Secure Remote Access to a Clinical Data Repository
Using a Wireless Personal Digital Assistant (PDA)
Raymond G. Duncan, MD, FAAP and M. Michael Shabot, MD, FACS, FCCM, FACMI
Cedars-Sinai Medical Center and UCLA School of Medicine, Los Angeles, California

Abstract
TCP/IP and World-Wide-Web (WWW) technology have become the universal standards for networking and delivery of information. Personal digital assistants (PDAs), cellular telephones, and alphanumeric pagers are rapidly converging on a single pocket device that will leverage wireless TCP/IP networks and WWW protocols and can be used to deliver clinical information and alerts anytime, anywhere. We describe a wireless interface to clinical information for physicians based on Palm Corp.'s Palm VII pocket computer, a wireless digital network, encrypted data transmission, secure web servers, and a clinical data repository (CDR).

Introduction
The explosive growth of the Internet and the World-Wide-Web (WWW) has resulted in the ready availability of inexpensive, platform-independent, graphically-based, n-tier client-server software tools. These tools are well suited to the rapid development of web-based, user-friendly interfaces to legacy hospital information systems, bedside clinical systems, clinical data repositories (CDRs), and other sources of biomedical information. Web-based interfaces find ready acceptance among end users, many of which are already using a web browser at home for information or entertainment, and require relatively little user support or training.

Within the last year, manufacturers have begun to incorporate wireless digital networking and web technology into pocket computers (sometimes known as personal digital assistants, or PDAs) and digital cellular telephones, in order to make the vast information resources of the WWW available anytime, anywhere. Two competing WWW coding standards for these devices have evolved — "web clipping", developed by Palm Corp., and Wireless Application Protocol (WAP), developed by an industry consortium. Both provide for the adaptation of web content to the small screen size and limited input capabilities of pocket-sized devices.

We have previously described the use of a rapid prototyping strategy and off-the-shelf software to build and deploy a WWW-based interface, called Web/VS (Web Viewing System), for a CDR at Cedars-Sinai Medical Center (CSMC), Los Angeles, California. In this paper, we report on the implementation of Palm/VS (Palm Viewing System), a PDA-based application for secure remote access to the CSMC CDR over a wireless network (Figure 1). Palm/VS runs on Palm Corp.'s Palm VII™ pocket computer and on compatible devices such as the Palm V with the OmniSky wireless modem.

Materials and Methods
The Palm VII is a battery-powered pocket-sized monochrome computer with an integrated radio transmitter and receiver. Palm devices are based on the Motorola Dragonball™ MC68x328 processor family, and run the Palm Operating System version 3.0 which features excellent power management, economical use of memory, and handwriting recognition based on a stylized script called Graffiti™. The Palm VII accesses the BellSouth wireless Mobitex network at rates of approximately eight Kilobits/second (Kbps). The Palm VII can also be "synchronized" with PC- or Macintosh-based electronic mail, calendaring, and task-tracking utilities using the desktop computer's serial port and a "dock." The ongoing costs for wireless networking follow a cellular telephone model, with a base cost ranging from $10 to $40/month for traffic quotas ranging from 10 kilobytes (KB)/month to 300 KB/month. A flat-rate pricing plan for unlimited network traffic is also available. The OmniSky wireless modems for Palm devices employ the AT&T Cellular Digital Packet Data (CDPD) network at approximately 19.2 Kbps but are otherwise functionally equivalent from the user's perspective.

The server side of a Palm VII wireless application can be implemented using any web server that supports CGI capabilities (scripting and dynamic generation of web pages). In this case, the server side of the Palm/VS application is implemented with Microsoft Internet Information Server version 4.0 and Active Server Pages™ (a Visual-Basic-like programming language), using the Active Data Objects™ (ADO) component, and running on Microsoft Windows NT version 4.0. The web server communicates with the CDR's database using standard ODBC function calls and SQL queries. The hypertext markup language (HTML) that is transmitted to the Palm VII is specially formatted for the Palm VII's screen, and includes special "meta"
tags that embed version information and update the Palm VII's "history list."
The client side of a Palm wireless application is called a "Palm Query Application" (PQA) and is delivered as a single file with a PQA extension on the filename. A PQA can be downloaded into a Palm VII from a desktop PC when it is "synchronized," or can be beamed directly from one Palm VII to another using the built-in infrared port. PQA applications are essentially a set of web pages and images that have been precompiled into a compact form using a free development toolset downloaded from Palm's website. Unique HTML tags defined by Palm Corp. provide access to device-specific features. The contents of the PQA are interpreted by a simple Palm VII-based web browser called "Clipper," which also manages connections to the server side of the application over the wireless network and renders the specially-formatted web pages delivered by the server.

