Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing PDAs in the Health Care Environment

Ultimately, the privacy and security of patient medical information is in the hands of each person who touches it. Every staff member should understand the importance of patients' privacy and take ownership of maintaining that privacy. Every person who works in the medical field, whether they be physicians, nurses, technicians, or IT support staff, must understand the HIPAA regulations and the significance of complying with them. For users of handheld computers storing patient data, it's imperative that they have an un...

Copyright SANS Institute
Author Retains Full Rights

AD

Securing PDAs in the Health Care Environment

Sarah H. Blanton
September 2001

The "Information Age" is upon us, and technology is the two-edged sword that both provides us access to a world full of data and bombards us with too much information. The medical field is no exception; information drives the practice of medicine (Tonks and Smith).[1] Doctors and nurses spend a quarter of their time searching for, sorting, and using information. Hospitals spend 15% of their budgets on information management. Health care professionals need information every time they encounter a patient, and that information must be accurate, up-to-date, and easily obtained. Fortunately, the development of technology in the last few decades has provided powerful tools to store and sort the plethora of medical data that is available. With the introduction of handheld computers, health care professionals now have a tool that they can carry with them to the bedside, the surgery, and the classroom. The portability of Personal Digital Assistants (PDAs) makes them ideal for this task, and with the ability to download data from servers, either via a wireless network or physical synchronization, handheld computers can provide instant access to accurate data about patients, drugs, and diagnostic or treatment information. They can even be used to upload patient information to the servers to be stored in the patient's electronic medical record. If managed correctly, they can become an indispensable tool for the medical professional.

There are already a number of extremely useful applications created for PDAs. Increasing numbers of health care providers are using applications such as ePocrates[2], a database of drug information including indications, dosage, administration, adverse reactions, and drug interactions. PatientKeeper[3] is an electronic medical record application used in direct patient care settings. The ePhysician Practice Suite[4] includes patient charge capturing, electronic prescriptions (they claim to have surpassed 1 million electronic prescriptions), drug reference, and patient management software. Tools such as these can allow the physician to have the patient's complete medical record as well as drug reference information in a searchable, sortable format. Ideally the physician would be able to update the patient's record, prescribe medications electronically while crosschecking for drug interactions or new physician alerts and transmit all the data electronically to a central database or transmit appropriate data to another physician, eliminating problems such as illegible handwriting and the cost of medical transcriptions.

Several leading medical institutions have endorsed the use of PDAs. Wake Forest Medical School issues Palm Pilots to its second-, third-, and fourth-year medical students.[5] "The Palm Computing® platform has the potential to revolutionize the way our medical center departments run and communicate," said Dr. Johannes Boehme II, associate dean for academic computing. "We see an unlimited potential with this platform that could lead to the development of customized departmental applications and the eventual deployment of several thousand WorkPads."[6] Wake Forest is using the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

IBM Thinkpads linked to a central synchronization server to deliver medical and reference information to the students. The students can download additional medical reference information on demand as they proceed in their studies.

Another institution supporting PDA use in medicine is Cedars-Sinai Medical Center[7]. They are using the wireless network-enabled Palm VII in the clinical setting to deliver patient data and lab reports instantaneously. They've designed, in-house, an Intranet and Oracle database that delivers physician look-up, paging, email, and wireless order processing for books and articles from the medical library [8].

The web site www.pdaMD.com is a very useful site in that is contains software review as well as case study articles about handheld computer use in the clinical setting. In particular, the article "A Day in the Life of an FP's PDA"[9] is a fun read and describes several scenarios in which a PDA can facilitate the physician's handling of information, leaving more time for direct patient care. Handheldmed.com is also a valuable reference site for users of PDAs in the medical field. They offer articles and reviews as well as purchase of handheld products and software for the physician.

Doctors are not the only medical professionals who can benefit from the use of the handheld computer. Karen Lusky, MSN, RN, in her article entitled "Is a Personal Digital Assistant in your Future?" [10] says, "This future is already in the hands, literally, of nurses who are beginning to use handheld computers called personal digital assistants (PDAs) in a way that may revolutionize healthcare delivery." The journal of mobile nursing informatics (www.rnpalm.com) provides articles, reviews, software, discussion lists, and an electronic newsletter geared toward the nursing field. Clearly the convenience of using a PDA to have instant access to medical references and patient information has the potential to impact all aspects of health care.

Many institutions allow the use of handheld computers but are not prepared to manage the security risks inherent in their use. While the PDA can be a valuable tool for the medical professional, it introduces risks as well. Being a physically mobile device, it can be lost, stolen, or damaged relatively easily. And while to date there are have not been many viruses or other hacks created that affect PDAs, security experts warn of an increase in hacking against handheld computers as PDAs make their way out of the home and into the workplace.

