Achieving HIPAA Compliance with Palm® handheld, mobile manager, and smartphone solutions

Mobile solutions equip healthcare workers with critical information to boost productivity, reduce risk, and improve the quality of patient care. For organizations that handle protected health information (PHI), HIPAA may apply to the usage of handhelds, mobile managers, and smartphones. This whitepaper outlines HIPAA security requirements and reviews solutions that meet these requirements.

Handhelds, mobile managers, and smartphones have become a fixture in healthcare. Fifty-seven percent of all physicians and 73% of residents regularly use a mobile device during the workday (Source: Forrester Research, 2004). Wireless network use has grown with the popularity of mobile devices. A 2004 IDC survey found that over 80% of healthcare organizations have deployed a wireless LAN or plan to deploy one in the next 12 months. Using mobile devices, clinicians can access patient, reference, and billing information anytime, resulting in improved patient care and greater operational efficiencies.

Along with the significant benefits of mobile computing comes the responsibility to secure information on the device. When clinicians access PHI from handhelds, mobile managers, and smartphones, ensuring that information is stored and transmitted securely becomes a primary concern.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by the U.S. Department of Health and Human Services (HHS). HIPAA establishes standards for the use, disclosure and protection of personally identifiable health information.

In February 2003, HSS issued the "Final Security Rule." The Final Security Rule outlines administrative, technical and physical safeguards to PHI in electronic form. Used together, these measures establish a security baseline. This paper will concentrate on the Technical Safeguards section of the Final Security Rule: what it means and how to secure mobile devices under its guidelines. Complete HIPAA information is located at: http://www.hhs.gov/ocr/hipaa.

Who is affected?

HIPAA affects specified "covered entities"—such as healthcare plans, clearinghouses and providers—that handle personal health information. Contractors or business associates of covered entities may also be affected. For example, technology vendors and service providers to covered entities may need to comply with HIPAA guidelines.

Technical Safeguards

HIPAA establishes a set of requirements and implementation specifications for protecting electronic health information but stops short of specifying solutions or standards. Like the original HIPAA technical guidelines, the Security Final Rule is technology-neutral. This allows entities to select the technology that best suits their needs and allows for new innovations in security.

Section 164.312 of the Security Rule section entails technical safeguards to protect the integrity, confidentiality, and availability of health data. Specified measures include:

- Authentication
- Encryption
- Data Integrity
- Access Control
- Audit Controls
- Transmission Security

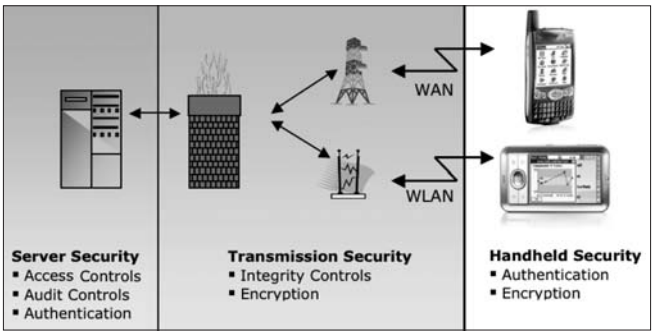


Diagram A: Layered Security in a Wireless Mobile Solution

Authentication

Authentication ensures that the party accessing a system is who he or she claims to be. Authentication should be considered at two levels: (1) device authentication and (2) network and server authentication. We discuss device authentication in this section and network and server authentication in the Transmission Security section below. Diagram A demonstrates the multiple points where security can be added to a wireless mobile solution.

Power-on authentication protects corporate data and network access in the event a device is stolen or lost. Because handhelds, mobile managers, and smartphones are prone to loss, it is important to ensure that an unauthorized person will not be able to view the data on a device. Every Palm® handheld, mobile manager, and smartphone comes with an integrated security application with power-on password protection. Users set a password that must be entered before the device can be accessed. This simple yet effective application has no back-doors and features automatic password locking options and password hinting for forgotten passwords. To ensure privacy, the password is hashed using the MD5 algorithm and only the hash value is stored. In addition, many Palm® products include built-in data encryption and data-wipe safeguards to further protect data privacy.

IT administrators may wish to go one step further and control end-user security policies. Managed security solutions enable the administrator to enforce security policies on handhelds, mobile managers, and smartphones. Managed policies include mandatory authentication, password length and strength, frequency of password change and timeouts. In addition, many solutions control infrared and application access, mandate data encryption and protect against dictionary attacks with data-wipe functionality. Policies are persistent on the device and can only be changed by the administrator.