The PQA development cycle differs markedly from traditional Palm application development in C++. It allows developers to use the web coding and graphic utilities they are already comfortable with, right up to the point of compiling the PQA and downloading it to the Palm VII. Conversion of existing web applications into wireless-enabled Palm VII PQA's is quick and straightforward. PQA development also differs from conventional web applications, in that the PQA architecture allows static text (such as "on-line help"), forms, images, and icons to be compiled directly into the PQA file so they are resident on the Palm VII device, increasing responsiveness and decreasing network traffic.

**Palm/VS User Interface**

In order to view clinical data with Palm/VS, the user signs into the application using his or her login and password (Figure 2). Once the user's credentials have been verified, the application displays the user's "Personal Patient List" (PPL) in a menu (Figure 3). The user can pick a patient from the PPL and jump directly to the results screen, or can search for a patient by name, medical record number, or nursing unit. When a search produces multiple candidate patients, they are listed on a menu similar to the PPL.

Figure 1. Data flow between the Palm VII and the CSMC secure web servers and CDR via the BellSouth Mobitex wireless network, the Internet, and the CSMC firewall.
After selecting a patient, the current day’s results are displayed in a scrollable page, with abnormal results indicated by an asterisk. The user can use a pop-up calendar control to select results for a different day, or can request a variety of flow-sheets that trend selected laboratory results over time (Figure 4).

Alternately, the user can view a list of transcribed reports available on the system, and “drill down” to the full text of a report (Figure 5). Summaries of emergency department visits and hourly snapshots of selected ICU vital signs, input and output, ventilator settings, and blood gases are also available. A searchable staff directory allows the user to quickly send e-mail to any attending physician or hospital employee. Buttons allow the user to log out at any time during the session or to search for another patient.

The design of Palm/VS is tightly constrained by the bandwidth of the wireless networking connection, the small screen size, and the capabilities of the Palm VII’s “Clipper” web browser. Accordingly, the functionality of Palm/VS is only a small subset of the functionality and data types available in the Web/VS application for desktop PCs.

Security and Confidentiality
Security and confidentiality of patient information has always been a high priority at Cedars-Sinai Medical Center. An explicit Clinical Systems Security Architecture was designed and incorporated into the CSMC Technology Architecture Guidelines in 1999, and all new systems (whether built or acquired) are measured against this model.9 The security architecture is compliant with HIPAA and HCFA guidelines.10,11
Palm/VS, Web/VS, and the CDR support CSMC’s security needs in a variety of ways, including random and patient-specific confidentiality warnings to users, detailed logging of all user accesses or attempted accesses to patient data, automatic daily audit reports for accesses to “sensitive” patient accounts or test results and employee medical records, and interactive applications to support ad-hoc audits on either a per-user or per-patient basis. Some security issues that are specific to Palm/VS are described below.

1) Firewall traffic control and alerts. The secure web server for the Palm/VS application resides in a special subnet, or “demilitarized zone,” that is attached directly to the CSMC campus firewall (CheckPoint FireWall version 4.0 running on Windows-NT 4.0). The firewall performs protocol-
level filtering, exposing secure web servers and other selected machines to non-campus users for approved types of connections, while blocking and logging all other connection attempts from the Internet.

2) **Data encryption.** Wireless (radio-frequency) data transmissions and land-based traffic over BellSouth's Mobitex network are encrypted with Certicom's proprietary elliptic curve cryptography technology, which is embedded in the Data Encryption Standard Extended (DESX) protocol. The data traffic enters the public Internet via a proxy server at Palm Corp's data center (Figure 1). The sessions between the Palm proxy server and the CSMC secure web servers are encrypted using the Secure Socket Layer (SSL) standard and 128-bit keys.

3) **Client-level authentication.** The Palm VII's unique device ID, which is transmitted in each data packet to the CSMC secure web server, allows the Palm VII to be used as a physical token for "two-factor authentication" ("something you have, and something you know"). The server side of the Palm/VS application tracks the physical ID of all Palm VII devices used by physicians and, if a Palm VII is lost, can configured to lock out attempted accesses by that specific device. Additionally, to prevent subversion of the Palm/VS application by someone using an ordinary web browser, the web server's virtual directory for Palm/VS application is configured to only accept incoming connections from the known IP addresses of the Palm Corp. and OmniSky proxy servers.

