Pervasive Health Care Applications Face Tough Security Challenges

Vince Stanford

National health expenditures this year are estimated at about US$1.5 trillion, or almost 15 percent of GDP, by the Centers for Medicare and Medicaid Services (www.cms.gov). This comprises the largest service sector in the US economy. Moreover, cost increases are outpacing general inflation, so the health care industry is again under pressure to become more efficient. These pressures—coupled with ready availability of personal digital assistants, wireless connectivity, mobility management middleware, and numerous medical applications—are driving very rapid deployment of pervasive computing solutions in health care. But as this article will show, these deployments must meet increasingly stringent privacy and security requirements that will be enforced in the coming year and beyond.

BALANCING USABILITY AND PRIVACY

Personal digital assistants are cheap and effective, and run a wide variety of applications. Many people simply bring their own PDAs to work. Physicians and nurses faced with continuing demands for increasingly efficient health care delivery also use them. According to recent reports such as "The Rise of Palmtop Technology in Medicine" by John Cochrane (*E-Healthcare-Connections*, www.e-healthcare-connections.com), and "Personal Digital Assistants: The Healthcare Matter at Hand," by Cheryl Berthelsen (*J. American Health Information Management Assoc.*, Oct. 2001; www.ahima.org/journal/main.html), from 15 to 20 percent of medical practitioners now use palmtops, and a vibrant specialty software sector has emerged, making hundreds of palmtop medical applications available.

But organizations apply the principle of benign neglect to PDAs containing individual medical records at their peril. Deployments of pervasive solutions in medicine come with legal and ethical complications, and inappropriate disclosure of medical records data involves real and substantial liabilities—liabilities that are about to get even more severe.

Specifically, the Health Insurance Portability Accountability Act (HIPAA) of 1996 dramatically changes the legal environment for medical records processing, defining felony offenses and penalties for disclosing individually identifiable medical records. Starting first with fines, the penalties then grow from a year in prison for simple violations, to five years for obtaining the information under false pretenses, to 10 years for selling the data. There is nothing like the threat of going to prison to concentrate the mind, so health care IT executives are now concentrating on bringing their systems into compliance as deadlines phase in. The administrative and standardization titles take force this October and the privacy title in April 2003, with security title dates yet to be established. Once they're set, changing these dates requires an act of Congress. (See the "Proposed Changes to HIPAA" sidebar.)

DEVELOPING SECURITY GUIDELINES

Currently, large health care enterprises are carefully considering how to comply with HIPAA's privacy and security titles. With the privacy title becoming effective next April, organizations developing pervasive systems must design them to comply now because all medical information systems are covered—not just the new ones.

Brent Lowensohn, Director of Kaiser Permanente IT Advanced Technologies, is developing his organization's guidelines for privacy and security in pervasive health care systems. His guidelines embody four basic principles:

- Active security administration
- Best network security practices
- Data security for palmtops if lost or stolen
- Strong user authentication

To Lowensohn, security is paramount and must be designed into pervasive systems from the outset. Because new exploits and security holes are constantly coming to light, security in pervasive wireless environments cannot be solved statically, but must be engaged on an ongoing basis. All pervasive projects should have a security administra-

1536-1268/02/$17.00 © 2002 IEEE

tor who remains current with the Computer Emergency Response Team (CERT) advisories, as well as developments at other security organizations.

A security administrator can handle multiple systems, so a full-time employee is not required for each project. But the projects must follow recommended security updates as new threats evolve. CERT, formed by the US Defense Advanced Research Projects Agency in response to an increasingly populous and dangerous Internet, maintains a presence at www.cert.org and publishes an ongoing series of security advisories that is available to security administrators. Computer security organizations, such as the Internet Security Alliance (www.isalliance.org) and System Administration Networking and Security Institute (www.sans.org), should also be monitored.