In the medical field, the security and privacy of electronic patient data are not only important, they are federally mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[11] that sets federal standards for privacy and security of patient-identifiable information. The privacy standards were finalized in December 2000 and are intended to give patients greater access to their own medical records and more control over how their medical information is used[12]. The security standards are still being debated, but when finalized, will set standards for security of patient medical information. The security standards will include requirements for encryption, audit trails,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

and disaster recovery of any patient-identifiable data in any format that has ever been stored or transmitted electronically. This includes electronic medical records, fax transmissions, and email whether stored in a data warehouse or on a handheld computer. The American Academy of Family Physicians published an article in March 2001 entitled "What You Need to Know About HIPAA Now"[13] by David C. Kibbe, MD, MBA that extols physicians to begin learning all they can about HIPAA now, because every practice in the United States will have to comply with the privacy regulations by February 2003 and will face severe civil and criminal penalties for non-compliance. After the security regulations are published, medical institutions and practices will have about 26 months to comply with them. This may sound like a lot of time, but the HIPAA regulations are going to require huge changes in how medical information is handled, and will ultimately encourage the computerization of all personal health information.

PDAs introduce some interesting vulnerabilities to the threats against the confidentiality, integrity, and availability of patient medical information. Lost or stolen handhelds put the confidentiality and availability of patient data at risk; damaged PDAs make the information unavailable at the least, and unrecoverable at the worst. In addition, many PDAs have the capability to use infrared to beam information to another handheld device or desktop computer. This opens up the possibility of accidentally beaming information to the wrong user, again threatening the confidentiality of the data. The infrared beaming could also become a conduit for the spread of viruses or other malicious code.

To comply with HIPAA regulations, the data stored on PDAs will have to be protected. The transmission of the data must be protected as well, whether it's sent via a physical connection or a wireless network. If the PDA syncs with a desktop computer or server, the data must be safeguarded there as well. And there must be some assurance that the data will not be put at risk if the PDA is taken out of the clinic or hospital. By the same token, to be useful, the PDA should be able to accompany the physician into other settings outside the institution so that valuable reference information can be accessed from home or other locations, particularly for the physician on call. In general, physicians who are called off-hours for patient consults don't have the patient's medical information at hand, as it is impractical as well as inadvisable to take traditional paper records out of the institution. A physician who is able to access a patient's medical history and drug information at any moment would be in a better position to address issues that arise when the doctor is on call. It is critical that the PDA have security measures in place such as password protection and encryption of critical databases.

Fortunately, sophisticated authentication and encryption programs are beginning to appear for handhelds, and there are already many third-party programs available for protecting the PDA by requiring authentication. For example, TealLock[14] for the PalmOS allows the user to lock the PDA and encrypt selected databases. PDA Defense Professional[15] is a multi-layered security application for the PalmOS. It provides 128-bit Blowfish encryption, limited number of login attempts after which it deletes all data

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

from the PDA, and other customizable options. At this time there are no encryption standards in place for PDAs. This needs to be addressed by the appropriate standards authorities, but in the meantime it is advisable to use at least 128-bit encryption.

Few users realize that there are several "back doors" to accessing handheld data. On the PalmOS, it is possible to put the PDA into a debug or console mode[16] making it possible to retrieve and modify any installed database, delete applications, and even retrieve the system password in an encrypted form. In a Wired News article[17], Chris Wysopal, director of research and development for @Stake says "that an attacker would be able to copy the contents of the average Palm 'in about five minutes,' and a password could be decrypted in a few seconds." Palm Computing claims that PalmOS version 4.0, which ships with the m500 series PDAs, has fixed this problem. However, many users have an older version of the operating system that does not include fixes. In these cases, there are at least two fixes available. One is called Shortfix, created by Daniel Seifert[18], that removes the shortcuts that put the unit into these debug modes. There is another free application called "Nodebug"[19] by Alejandro David Weil that removes at least one of the shortcuts into the debug state.

While handheld computer malware has so far been scarce, there has been at least one instance of a Trojan designed to target the PalmOS. Palm_Liberty.A[20] appeared in August 2000 and masquerades as a file that can convert a shareware game program called Liberty into a registered copy, but instead it deletes all executable applications on the handheld. It was considered proof of concept code and its spread was limited, but it's likely we'll see more malicious software aimed at handhelds in the future.

There are quite a number of companies now marketing antivirus software for handhelds. Trend Micro has a product called "PC-Cillin for Wireless"[21] that provides real-time scanning to prevent viruses from propagating by beaming, syncing, email, or internet downloads. The software runs resident on the device and is supported on PalmOS, WinCE, and Psion devices. They provide a free download of their software. Symantec also has a PDA antivirus product called "Symantec Antivirus 2001 for Palm OS"[22]. It runs on the Palm and automatically updates its virus definition files upon hotsyncs. One year of application and virus definition updates is included with the initial $39.95 purchase price. An Internet search should turn up numerous options for the various handheld models.

