Security Brief: Implementing HIPAA-Compliant Palm™ Handheld Solutions

Security technologies are available for the Palm™ platform to help healthcare organizations implement HIPAA-compliant handheld solutions. This planning brief discusses security technologies and products that are compatible with Palm handhelds.

HIPAA Requirements

Two sections of the Health Insurance Portability and Accountability Act (HIPAA) specifically address technical security measures for protecting health information:

- The **Technical Security Services** section (§142.308(c)) describes measures needed to safeguard the integrity, confidentiality and availability of sensitive health data. These measures include access control, audit procedures, user authorization and data and entity authentication.

- The **Technical Security Mechanisms** section (§142.308(d)) outlines security measures meant to protect sensitive health data from unauthorized access during transmission over a communications network. HIPAA requires that IT administrators implement integrity controls, message authentication, access controls and encryption.

Security Solutions for Palm™ Handhelds

Security technologies available for the Palm platform help healthcare organizations implement HIPAA-compliant handheld solutions. Security solutions compatible with Palm handhelds include the following:

Handheld Authentication and Data Encryption Solutions

Power-on authentication and on-device data encryption address some of HIPAA's data security guidelines. Every Palm handheld comes with an integrated Security application that allows the user to set a password, which must be entered before the handheld can be accessed. Partner solutions provide additional password protection and typically add data encryption capabilities:

Product	Features
Asynchrony's PDADefense Enterprise	• PDADefense Enterprise provides enhanced password protection, 128-bit or 512-bit Blowfish encryption and hardware button password entry. IT managers can enforce password, encryption and beaming policies and set restrictions on application usage.
Certicom movianCrypt	• movianCrypt uses 128-bit Advanced Encryption Standard (AES) to encrypt handheld data and provides advanced password security and auto-lock functionality.
Communications Technologies Corporation 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.
Credant Technologies Mobile Guardian	• Mobile Guardian addresses mobile security issues with centrally managed, policy administration and strong on-device user authentication and policy enforcement.
IS/Complete PDA Restrictor	• Restrictor allows an administrator to create profile categories for different users on a single Palm handheld and enables users to automatically lock their Palm and hide records.
Kasten Chase Assurancy SecureData Enterprise	• Assurency SecureData provides record-level encryption for all data stored on the handheld and decrypts only as required, ensuring a fast user experience.
TealPoint Software Corporate TealLock	• Corporate TealLock is a secure automatic locking program. Features include serial and infrared lockout, data encryption, administrator password, remote-unlocking and password controls.
Trust Digital PDA Secure	• PDASecure encrypts data on the handheld using AES. It features universal integration with all applications installed on the handheld and allows administrators to define security policies

Virtual Private Network (VPN) Solutions and Complementary Authentication Solutions

VPNs are used to provide secure access to intranet and extranet resources and data. Properly implemented, VPNs provide integrity controls, message authentication, access control and encryption. VPN technology is in wide use today for laptops and workstations, enabling mobile users and satellite offices to access centralized health data. This same trusted security can be extended to the Palm handheld

Product	Features
Certicom movainVPN	• movianVPN is an IPSec-based VPN client that provides strong authentication, encryption and data integrity assurance to secure remote access to email and Nortel.
Mergic VPN for Palm OS	• Mergic VPN is a Point-to-Point Tunneling Protocol (PPTP) VPN client for securing remote access.
RSA Security SecurID	• SecurID software, used in conjunction with RSA ACE/Server software, generates a random, one-time-use access code that automatically changes every 60 seconds. Palm™ handhelds can store up to eight RSA SecurID tokens,
SafeNet SoftRemotePDA	• SoftRemotePDA is an IPSec-based VPN client that offers secure client-to-gateway communications over wireless networks and works with many popular gateways.
Secure Computing e.iD for Palm	• From the maker of SafeWord authenticators, e.iD for Palm is a software authenticator. It allows any device running Palm OS® v2.04 (and higher) to become a PremierAccess enabled authenticator.
V-ONE Corp. SmartPass for Palm	• SmartPass is a VPN client that provides secure remote access. SmartPass connects to V-ONE's SmartGate VPN server.

Cryptographic and PKI Toolkits

Public Key Infrastructure (PKI) is a system that uses digital certificates to authenticate and verify the identity of both parties. PKI can be used to securely authenticate parties before medical information is exchanged. Combined with strong encryption and message integrity, these technologies can be used to secure the transmission of sensitive data over an insecure network like the Internet.