Moreover, Lowensohn continued, pervasive health information systems have security risks beyond conventional networks because they use highly portable devices that can be lost or stolen. System designers must defend against physical security compromises of the devices, whether accidental or deliberate. For this, they can use session timeouts, employing biometrics such as fingerprint readers and requiring pass phrase entry when sessions are initiated. Palmtop operating systems and applications must also be engineered and configured to resist tampering. For example, recent versions of Palm OS contain a security application that prevents unauthorized hot syncs. (The hot sync is the process of synchronizing and updating information captured using the palmtop, or downloading updates from the desktop database to the palmtop. This is usually done by placing the palmtop in its cradle and activating the hot sync software component. Early palmtop systems had little or no authentication capability during the hot sync process, under the assumption that the user would maintain physical control of the palmtop. By contrast, in pervasive environments this can be done using wireless connections, so authentication and encryption are becoming crucial capabilities.)

As PDAs are deployed in large numbers, inevitably some will be mislaid or stolen. Individually identifiable medical records data must be protected when that happens. Many commercial products are coming online for protecting vital data on lost or stolen pervasive devices, including Asynchrony's PDA Bomb, TealPoint's TealLock, Trust Digital's PDA Secure, and Chapura's Cloak, to name only a few. These variously support multiple password levels, administration and enforcement of security policies, data and application encryption, as well as destruction of data on tampering.

A LAYERED APPROACH TO SECURITY

Rich Grosser, an in-house consultant specialist at Kaiser Permanente, points out that a thief can easily steal a car with its doors open and engine running, but the solution is not to ban cars. Instead, we use simple layered security procedures, locking the ignition, steering wheel, and doors to present series of problems to thieves. Likewise, Grosser described a layered approach to securing pervasive networks.

A recent network security study he helped conduct showed that up to 80 percent of wireless access points are simply turned on with minimum setup. The service set identifier (SSID), which lets other 802.11 stations join its group, thus might be left as the access point manufacturer's name—or even "default." Others, perhaps outside your building, could access your wireless network, apply cracking tools to gain further access, decrypt message packets, and possibly gain access to your wired infrastructure through a gateway.

Grosser recommends a layered access control strategy, starting at the most rudimentary level with the SSID, then creating additional authentication and encryption layers, each raising its own barrier to intrusion. Most access points broadcast their SSID by default, but you can change this arrangement so that stations must know the SSID in advance to initiate communication. This step adds a level of shared secret authentication, although not enough by itself to secure a system.

Next, during dynamic allocation of Internet protocol addresses during the device discovery process, the DHCP server can authenticate the media access control (MAC) hardware addresses of stations seeking access to

PROPOSED CHANGES TO HIPAA

At press time, Health and Human Services Secretary Tommy Thompson proposed changes to the HHS regulatory standards for privacy of individually identifiable health information. The HHS Office of Civil Rights was charged with formulating specific regulations that embody the privacy sections of HIPAA legislation.

Thomson said that: "… the changes we are proposing today will allow us to deliver strong protections for personal medical information while improving access to care." He also said that the changes are designed to avoid requiring written consent forms by patients who need prescriptions, or individual forms for every consulting physician on a health care team.

The proposed changes also tighten the restrictions on the use of medical records data for marketing purposes, clarify that minors need not provide written consent for parents or guardians to access their records, and streamline forms processing for patients who elect to participate in research. The effects of the proposed changes will become clearer as public review and comment continues, but strong privacy requirements are likely to remain in force.

WIRELESS SECURITY

Additional security issues arise because almost all complex pervasive systems use wireless networking in some form, often IEEE 802.11, and by nature must support dynamic device and service discovery. They are thus open to several types of attack specific to wireless connectivity and pervasive networking environments, many focusing on the session ciphers used to encrypt the channels at the hardware level.

Public key encryption algorithms such as RSA, Diffie-Hellman, and Elliptical Curve use keys with upwards of 1,024 bits, ensuring that they will remain hard to crack but also making them computationally expensive. They are better used for secure exchange of shared secret keys for more economical ciphers. Unfortunately, these also present easier targets.