Biometric authentication combines strength with ease of use. Biometric verification uses "something you are" (e.g. fingerprint, handwriting, or voice) to authenticate the user. Biometric Solutions offers a fingerprint reader that validates a user in seconds. CIC Sign-On uses signature verification for fast and easy authentication.

Encryption

Encryption, one of the pillars of data security, protects sensitive health information during storage and transmission. Modern cryptographic techniques use a combination of a cipher and a key to maintain privacy. The strength of the privacy depends on the strength of the algorithm and the size of the key, measured in number of bits. The AES (Advanced Encryption Standard or Rijndael) algorithm is considered the "gold standard" in encryption today, and other algorithms such as 3DES and ECC are also well-respected for combining strength with performance.

PHI stored on a mobile device should be encrypted when not in use. LifeDrive™ mobile manger and many Palm® handhelds include on-device data encryption. Palm Security 5p, an industry-leading security application, features 128-bit FIPS-certified AES encryption, the ability to encrypt all or only selected databases, and dictionary attack protection.

Managed security solutions from Palm Solution Providers allow the IT administrator to mandate data encryption. If sensitive data is stored on an expansion card, the card should also be encrypted. The applications listed below have additional functionality such as IT-controlled security policies, application-specific password protection, synchronization detection, and data wipe ("kill pill"). A variety of encryption algorithms are available including AES and 3DES.

Table A: Authentication Solutions

Solution	Strengths	Limitations	Solution Vendor *
Palm® Security 5p	Strong, effective Built-in – no additional software needed Intrusion protection prevents dictionary attack (on select Palm products)	Must rely upon user to enable password protection	Palm
Managed Security Solutions	Administrator can enforce password length & strength Dictionary attack protection Features vary and include encryption, access control, infrared lock, etc.	Must purchase and administer	CREDANT GoodLink Trust Digital And more…
Biometric Authentication	Fast authentication No forgotten passwords	Must purchase and administer	Biometric Solutions CIC

Table B: Encryption Solutions

Solution	Strengths	Limitations	Solution Vendor *
Palm Security 5p	Choice of algorithms, including FIPS-certified AES Encrypt all data or selected databases Currently LifeDrive and most Palm handhelds	Must rely upon user to enable encryption	Palm
Managed Security Solutions	Administrator can enforce encryption use and algorithm Encrypt all data or selected databases	Must purchase and administer	CREDANT GoodLink Trust Digital And more…

* See Appendix for more product information

Data Integrity

Data integrity controls protected data from tampering and alteration. Data residing on handhelds, mobile managers, and smartphones can be protected from unauthorized changes via:

- Authentication—ensures only authorized entities can access the device
- Encryption—protects the data during transit and storage
- Integrity controls—detects changes to data (e.g. using checksums)

For additional assurance, frequent data backups are recommended. Comparing backup files (via checksums or comparison programs) will reveal if and when data has been changed. In the event of data corruption, backups ensure a reliable copy of the data is available. Data backup can be as simple as synchronizing to a workstation using the Palm® desktop software included with every Palm® handheld, mobile manager, and smartphone. Alternately, administrators can choose server-based systems that automatically backup selected data to a central server.

Access Control

Access control is a system of limiting user access to resources, such as applications and data, based on administrator-granted access rights. Role-based access controls, where access privileges are granted based on groups or functional roles, are an efficient way to manage access rights.

HIPAA's Final Security Rule outlines access control standards for systems that maintain PHI. This rule would apply to mobile device implementations that retrieve sensitive data from a backend server. For example, databases or application servers that store and forward PHI must have access controls. Furthermore, the Security Rule delineates four implementation specifications:

- Unique user identification
- Emergency access procedures
- Automatic log off
- Encryption

The first two specifications are mandatory, while the latter two are "addressable," meaning that organizations can either choose to implement them or explain why the safeguard is not needed. Access control will typically occur at the database and/or application server. When a user requests PHI from their handheld, mobile manager, or smartphone, the responding server first authenticates the user, then determines if the user is authorized to access the requested information.

Software applications that manage PHI should address the access control requirement. For example, MercuryMD MData uses server-side, role-based access controls to prevent unauthorized access to patient information.

Audit Controls

Audit controls allow the administrator to review who is using the system and what data is being accessed. Normally, audit control functionality will be part of the application and database servers. When a wireless device requests data access from the server, request details (e.g. user name, data request and timestamp) are written to a log file. This log file can be viewed directly by an administrator or fed into a central monitoring system.