Clearly, tools are becoming available to make handheld data less vulnerable to loss or unauthorized exposure or modification. The security tools will mature with time, but the need is there to have better security measures in place now. Users must be made aware of the risks as well as the benefits of using handheld computers. Policies must be implemented that require adequate security measures be put in place for PDAs, and appropriate procedures must be created and followed. Suggestions for PDA Policies include:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Require a password protection program, preferably one that allows only a limited number of login attempts
- Require that patient data be encrypted while on the handheld, on the network, or in a central database.
- Require that the encryption be at least 128-bit.
- Install the applications that remove the shortcuts into the debug modes of the PDA
- Require antivirus software to be in place

As in many other settings, the biggest hurdle to achieving "secure" data is user education. Making PDA education a part of new employee orientation (for positions that will involve use of a PDA) is a good start, but wise PDA use must become a part of the culture of the organization if it is to be successful. Users should be educated about the risks of carrying a PDA that contains sensitive data. They should be advised that:

- The loss or corruption of data could impact their patients and exposure of the data to inappropriate entities could carry civil and criminal penalties under the HIPAA guidelines
- The PDA should not be shared with others.
- They should use care with regard to the infrared beaming. It would be advisable to turn off the beam-receive option and enable it only when one is intentionally receiving data from another user. Even then, they should be wary of what data is being sent to them and guard against the possibility of receiving malicious code.
- Users should safeguard the PDA against theft or loss as they would their own credit cards or car keys.
- They should use care in downloading and installing non-approved applications from the web to avoid the possibility of accidentally installing malicious software

Ultimately, the privacy and security of patient medical information is in the hands of each person who touches it. Every staff member should understand the importance of patients' privacy and take ownership of maintaining that privacy. Every person who works in the medical field, whether they be physicians, nurses, technicians, or IT support staff, must understand the HIPAA regulations and the significance of complying with them. For users of handheld computers storing patient data, it's imperative that they have an understanding of the risks involved and the steps they can take to protect the sensitive data they carry in the palms of their hands.

---

[1] http://bmj.com/cgi/content/full/313/7055/438 British Medical Journal Editorials: Information in Practice, August 1996, Alison Tonks and Richard Smith
[2] http://www.epocrates.com/ ePocrates Home Page
[3] http://www.patientkeeper.com/ Patientkeeper Home Page
[4] http://www.ephysician.com/ Ephysician Home Page

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[5] http://www.wfubmc.edu/academic_computing/ACAbout.htm Wake Forest Medical School Office of Academic Computing web page
[6] http://www.pdamd.com/vertical/tutorials/wake_forest.xml pdaMD case study article "Wake Forest Medical Center using Palm OS PDAs to Train Tomorrow's Doctors"
[7] http://www.csmc.edu/ Cedars-Sinai Health System Home Page
[8] http://www.pdamd.com/vertical/tutorials/cedars.xml pdaMD case study article "Cedars-Sinai Uses Palm VIIs To Access Clinical Information"
[9] http://www.pdamd.com/vertical/features/ADayLife.xml pdaMD feature article "A Day in the Life of an FP's PDA" by the PDA of K. Meg Morrison, MD
[10] http://www.nurses.com/content/news/article.asp?DocID={D729D42D-BF95-11D4-8C7F-009027DE0829}&Bucket=&Featured=True&VNETCOOKIE=NO "Is a Personal Digital Assistant in your Future?" by Karen Lusky, MSN, RN November 2000
[11] http://www.hcfa.gov/medicaid/hipaa/ HCFA (Health Care Financing Administration) HIPAA web page
[12] http://www.hcfa.gov/medicaid/hipaa/adminsim/privacy.htm HCFA HIPAA Privacy Standards web page
[13] http://www.aafp.org/fpm/20010300/43what.html "What You Need to Know About HIPAA Now" by David C. Kibbe, MD, MBA, American Academy of Family Physicians March 2001
[14] http://www.tealpoint.com/softlock.htm Teal Software's Teallock web page
[15] http://www.pdadefense.com/ PDA Defense Home Page
[16] http://www.atstake.com/research/advisories/2001/a030101-1.txt @Stake Security Advisory "Palm OS Password Lockout Bypass" by Kingpin (kingping@atstake.com)
[17] http://www.wired.com/news/technology/0,1282,42198,00.html Wired news article "Threat in the Hand of Your Palm" by Michelle Delio
[18] http://www.dseifert.com/shortfix/ Shortfix web page by Daniel Seifert
[19] http://freewarepalm.net/utilities/nodebug.shtml Nodebug page
[20] http://news.cnet.com/news/0-1006-200-2635223.html CNET News article "Trojan Horse Rears Its Head on Palms" by Stephanie Miles, August 28, 2000
[21] http://www.antivirus.com/free_tools/wireless/ Trend Micro PC-Cillin web page
[22] http://www.symantec.com/sav/ Symantec Palm OS antivirus web site

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**