The Wireless Equivalent Privacy protocol of the 802.11 standard uses an RC-4 stream cipher. There are many documented attacks on the WEP protocol, and cracking tools have even been published as open source that show how to do it most effectively. Early attacks were based on the 40-bit key first used for WEP, so newer versions of 802.11 hardware support 128-bit keys. But even this improvement is not enough, because the initialization vector (IV) transmitted with the cipher blocks repeats every few hours on busy access points. Because blocks in the same session with the same IV can yield the exclusive-or of the plain texts, they are still vulnerable to statistical attack. Defeating this attack requires frequent changes of session key, effectively establishing a new session before the IV and cipher streams repeat together.

The Lightweight Extensible Authentication Protocol provides dynamic WEP initialization and manages the session keys to enhance the integrity of the 802.11 channel encryption. Additional in-channel encryption will provide greater security for critical data. Also, there are working groups in the IEEE that are actively developing next generation security protocols, such as the Technical Committee on Security and Privacy (www.ieee-security.org).

your network against a list of devices belonging to legitimate system users. While MAC addresses can be spoofed, this precaution still adds another barrier to unauthorized access. Once the server has authenticated the MAC address, the Wireless Equivalent Privacy protocol is invoked and a session key exchanged, establishing an encrypted session using the RC-4 stream cipher.

As a final line of defense, some middleware infrastructure systems for mobile workers provide additional in-channel encryption, such as the secure sockets layer (SSL), for virtual private networks within the wireless channel. This technique adds an additional level of security. Mobility middleware can also provide authentication and access privilege levels for specific users in the organization and user-device administration capabilities. Some middleware systems run secure client-to-server sessions through the SSL with 128-bit encryption using a variety of ciphers or the newer Transport Layer Security protocol.

Grosser believes that pervasive systems are only truly secure when they are locked up, disconnected, and powered down. Everything else entails risk management. However, he thinks we can manage security risks in pervasive systems, but must stay on top of them—new attacks emerge that must be tracked and thwarted with countermeasures. While systems will never be 100 percent secure, precautions as simple as reading the manuals and following their security recommendations when setting up the wireless infrastructure can help.

Jeff Sutherland, who is developing a mobile patient record and charge capture infrastructure as PatientKeeper Corporation's CTO, detailed a layered security hierarchy. Because he works with customer organizations, his approach to security involves a thorough review and discussion, proceeding through the following steps:

- Verifying physical security of the server infrastructure (making sure the data center doors are routinely locked)
- Conducting password audits to assure that all default passwords have been changed
- Auditing the system software against the CERT advisories, making sure that libraries are up to date
- Verifying administration of database management systems or other server software, closing any default accounts
- Recommending regular monitoring of system logs
- Verifying that no unauthorized software has been installed from outside
- Closing primitive services such as telnet and FTP
- Auditing server security from the outside using port scans
- Encrypting private data while it is actually on the pervasive devices
- Encrypting backups before they leave the medical servers for off-site storage

Sutherland also pointed out that PDA infrared ports must be managed carefully. For example, when physicians want to exchange data about a patient, only tokens are directly exchanged by beaming. The receiving physician must then establish an authenticated connection with the secure middleware and download the actual patient record data for herself.

An industry group including IBM and others (described at the Tivoli Web site in the "Pervasive Computing in Medicine" sidebar) is defining HIPAA security requirements and responses that can be made using existing software architectures. The requirements include contingency planning, personnel security, software security configuration management, access control,

communications and network controls, electronic signatures, and privacy rules. See the "Wireless Security" sidebar for pointers to a matrix of HIPAA requirements versus software features you can use to comply with these requirements.

PERVASIVE HEALTH CARE APPLICATIONS

There is an increasing range of pervasive health care applications available for palmtop PDAs (see the "Pervasive Computing in Medicine" sidebar). Some applications are either freeware or have downloadable demo versions, so interested readers can evaluate them for themselves. Figures 1 and 2 show several screenshots that illustrate the functions palmtop patient record systems provide.

Space does not permit a comprehensive review, but I've listed some of the major categories in the bullets below. For purposes of HIPAA requirements, we can classify palmtop applications into those that contain individually identifiable patient record, patient tracking, and charge capture applications; and those that do not, such as reference manuals and technical computing aids.