4) **Application-level authentication.** The Palm/VS user must supply a valid CDR login and password. The system enforces a password change at least every 90 days. Each Palm/VS access to CDR data is logged with the user's name, patient name, medical record number, the date and time, and specifics of the data viewed.

**Results and Discussion**

Several earlier reports of clinical applications based on wireless technology exist in the literature. In the pre-Internet era, development of such applications was extremely complex both technically and logistically, requiring integration and coordination of pocket computers, wireless modems, and connectivity from diverse providers, as well as the development of custom software in C/C++ or assembly language.

The recent availability of completely integrated wireless PDAs and web-enabled digital cellular telephones which are immediately functional "out of the box," requiring only activation with a credit card, short-circuits many of the historically difficult logistical issues. The use of Internet protocols and subsets (or supersets) of WWW formatting and coding standards for wireless applications shortens the development cycle drastically, freeing up health care systems developers to concentrate on more important issues -- such as the marshalling and presentation of clinical data, and the development of sophisticated decision support rules and strategies.

The acceptance of Palm/VS and similar wireless applications among the CSMC attending staff and faculty has been excellent. Our CSMC web and CDR development teams are continuing to enhance Palm/VS, convert additional web-based applications for the Palm VII, and explore related wireless technologies such as WAP and two-way alphanumeric pagers. The teams sponsor user group meetings every quarter to discuss development plans and solicit feedback, and also maintain an electronic mailing list to distribute new or updated wireless applications to CSMC PDA owners.

However, we still have not arrived in a wireless Nirvana. During the last year's practical experience with use of the Palm VII in a clinical environment, we have identified a number of concerns and issues that will need to be taken into account by other developers planning to deploy wireless health care applications, particularly those selecting the Palm VII device.

**Browser Capabilities:** From a web developer's perspective, developing wireless applications for the Palm VII is like developing first-generation WWW applications circa 1995. The Palm VII's "Clipper" application does not support JavaScript, cookies, caching pragmas, nested HTML tables, frames, horizontal scrolling, or a number of other features found in modern web browsers. Session state must be maintained by passing information back and forth in hidden fields between forms on the client and scripts on the server. This leads almost inevitably to the divergence of separate code bases for web browser clients and Palm VII wireless clients, increasing the overhead of program maintenance.

**Security and Confidentiality:** The Palm VII's provisions for security and encryption were better than we expected, especially the availability of a unique Device ID within wireless transactions that can be used to correlate the user's login with a physical token (the Palm VII itself). However, there are two security concerns on the Palm VII that need to be fixed in subsequent models. The first is the local page cache or "history list," which persists from one invocation of a PQA application to another, and cannot be cleared programmatically from within the Palm/VS application. This makes it possible for someone to launch Palm/VS and view patient data
from a previous session without logging in. The workaround is to put global password protection on the Palm VII, but clinicians regard this as quite inconvenient. Another security weakness is inherent in the Palm’s handwritten input. Unlike the text boxes for password entry found in conventional web applications, which echo each keypress with a “blob” character, handwritten passwords must be displayed on the screen in the clear so that the user can confirm that the individual characters were recognized correctly. Consequently, the potential exists for a user to inadvertently reveal their password to a bystander. The Palm VII mitigates this risk by popping up a special dialog box to accept passwords and removing the information from the screen immediately after the input is completed.

**Display Characteristics:** The limited size (160 by 160 pixels) and color depth (black, white, and two shades of gray) of the Palm VII’s screen severely limits the types and amount of information that can be presented. Use of fonts small enough to allow formatting of a flowsheet, for example, puts readability at the lower limits of acceptability. Transmission of images and waveforms, even at thumbnail sizes, must await later models with better display technology, at least in the Palm family of devices.

**Connectivity and Bandwidth:** The bandwidth of the Mobitex network is comparable to a mid-1980’s modem. This is offset by the relatively small size of the data packets, which are a function of the screen size. Signal quality can be poor inside of buildings with metal shells. There is also some controversy over the safety of wireless devices in patient care areas, particularly intensive care units. Many hospitals have unilaterally forbidden the use of cellular phones in ICUs, and by implication Palm VII-like wireless devices, although the actual risk involved in such usage is not well documented.

In spite of these issues, it is clear that the wireless deployment of clinical applications has many compelling advantages. We expect these applications to proliferate rapidly over the next few years as wireless technology improves, PDAs, and cellular phones converge, and bandwidth costs decrease.

**References**


10. HIPAA rules and standards can be found at: http://aspe.hhs.gov/adminsimp/


