physicians that have not brought in their PDAs for scheduled updates would not be far behind. The responsibility and liability of keeping the information stored on the PDA secure and current is best left to the person who has the device in his or her possession and control.

Wireless technology is in its infancy and security experts are just beginning to explore how communications with wireless devices can be made secure. It is a very complex issue and there is no single, simple solution. Smart cards may be able to keep wireless networks secure, by inserting them in the PDA to support encryption and authentication.[19] Biometric authentication is another option in the same way it has been suggested that handguns be adapted so only the recognized owner could fire the gun.

PDAs can enhance the quality of patient care, and they are becoming more prevalent in the hospital environment. The risks to privacy of patient information and the security of an enterprise's entire information network must be addressed. The risks are high but there are remedies. And if HIM professionals and medical staff take measures to reduce the risks, the benefits can far outweigh them. The wise organization will seek flexible, enabling solutions rather than establishing a prohibitive, restrictive environment. If the secret to quality healthcare is getting the physician to personally interact with information systems, then the hand-held computer may be the key to achieving that goal.

New to PDAs? Here's a Glossary

Beaming: Exchanging data and files between PDAs by pointing the built-in infrared ports toward each other and telling the devices to send and/or receive. PDAs can also communicate with any device that has an infrared receiver including a television, VCR, printer with IrDA port, and laptop computer.

Cradle: A PDA accessory that hooks to any PC's USB/serial port and with the appropriate software installed on the PC allows data transfer between the PDA and the PC. The cradle usually includes a battery charger so the PDA can be recharged while in the cradle. The cradle also serves as the conduit to download PDA software from the internet directly to the PDA.

Graffiti: A form of shorthand used to enter data into a PDA comprised of simple stylus strokes on pressure-sensitive screen.

HotSync or Syncing: The processing of exchanging data and information between a PDA and a PC using the cradle. "Syncing" uploads new data on the PDA to the PC and downloads new data on the PC to the PDA so the data files are synchronized.

Notes

1. Morrison, K. Meg. "The Handheld Computer Medical Software Craze." *MD Net Guide* 3, no. 5 (2001): 21-27.

2. Stammer, Lisa. "A Show of Handhelds." *Healthcare Informatics* 18, no. 4 (2001): 37-44.

3. "The Handheld Computer Medical Software Craze."

4. Edwards, John. "Mobile Medicine Starts Slow." *Mbusiness*, January (2001): 81-86.

5. NASA, Information Technology & Communications Division. Palm PDA User Security Notice (2001). Available at www.hq.nasa.gov/office/codec/codeci/help/hardware/ palm.htm#security.

6. Anderson, Brian. "Palm VII Banned From Lab as Security Threat." *Valley Times* (April 20, 2000). Available at www.infowar.com/class_3/00/class3_050100a_j.shtml.

7. Worthen, Ben. "Time To Get Nervous." *CIO* 14, no. 11 (2001): 102-112.

8. Delio, Michelle. “Threat in the Hand of Your Palm.” *Wired News* (March 5, 2001). Available at www.wired.com.

9. Lemos, Robert. “Passwords Don’t Protect Palm Data, Security Firm Warns.” CNET News.com (March 2, 2001). Available from yahoofin.cnet.com/news/0-1006-201-5005917-0.html.

10. White, Aoife. “Palm PDA Threat to Network Security.” Network News (March 15, 2001). Available at www.vnunet.com/News/1119214.

11. “Time To Get Nervous.”

12. Delio, Michelle. “Palm Virus Hits, But Don’t Worry.” *Wired News* (September 22, 2000). Available at www.wired.com.

13. “Wireless Application Protocol White Paper: Wireless Internet Today.” *WAP Forum* (June 2000). Available at www.wapforum.com.

14. Chin, Tyler. “Lending Doctors a Hand(held).” *American Medical News* 43, no. 34 (2000).

15. “Threat in the Palm of Your Hand.”

16. “Passwords Don’t Protect Palm Data, Security Firm Warns.”

17. “Palm PDA Threat to Network Security.”

18. “Kasten Chase To Deliver RASP Data Security

For Palm Handheld Devices.” Kasten Chase Applied Research Limited (May 17, 2001). Press release. Available at www.kastenchase.com.

19. Crouch, Cameron. “Experts Ponder Securing the Wireless World.” *PC World.com* (April 11, 2001). Available at http://www.pcworld.com/news/article/0,aid,47063,00.asp.

References

Freudenthal, Margus, Sven Heiberg, and Jan Willemson. “Personal Security Environment on Palm PDA.” Presented at the Annual Computer Security Applications Conference, New Orleans, LA, December 2000. Available at http://citeseer.nj.nec.com/freudenthal00personal.html.

Halonen, Teppo. “Authentication and Authorization in Mobile Environment.” (2000). Available from http://citeseer.nj.nec.com/400921.html.

Kalaja, Salla. “Security in Mobile Health Care Work.” TIK-110.501: Seminar on Network Security, 2000. Available at www.hut.fi/~skalaja/netsec.pdf

Cheryl Berthelsen *is associate professor of HIM at University of Mississippi Medical Center. She serves on the Medical Center’s Implementation and Compliance Subcommittees for HIPAA Privacy and Security and Focus Group for Development of Five-Year Strategic Plan for Information Technology.*

Article citation:
Berthelsen, Cheryl L. "Personal Digital Assistants: the Healthcare Matter at Hand." *Journal of AHIMA* 72, no.9 (2001): 40-48.