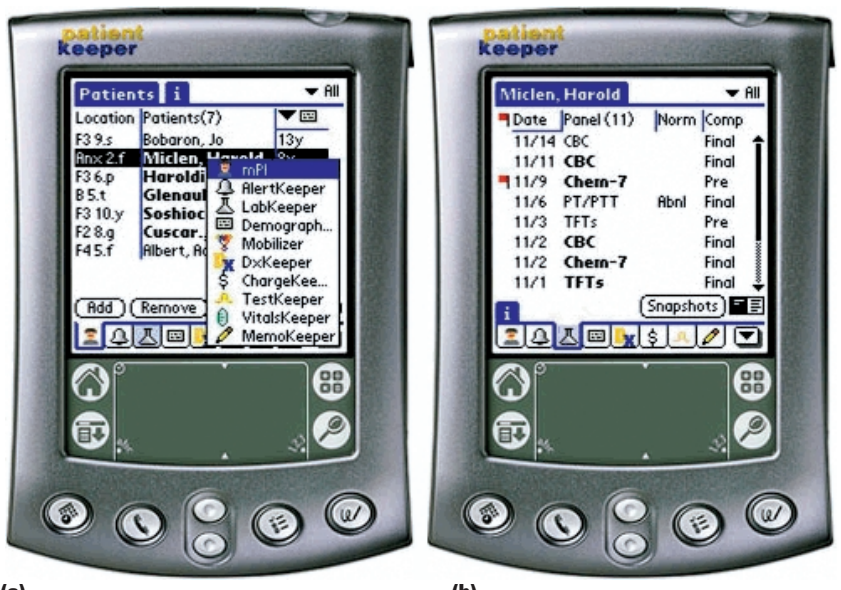
Patient record systems might typically include

- *Patient record tracking*: Tracking their vital data over time such as blood pressure, diet, weight, and medications taken.
- *Patient record suites*: Applications for downloading patient records into palmtop devices, collecting updates during patient consultations, and uploading to enterprise medical servers for disposition and retention. Figure 2a shows the lab results for blood chemistry tests from a hypothetical patient.
- *Billing and coding*: Palmtop reference data for identification and capture of disease diagnosis by International Classification of Diseases (ICD-9), and coding of treatment

PERVASIVE COMPUTING IN MEDICINE

Hundreds of medical applications for palmtops are already available and in wide use, and an extensive Web community is making them accessible. Applications include integrated patient record tracking, physician's references for drug formularies, pharmacy, diagnostic criteria for diverse clinical consultations, practice management, charge capture, billing, positive patient identification, and others too numerous to catalog here. Representative resource sites, chosen for numerous links to the burgeoning pervasive medical field, include