Secure Enterprise Messaging

For a secure email solution for the healthcare enterprise, Palm offers the Tungsten™ Mobile Information Management Solution (MIM Solution), which enables users to securely send and receive enterprise email on Palm™ i705 or Palm™ m500 series handhelds. The MIM Solution implements multiple layers of security to protect sensitive email communications. Security mechanisms include:

- Unique User Authentication. The MIM Solution Mobile Mgr client software must authenticate against the MIM Server before the user can access messages. In addition, the Security Plus application, which is included with the Tungsten MIM Solution, allows IT administrators to enforce password protection and other security policies on the Palm handheld.
- Encryption. End-to-end encryption using the AES algorithm is applied to each message. In addition, Security Plus, encrypts data stored on the handheld and expansion cards.
- Data Integrity Controls. Each message is sent with a data integrity checksum to ensure that data has not been altered during transmission
- Access Control. Users are authenticated to the corporate mail server with their mail server user id, giving the IT administrator control over each user's data access.
- FIPS 140-2 Certification Pending. Palm Crypto Manager provides cryptographic services such as encryption and integrity controls. Crypto Manager is currently pending Federal Information Processing Standard (FIPS) 140-2 certification.

Product	Features
Blueice Research Mulyipass Client	• Multipass Client is based on open PKI standards. This multi-platform client provides strong encryption functionality and the ability to perform secure digital transactions.
Certicom Trustpoint Client	• Trustpoint Client adds PKI security to client-side applications running on Palm OS. Supporting both X.509 and Wireless Transport Layer Security (WTLS) digital certificates, Trustpoint Client allows developers to add digital signature and strong encryption to applications to support trust, authentication, confidentiality, privacy and message integrity.
Diversinet Corp Passport	• Passport client/server security software facilitates digital signatures, authentication and encryption with PKI products specifically optimized for wireless environments and devices.
Ntru Cryptosystems Inc. Security Toolkit	• Ntru offers a full range of public and symmetric key functionality, including encryption, decryption, signing and verification.
RSA Security Cert-C Micro Edition	• RSA BSAFE Cert-C Micro Edition software is specifically designed to deliver PKI technology to mobile devices.

Frequently Asked Questions about Palm™ Handhelds and HIPAA Compliance

Q1. Are Palm devices HIPAA compliant?

HIPAA does not set guidelines for hardware or require that specific technologies be implemented in healthcare environments. Rather, HIPAA requires that healthcare organizations implement authentication, encryption and other security technologies to protect patient data.

Palm handhelds running Palm OS® 5, in conjunction with applications from Palm Solution Partners, provide a wide range of security measures to meet or exceed HIPAA requirements. Palm OS 5 includes built-in security technologies such as system-level authorization and authentication and Secure Socket Layer (SSL) encryption. Applications available from Palm Solution Partners include solutions for advanced password protection, enhanced encryption and virtual private networks (VPNs) to further protect sensitive data.

Q2. How can I lock my Palm device to prevent unauthorized access to data?

Every Palm™ handheld running Palm OS® version 4.1 or later has built-in password protection, and automatic password locking options. Additionally, Palm Solution Partner applications such as Asynchrony PDA Defense Enterprise, Communication Intelligence Corporation Sign-On, and TealPoint Software Corporate TealLock offer advanced password protection, biometric signature verification, serial and infrared lockout and other safeguards to further protect against unauthorized access.

Q3. How can I encrypt data on my Palm handheld to prevent unauthorized access?

The Palm platform supports a wide range of encryption technologies and standards. The Security Plus application, included with the Tungsten™ Mobile Information Management Solution (MIM Solution), encrypts data using a 128- or 512-bit symmetric key algorithm and enables IT administrators to control which data is encrypted.

Enterprises can also employ Palm Solution Partner applications, such as Asynchrony PDA Defense Enterprise, Certicom movianCrypt or Trust Digital PDA Secure to implement Advanced Encryption Standard (AES) and other encryption technologies to further protect handheld data. Solutions such as RSA Security SecurID and Mergic VPN for Palm OS also enable organizations to extend VPN protection to handheld devices.

Q4. What new security features is Palm adding in OS 5?

Palm OS 5 was specifically designed to bring enterprise-class security to handheld devices. The new operating system includes a suite of best-in-class security services including support for AES encryption algorithms, digital signatures, SSL encryption and VPNs using the IP Security (IPSec) protocol and Point-to-Point Tunneling Protocol (PPTP). Palm OS 5 also supports the latest device identification standards, including Flash ID, Mobitex Access Number (MAN) and Electronic Serial Number (ESN).