Many Palm solution providers include audit functionality in their products, such as MercuryMD, PatientKeeper and CREDANT Technologies. Common features include administrator visibility into who synchronized a device to the network, when data was requested, and which data was retrieved.

Transmission Security

Transmission security requirements safeguard health data from unauthorized access during transmission over a network. This section applies to any network, whether a wired LAN (local area network) or wireless networks such as 1xRTT, GPRS, 802.11 and Bluetooth.

To secure transmitted information, HIPAA suggests that IT administrators implement:

- Encryption
- Integrity controls

Both of these specifications are "addressable," meaning that organizations can either choose to either implement or explain why the safeguard is not needed.

A transmission security plan is essential when users are wirelessly transmitting or accessing PHI with a mobile device. If users only access PHI via cradle-based synchronization, then this section does not apply. With appropriate authentication controls, cradle synchronization is inherently private and transmission security measures such as encryption are most likely unnecessary.

Administrators have multiple options for securing PHI transmitted over a wireless network with Palm handhelds, mobile managers, and smartphones. Most mobile healthcare solutions include sufficient transmission security safeguards. For example, PatientKeeper incorporates two-factor authentication, AES encryption, TLS/SSL transport security and data integrity controls in their mobile suite. For organizations that require a separate transport security solution, the most popular choices for healthcare today are VPNs (Virtual Private Networks) and 802.1x security.

Table C: Transmission Security Solutions

Solution	Strengths	Limitations	Solution Vendor *
VPN	Encryption Authentication Data Integrity Vetted technology Utilizes existing VPN infrastructure	Requires client installation Some performance impact	WorldNet21 Mergic IBM
SSL VPN	Encryption Authentication Access control Low performance impact	Not compatible with all applications (primarily for browser-based applications)	Aventail F5 Nortel Networks
802.1x (LEAP)	Mutual authentication Encryption Dynamic key distribution Low performance impact	Dictionary attack (Correctable via RADIUS server settings) Only for 802.11 networks	Meetinghouse

* See Appendix for more product information

VPN

A VPN is a popular solution for securing access to intranet and extranet resources and data. Properly implemented, VPNs provide user authentication, encryption, and access control. VPN technology is widely deployed today for laptops and workstations, enabling mobile users to leverage an existing infrastructure investment.

An IPSec VPN client will conduct data integrity checks, in addition to authentication and encryption. Most VPN clients offer a selection of encryption algorithms, allowing an organization to choose a level of encryption that balances privacy and performance. PPTP VPNs are easy to configure, deliver fast performance and are supported by most Microsoft servers, as well as many Cisco gateways.

VPN technology is great choice for deployments that utilize a variety of networks. VPNs work over a virtually any network, including Ethernet LANs, GSM/GPRS, 1xRTT, 802.11, Bluetooth and CDMA.

SSL

SSL (Secure Sockets Layer) is a popular transport security standard used in virtually every web browser on the market today. SSL VPNs take advantage of the SSL built into browsers to authenticate and encrypt transmitted data. The main advantage of an SSL VPN is that, for many products, no software is needed other than a web browser. Using a backend SSL server, information is transmitted securely using the browser software included on all Palm® smartphones, mobile managers, and wireless handhelds. Another advantage is that this technology can be used over WAN, LAN and WLAN networks. A current limitation is that only browser-based applications can be secured using SSL VPN.

802.1x / WPA

WPA substantially improves upon WEP security by using 802.1x authentication, TKIP encryption and message integrity checks. 802.1x uses EAP (Extensible Authentication Protocol) to authenticate between a wireless device and an access point before the device can access the WLAN. In addition, 802.1x uses automatic key rotation to solve the much publicized WEP issue of key reuse. The most popular EAP types are LEAP, PEAP, TLS, TTLS and MD5. Meetinghouse's AEGIS client provides a choice of LEAP and EAP-MD5 for the Tungsten C handheld.

Cisco's LEAP (Lightweight EAP), based on the 802.1x standard, enforces mutual authentication between the client and access point. The "Lightweight" in LEAP refers to the processing usage, not the level of security, making LEAP particularly well suited to mobile devices. Because LEAP relies on password authentication, LEAP's one known vulnerability is dictionary attack. This vulnerability can be effectively countered by limiting failed password attempts at the RADIUS server.

