

Formotus™ Mobile Solutions and HIPAA Compliance

A Formotus Application Note

The Health Insurance Portability and Accountability Act (HIPAA) sets privacy and security rules for the safe handling of personal health information. These rules apply directly to 'covered entities' such as hospitals and health plans, but if you provide technology or services to such covered entities, you too need to understand and comply with HIPAA rules. This paper explains how Formotus mobile software applications can be used to handle protected health information (PHI) on Windows Mobile devices in a HIPAA compliant workplace.

Contents

What HIPAA Requires for Compliance.....	2
Windows Mobile Provides Powerful Compliance Tools	2
Formotus Adds Security, Not Risk	4
Formotus Servers Never Touch Your Sensitive Data	4
Formotus Adds an Extra Layer of Authentication	5
Formotus Adds Extra Audit Control Tools.....	5
Appendix: Windows Mobile Compliance Features.....	7
Disclaimer	8

What HIPAA Requires for Compliance

HIPAA is technology neutral in that it does not specify or endorse any particular technology solutions. Instead it specifies standards to be met. Some standards specify implementation guidelines, which can be either required or 'addressable' – meaning optional with a good explanation.

The Security Rule of HIPAA enumerates five technical safeguard standards. The associated implementation guidelines are listed below.

The Five HIPAA Security Safeguard Standards:

1. Access Control
 - a. Unique User Identification (Required)
 - b. Emergency Access Procedure (Required)
 - c. Automatic Logoff (Addressable)
 - d. Encryption and Decryption (Addressable)
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security
 - a. Integrity Controls (Addressable)
 - b. Encryption (Addressable)

Detailed discussions of these standards and what they require in practice are readily available elsewhere.¹ The question we want to address here is whether and how Windows Mobile devices can be used in a HIPAA compliant environment that meets these standards.

Windows Mobile Provides Powerful Compliance Tools

Microsoft is well aware of the regulatory hurdles faced by IT organizations in HIPAA covered entities, and has published a white paper specifically addressing how Windows Mobile devices can be used in compliance with these HIPAA standards.² Microsoft's compliance vision statement says, in part:

¹ See for example the Security Series papers by the Centers for Medicare & Medicaid Services (CMS), especially paper #4 on Technical Safeguards, which can be found at: http://www.hipaadvisory.com/action/Security/CMS_Series/TechnicalSafeguards.pdf.

² For more detailed information on Windows Mobile, see the Microsoft white paper "Windows Mobile and the Health Insurance Portability and Accountability Act (HIPAA),"

Since technology and software cannot be compliant on their own, the most effective and secure policy is one that combines both technology and IT policies and strategies. Technology is merely an enabler for compliance. And using Windows Mobile can help make it easier to be HIPAA compliant.³

The Microsoft white paper details which specific features and capabilities of Windows Mobile devices enable compliance with each of the five HIPAA standards (see the Appendix for a summary chart). A few highlights of Windows Mobile control capabilities discussed in the paper are listed below.

Windows Mobile Features that Support HIPAA Compliance

- Windows Mobile 6 uses Enhanced Advanced Encryption Standard (AES) and enhanced device locks to help protect passwords and PINs.
- Windows Mobile encryption algorithm implementations are certified as compliant with the US Federal Information Processing Standard (FIPS) 140-2, level 1.
- Data on mobile devices can be encrypted.
- With Exchange, devices can be wiped automatically after a specified number of incorrect login attempts, or remotely if a device is lost or stolen.
- Exchange can encrypt and synchronize email, calendars and contact data
- Exchange 2007 allows for an administrator to recover a user's pin and unlock the Windows Mobile device in the case of an emergency.
- Information Rights Management can be implemented on Exchange email and Office documents.
- Network level encryption is supported for VPN, HTTPS and WPA
- Windows Mobile devices support power-on authentication, strong password enforcement (with Exchange), and hashed password storage on the device.

These features enable organizations that deal with protected health information to use Windows Mobile devices confidently, knowing that the sensitive data is encrypted on the device, encrypted in transmission, and available only to authenticated users.