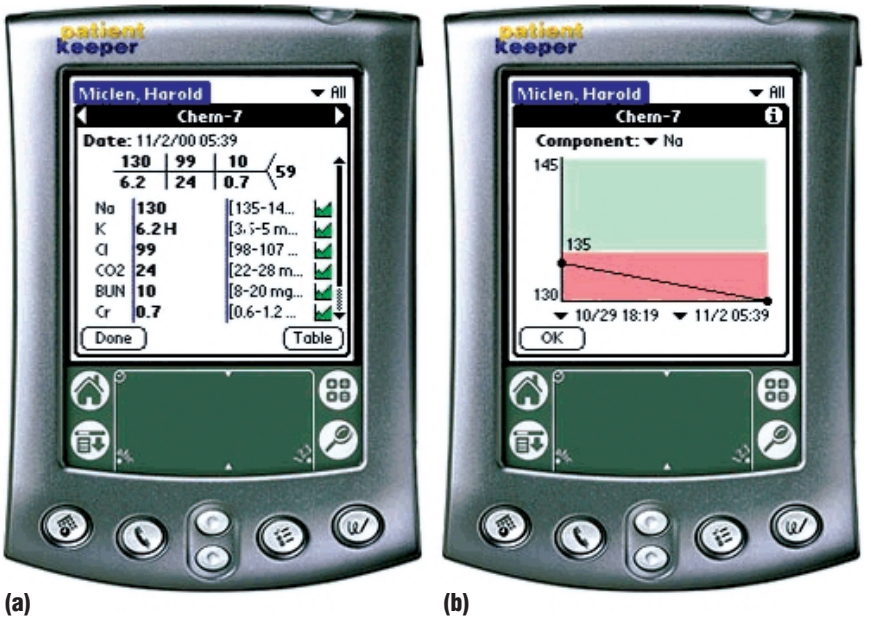
- *www.amia.org*: The American Medical Informatics Association is an organization of about 3,000 medical professionals, with special interest groups in mobile computing, natural language interfaces, and telemedicine.
- *www.handheldmed.com*: Commercial site with a software store with many titles and an extensive listing of articles focused by practice areas such as cardiology, emergency medicine, nursing, obstetrics, pharmacy, and radiology.
- *www.palminformatics.com*: Commercial site that distributes a patient tracking system with an excellent link page with software categories, hardware, and links to other resources such as associations.
- *www.pdacortex.com*: An online journal of mobile informatics covering a range of topics including palmtop computing in medicine, middleware, clinical trials informatics, hardware, and legal aspects of pervasive computing in medicine.
- *www.pdaMD.com*: A topical Web site with a variety of current articles on palmtops and a medical application directory with many programs, some downloadable and some commercial.
- *www.tivoli.com/products/solutions/security/healthcare*: This site has a detailed analysis of HIPAA security and privacy requirements and a software architecture that can be used to meet them.



(a) (b)

Figure 1. Palmtop displays showing a patient list downloaded onto the palmtop for office visits or rounds: (a) the system function menu and (b) laboratory results display screen.

APPLICATIONS



(a) (b)

Figure 2. Palmtop display of (a) patient blood chemistry electrolytes laboratory group and (b) a trend plot for the calcium (Na) level over time.

under the Current Procedural Terminology (CPT) coding standards.

Reference and technical applications and pervasive tracking systems include

- *Clinical applications and calculators:* Reference materials and specialized technical calculations for diagnosis and case management in emergency medicine, cardiology, pediatrics, and other specialties.
- *Medical references*: Physician's drug references and norms for pediatric development, nutrition, electrolytes, and many more.
- *Physician order entry and verification*: Systems that use barcode readers to track and verify the administration of medications and recording of orders for lab procedures.
- *Durable medical equipment*: Many medical centers now use smart tags on valuable mobile medical equipment, such as wheelchairs and cardiogram carts, that must be utilized efficiently but are attractive targets for theft. The smart tags help hospital staff find the equipment quickly and alert security staff when it is being taken off the premises.

Behind the palmtop systems, a privacy and security middleware layer must protect individually identifiable medical records, allowing secure access by highly portable pervasive systems with wireless links to the servers. The access management and security infrastructure must provide continuous coverage for medical records data in transit to the PDA and while it resides on the PDAs. Access must be managed and authenticated at the device, data, and user levels.

The explosive growth of pervasive computing in medicine has begun to produce many useful applications, systems, and tools. The legal environment in which these tools must operate is rapidly evolving, so procedures must be developed to effectively comply with the law and regulations now in preparation. As in the PC's early days, many isolated tools are emerging that have great potential. But these need additional integration, security, and standards work, especially to protect confidential medical records data, to realize their full potential while protecting the organizations and end users that employ them. P

Vince Stanford is the lead engineer for the NIST Smart Space Laboratory, project manager for the NIST Smart Space project, and a founding member of *IEEE Pervasive Computing* magazine. Contact him at vince-stanford@users.sourceforge.net.

next issue

Pervasive Computing Comes to Work

As pervasive computers assume varied and portable forms including PDAs, tablets, and ultra portables, we will carry them at all times and integrate them into our daily work. Thus, we are going to have to stay connected to the enterprise as we move through its work spaces. Dynamic connectivity, including device and service discovery, and equally agile information access middleware will be the sine qua non of enterprise pervasive computing. In the next installment, I will talk to technologists at AvantGo, IBM, Sun Microsystems, and others about the tools they are developing for pervasive enterprise computing.