Palm® devices with built-in Wi-Fi include WPA-PSK (Pre-Shared Key), also known as WPA Personal. WPA-PSK provided strong security without the need for a server or additional software.

802.11i / WPA2

WPA2 is the Wi-Fi Alliance approved implementation of 802.11i. The main difference between WPA and WPA2 is WPA2's use of AES for data encryption. While the upgrade from WEP to WPA security only required a software upgrade in most case, the upgrade to WPA2 will probably require a hardware upgrade or replacement.

The good news is that WPA2 is backward compatible with WPA. Since WPA offers strong security and WPA2 typically requires a hardware replacement, many organizations wait until new equipment is needed to upgrade to WPA2.

When selecting a transport security solution, first determine what networks will be utilized. Then consider technology benefits and drawbacks, as well as cost factors such as administrative burden and user training.

Conclusion

The good news is that the Final Security Rule allows organizations the freedom to select products and solutions best suited for their specific situation. The flip-side is that lack of standards can create confusion about how to attain HIPAA compliance. By selecting reputable security solutions that meet each of HIPAA's requirements for electronic health information, organizations can feel confident in their ability to achieve HIPAA compliance. Solutions should be easy for users to understand and synergistic with an organization's policies, practices, and technologies.

Security in Action: Mobile Healthcare Solutions that Incorporate HIPAA Security Tenets

Instant Communication for Successful Patient Care

Featuring Palm® + Horizon MobileCare™ Rounding from McKesson

McKesson Horizon MobileCare Rounding connects clinicians with patient information from their handheld, mobilw manager, or smart-phone. Authorized users see real-time laboratory and radiology results, vital signs, medication updates and patient history. Mobile access to this vital patient information enables physicians and staff to provide top quality care and reduce costs.

Mobile Access to Critical Data

Horizon MobileCare Rounding allows hospitals to leverage existing hospital systems to deliver data directly to their clinicians. This application integrates with core hospital and clinical information systems so that vital patient information is available. The Horizon MobileCare Rounding server is able to interface with both McKesson and non-McKesson backend systems. With information where and when they need it, physicians and nurses are able to make better decisions and improve patient care.

Guarding Sensitive Patient Information

McKesson Horizon Mobile Care Rounding teamed with PDA Defense to secure patient on the device or over the air. Security features include:

Authentication

- Password Authentication: Using PDA Defense, a PIN or password authenticates the user before access is granted.
- Dictionary Attack Protection: With PDA Defense, data is bit-wiped after a configurable number of failed password attempts.

Encryption

- On-device Encryption: Device data remains encrypted until viewed by an authorized user with PDA Defense. A variety of encryption algorithms can be selected for encrypting keys, data and passwords.
- Transport Encryption: SSL is used to encrypt data from the server to the device.

Access Control

- Role-based: Data access is permitted or denied based on roles.
- Administrative Control: When using PDA Defense, access levels, configurations and device lock-outs are controlled from an administrative console.

Transmission Security

- SSL: The Horizon Mobile Care Rounding Proxy Server Security Framework uses SSL to securely communicate between the mobile device and the server.
- Encryption: With PDA Defense, data remains encrypted until viewed by the user.
- Time-Out: When using PDA Defense, a configurable time-out forces the user to reenter the passkey after a period of inactivity.

For more information about McKesson Horizon Mobile Care Rounding, see **http://infosolutions.mckesson.com**

Security in Action: Mobile Healthcare Solutions that Incorporate HIPAA Security Tenets

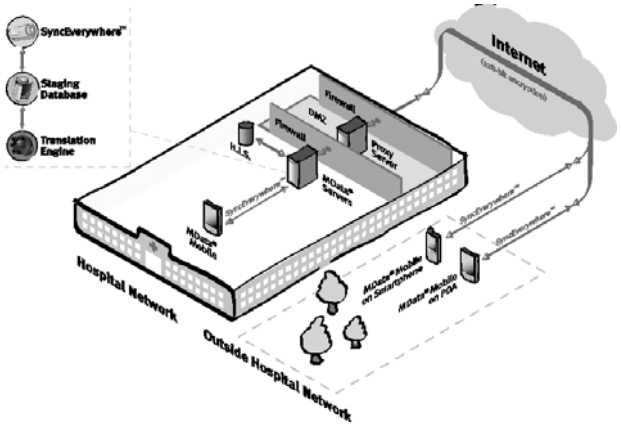
Mobile Clinical and Patient Data

Featuring Palm® + MData® from MercuryMD

As technology continues to reshape the way clinicians perform their job and care for patients, mobile technologies, like MData from MercuryMD, are improving clinical and operational efficiencies. With MData, clinicians can access patient information from their Palm® device—resulting in more informed decisions, quicker treatment, and better, more efficient care. Mobilized patient information includes patient census lists, demographics, laboratory results, diagnostic reports, medication lists, and transcribed reports—all of which are securely delivered from the hospital's information systems directly to clinicians' handheld devices.