July 2007, found at http://download.microsoft.com/download/c/b/d/cbdc18d1-1a01-4736-a557-08474ec73443/Windows_Mobile_and_HIPAA.pdf.

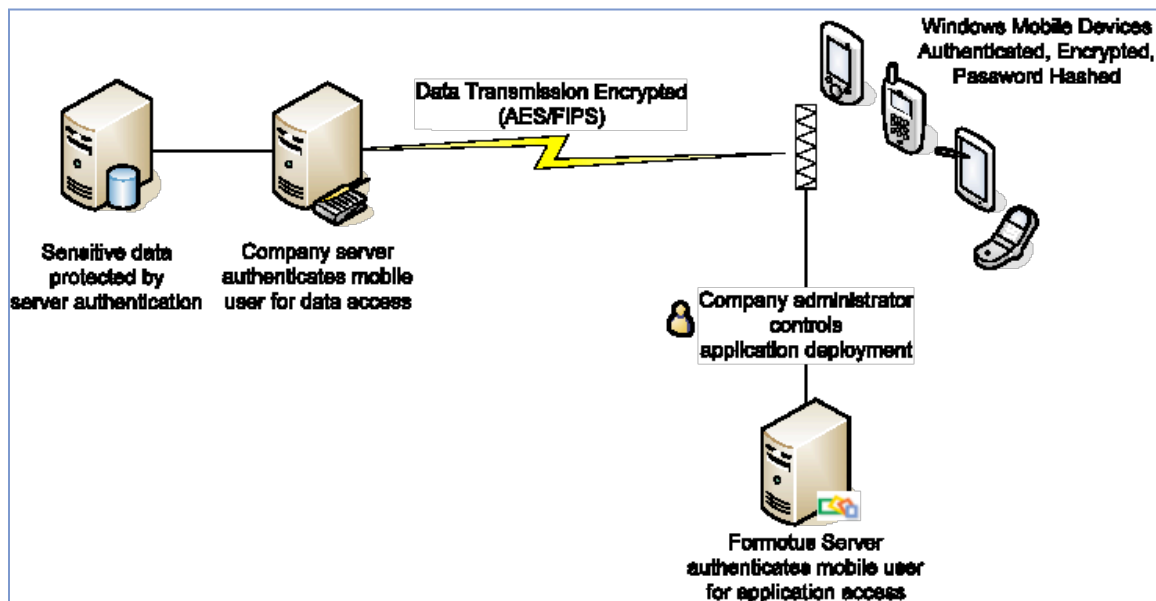
³ "Windows Mobile and HIPAA," p. 8.

Formotus Adds Security, Not Risk

The beauty of the Formotus solution, in terms of HIPAA compliance, is that it handles your sensitive data entirely within your protected Microsoft ecosystem. As secure as you choose to make your Windows Mobile devices and their connections to your network servers, that's how secure the information is when you use Formotus applications on those devices. Formotus even adds an extra layer of security in its application authentication architecture.

Formotus Servers Never Touch Your Sensitive Data

The Formotus solution is combination mobile software and Web services. Mobile users authenticate on the Formotus server in order to install and use the mobile applications that will handle your company's data, including protected health information. Once the application is installed on the device, however, all data transmission takes place directly between your devices and your servers. Depending on your backend architecture, Formotus mobile users may authenticate themselves against your SharePoint, SQL, Exchange, IIS, Active Directory and/or other servers where your data resides. Everything Formotus applications do with the data on your Windows Mobile devices is wrapped in the encrypted security of the device and the authentication security of your servers. Only the application itself is connected to the Formotus server, not the data.