The Palm Crypto Manager, which is part of the Tungsten MIM Solution, is currently pending Federal Information Processing Standards (FIPS)140-2 certification. Crypto Manager ensures that critical security functions, such as encryption, decryption, key generation, checksums and Pseudo Random Number Generation (PRNG) are performed correctly.

Q5. How secure is Bluetooth in a healthcare setting, and how does it compare to WiFi/802.11?

Healthcare organizations can use either Bluetooth or 802.11b wireless technologies—or a combination of both. While technology has certain security vulnerabilities that must be addressed, it is possible to effectively safeguard data using either wireless standard. Organizations should choose a wireless technology based on the functionality they require rather than security concerns.

Historically, 802.11b encryption and authentication technologies have been regarded as vulnerable, but organizations can implement solutions such as RADIUS, RSA SecurID and VPN to address these issues and implement secure wireless 802.11b LANs.

Bluetooth includes more stringent built-in authentication and encryption technologies, but is vulnerable to "man-in-the-middle" attacks, as well as the risk of unauthorized devices trying to access sensitive data by masquerading as authorized devices on the network. These shortcomings can be addressed through Public Key Infrastructure (PKI) solutions provided by RSA Security and others

Q6. Can I transmit data wirelessly over a WAN (for example, using your i705) securely?

Yes. Palm's Tungsten MIM Solution provides robust remote authentication and encryption to protect communications between handhelds and corporate systems. Every communication to the MIM Server from a Palm i705 handheld is encrypted

Q6. Can I transmit data wirelessly over a WAN (for example, using your i705) securely? (Continued)

using the AES standard, and uniquely identified and authenticated with the MIM Server's database of authorized, active handhelds.

The Tungsten MIM Solution can also integrate with the organization's Lightweight Directory Access Protocol (LDAP) server and Microsoft Exchange or Lotus Domino mail servers. Organizations can also take advantage of a wide range of cryptographic toolkits, PKI toolkits and cryptographic libraries available through Palm Solution Partners to implement even stronger encryption.

Q7. How can I enforce security policies (for example, password lengths) on my organization's Palm handhelds?

The Security Plus application included in the Tungsten MIM Solution enables IT administrators to centrally enforce password protection policies, such as password length and type, frequency of password changes and time-outs, and access to applications and encryption tools.

Q8. Can I maintain administrative control over my Palm handhelds to prevent users from undoing the security mechanisms?

Yes. The Security Plus application included with the Tungsten MIM Solution enables enterprises to set persistent security policies that can only be changed by the designated Administrator. Palm Solution Partner applications, such as Credant Technologies Mobile Guardian and IS/Complete PDA Restrictor, also provide centralized administrators with expanded security policy management and enforcement options.

Q9. What are the various authentication mechanisms I can use for Palm handhelds connected to my network resources?

Every communication to the MIM Server from a Palm handheld is uniquely identified and authenticated with the MIM Server's database of authorized, active handhelds. Palm devices also include built-in PPP support for authenticating users, as well as support for popular authentication protocols such as the Challenge-Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP) and Password Authentication Protocol (PAP). Palm also offers multiple methods to uniquely identify each handheld, including Hardware Serial Number (HSN), flash ID, and MAN. Palm Solution Partner applications offer biometric signature verification and advanced password and security policy control.

Q10. How can I protect Palm devices and corporate systems from virus attacks?

Since viruses are platform-specific, Palm handhelds are not susceptible to the thousands of viruses developed for the Windows platform, and cannot pass viruses back to desktop computers during synchronization. In fact, to date there have been no successful virus attacks on the Palm platform. However, since any connected system could potentially be at risk for malicious code, organizations can leverage anti-virus applications specifically created for Palm handhelds by best-in-class anti-virus software vendors such as McAfee, Symantec and Computer Associates.

Q11. How can I monitor the effectiveness of my security mechanisms?

The Tungsten MIM Solution enables system managers to proactively monitor server status using Simple Network Management Protocol (SNMP) and SNMP-compliant management consoles such as HP OpenView or Microsoft SMS. The MIM Server also maintains comprehensive logs of all components and transactions, enabling administrators to identify abnormal usage patterns and track metrics such as unsuccessful logins and multiple simultaneous requests from single users.

Palm Solutions Group
400 N. McCarthy Blvd.
Milpitas, CA 95035
1-888 223-4817
USA
www.palm.com/enterprise