How MData Works

Acting as a bi-directional data gateway, MData communicates HL7 messages in real-time, outbound and inbound, between the hospital information system and clinicians' mobile devices. Utilizing the SyncEverywhere™ conduit, MData supports all network connectivity platforms, including cellular, Internet, 802.11x, and infrared synchronization.



Layered Security Protects Patient Information

Authentication

- Client Authentication: MData users must be authenticated to access data, which is achieved through user registration and the use of secure passwords.
- User Lockout: A PIN is required after one hour (configurable) of inactivity and when the "lock & exit" function is activated. After multiple unsuccessful login attempts, the user's account is disabled and data is purged until the user is re-authorized.

Encryption

- Data Encryption: Clinical data and patient identifiers are stored separately on the device and are only decrypted and merged after user authentication.

Data Integrity

- Data Expiration: After seven days of non-use (site-configurable), where the user has not synchronized the device, all data is purged until the user logs into the system and synchronizes the device.

Access Control

- Role-based controls: Role-based access rules manage the flow of specific information to only those users with authorization.
- Beam Control: "Beaming" of protected data to other handheld users can be prevented.

Audit Controls

- Audit Trail: MData Manager's Audit Trail feature provides an "audit" of all lists and patients associated with an MData user.

Transmission Security

- Server Authentication: Users must be authorized by the hospital and then authenticated by MData before accessing their patients' data.
- End-to-end Encryption: From the hospital's network to the handheld device, patient data is secured by 128-bit encryption.

For more about MercuryMD, see **www.mercurymd.com**

Security in Action: Mobile Healthcare Solutions that Incorporate HIPAA Security Tenets

Secure Messaging and Data Access from Anywhere

Featuring Palm® + PatientKeeper® Clinical Results™ + PatientKeeper Platform™

With PatientKeeper Clinical Results, physicians can retrieve patient conditions, medication histories, lab results, and more via their mobile devices. Up-to-date patient lists with accurate patient locations eliminate the need for "pre-rounding".

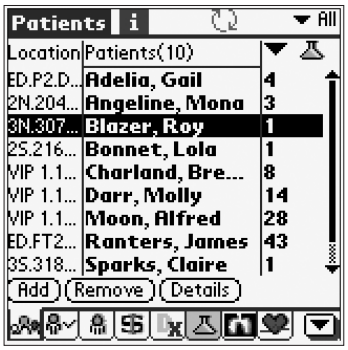
The PatientKeeper platform is designed to extend existing systems infrastructure by supporting mobile applications in a healthcare environment. In addition, PatientKeeper Software Development Kits (SDKs) allow application developers to rapidly create and port mobile applications. PatientKeeper supports both wired and wireless technology, including 802.11, Bluetooth®, infrared and cellular data networks.

HIPAA Security and Patient Confidentiality Support

PatientKeeper Platform has been designed to fully conform to HIPAA guidelines for patient confidentiality and privacy. Key security features include:

Authentication

- Two-factor server authentication: A PIN/password along with a private-key signed message to authenticate both the user and the device.
- Dictionary attack protection: After a configurable number of incorrect password attempts, the system can either lock-out the user or erase all PHI from the device.



PatientKeeper's PatientList module

Encryption

- AES Encryption: AES and ECC algorithms are used to encrypt data from the server to the device.
- On-device Encryption: Device data remains encrypted until viewed by an authorized user.
- Public/private key infrastructure is used for encrypting all keys and passwords.

Data Integrity

- Data Authenticity: Data updates must be signed by the authorized user's private key.
- Non-repudiation: Digital signatures ensure that a transaction originates from an authorized physician and device, and the transaction remains unaltered since it was signed.
- Copy Control: Users cannot copy data outside of a PatientKeeper application.

Access Control

- Role-based: Data access can be assigned based on groups and roles.
- Central Administration: Access levels, configurations and device lock-outs are controlled from an administrative console.

Audit Controls

- Logs: A complete set of logs are maintained on the device and PatientKeeper Mobilizer™ Servers.
- Data access is tracked down to the individual result level (e.g. a specific lab test on a specific patient).

Transmission Security

- TLS/SSL: The PatientKeeper Security Framework uses TLS/SSL to securely communicate between the mobile device and the PatientKeeper server.
- Encryption: Data remains encrypted from the server to the device until viewed by the user.
- Time-Out: A configurable time-out forces the user to re-enter the passkey after a period of inactivity.

For more information about PatientKeeper solutions, see **www.patientkeeper.com**

APPENDIX A: Security Solutions for Palm® handhelds, mobile managers, and smartphones

This appendix provides more information on the products that you can use to implement HIPAA compliant handheld, mobile managers, and smartphone solutions.

Authentication and Data Encryption Solutions

Power-on authentication and device data encryption address the need to secure data that resides on the mobile device. Managed security solutions allow IT to control policies such as password length, strength, application access, and data encryption.

Vendor	Product	Description
Biometric Solutions	FobLock	Using fingerprint recognition, FobLock controls access to Palm® and other IrDA-enabled devices. FobLock can be used with its own or customized or an organization's database.
CIC (Communications Technologies Corp.)	Sign-On	Sign-On uses biometric signature verification to safeguard data on a device. Users simply sign their name or create a personalized drawing or design, and Sign-On verifies it to unlock the device.
GoodLink	GoodLink Mobile Defense	GoodLink Mobile Defense provides enhanced password protection, data encryption and hardware button password entry. IT managers can enforce password, encryption and beaming policies and set restrictions on application usage.
CREDANT Technologies	Mobile Guardian	Mobile Guardian addresses mobile security issues with centrally managed, policy administration and strong on-device user authentication and policy enforcement.
Pointsec	Pointsec for Palm OS®	Pointsec combines sophisticated access control, data encryption and user authentication, including authenticated infrared and HotSync.
TealPoint Software	TealLock Corporate Edition	Corporate TealLock features serial and infrared lockout, data encryption, administrator password, remote unlocking and password controls.
Trust Digital	TRUST Enterprise Secure	TRUST Enterprise Secure provides a policy-based framework to automate the creation, deployment, enforcement, auditing and control of security policies.

Transmission Security Solutions

A VPN (Virtual Private Network) is a popular solution for securing data access over virtually any type of network. Properly implemented, VPNs can provide user authentication, encryption, access control, message authentication and integrity controls. VPN technology is in wide use today for laptops and workstations, enabling mobile users to leverage the existing infrastructure.

For 802.11 networks, a security solution based on the 802.1x standard may be the right choice. With 802.1x, a wireless device must authenticate with the access point before accessing the WLAN (Wireless Local Area Network). 802.1x also solves the much-publicized issue of key reuse by exchanging dynamic WEP keys.

Vendor	Product	Description
Aventail	WorkPlace	SSL VPN technology delivers strong security using SSL, proxy protection from direct network access, and seamless integration with directories.
F5	FirePass	F5 FirePass SSL VPN provides a Web-based method of extending secure remote access to mobile users - with no special software on the client and no modifications to back-end resources.
IBM	WebSphere Everyplace Access (WEA)	WEA provides secure, wireless access to enterprise applications and data. Features include: PIM and email sync, mobile instant messaging and device management.
Meetinghouse	AEGIS WLAN Security Solution	AEGIS supports LEAP, an 802.1x standards-based authentication method developed by Cisco. LEAP requires mutual authentication, which means both the user and access point must authenticate one to the other before network access is granted.
Mergic	Mergic VPN	Mergic VPN is a Point-to-Point Tunneling Protocol (PPTP) VPN client for securing remote access.
Nortel Networks	SSL VPN	Alteon SSL VPN is a remote access security solution that extends the reach of enterprise applications to mobile workers. By using secure sockets layer (SSL) as the underlying security protocol, Alteon SSL VPN allows for truly unrestricted remote access; using the Internet for remote connectivity and the ubiquitous Web browser as the primary client interface.
RSA Security	SecurID	SecurID software token, used with RSA ACE/Server software, generates a random, one-time-use access code that automatically changes every 60 seconds.
WorldNet21	anthaVPN (formerly movianVPN)	anthaVPN, an IPSec-based VPN client, provides strong authentication, encryption and data integrity assurance for secure remote access to email and data. anthaVPN supports many popular gateways, including Cisco, Lucent and Nortel.

Palm, Inc.
950 W Maude Ave
Sunnyvale, CA 94085-2801
www.palm.com

P 316 05 5K 8/05