Formotus servers do not touch sensitive data but do add an extra layer of authentication

Formotus Adds an Extra Layer of Authentication

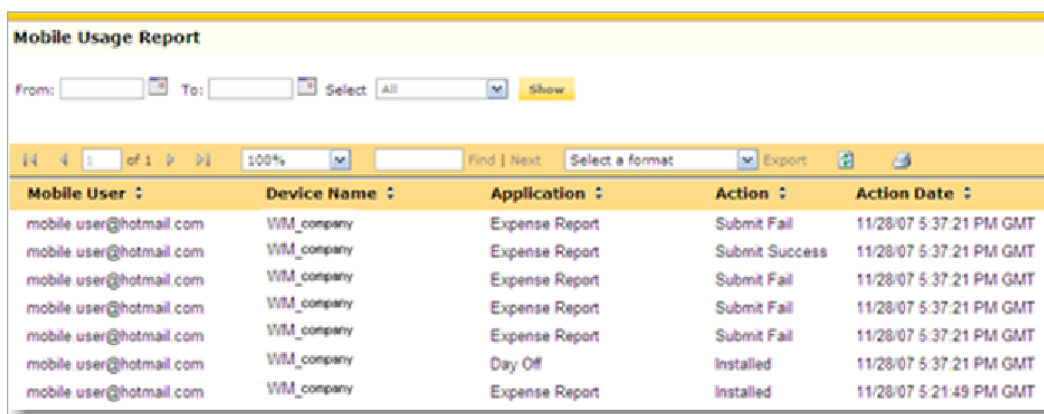
Along with all the security measures you choose to implement on your mobile devices and your servers, the Formotus solution injects one additional layer of security. In order to access any of your sensitive data using a Formotus application, the mobile user must be authenticated not only your data server but on our Formotus application server as well.

Each mobile user is required to submit a unique ID and password in order to use the Formotus service. Without such authentication, the mobile applications will not run and the user cannot even attempt to authenticate on your data server to access or change protected health information.

Formotus Adds Extra Audit Control Tools

One of the technical safeguard security standards of HIPAA is Audit Controls, which calls for mechanisms to record and examine activity in the systems that contain or use protected health information.

Logged information on your servers is the best mechanism for tracking data access activity. The Formotus application server, however, provides you a supplementary reporting capability for auditing data access activity from your mobile devices. Our server tracks and allows you to generate reports on every interaction your mobile users have with the Formotus application.



The screenshot shows a web-based interface for a 'Mobile Usage Report'. At the top, there are search filters for 'From:' and 'To:' with a 'Show' button. Below this is a navigation bar with '100%' zoom, 'Find | Next', and 'Export' options. The main content is a table with the following data:

Mobile User	Device Name	Application	Action	Action Date
mobile.user@hotmail.com	WM_company	Expense Report	Submit Fail	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Expense Report	Submit Success	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Expense Report	Submit Fail	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Expense Report	Submit Fail	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Expense Report	Submit Fail	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Day Off	Installed	11/28/07 5:37:21 PM GMT
mobile.user@hotmail.com	WM_company	Expense Report	Installed	11/28/07 5:21:49 PM GMT

Formotus reports track application installations and all attempts to interact with sensitive data, even failed attempts

By generating and reviewing Formotus reports regularly, you can supplement your Audit Controls with extra information such as:

- A record of how many and exactly which devices have applications installed that can access your data at any given time.
- A time stamped log of every attempt by every user to access your data with any Formotus application, and whether the attempt succeeded or failed.

You can use this reporting capability to continuously monitor and control your mobile devices' interactions with protected health information, and to create an audit trail demonstrating you have done so.

Appendix: Windows Mobile Compliance Features

Summary of HIPAA Security Rule Standards ⁴

Technical Safeguard	HIPAA Section	Implementation Specification	Windows Mobile's Response
Access Controls	164.312(a)	Unique User Identification	<ul style="list-style-type: none"> Enhanced Advanced Encryption Standard (AES) Enhanced device locks
		Emergency Access Procedure	<ul style="list-style-type: none"> Administrator pin recovery
		Automatic Logoff	<ul style="list-style-type: none"> Automatic logoff after designated period of inactivity
		Encryption and Decryption	<ul style="list-style-type: none"> Enhanced Advanced Encryption Standard (AES) FIPS compliant cryptographic algorithms
Audit Controls	164.312(b)		<ul style="list-style-type: none"> Microsoft Exchange 2003 with Exchange ActiveSync (EAS)
Integrity	164.312(c)		<ul style="list-style-type: none"> CryptoAPI Advanced Encryption Standard (AES) Microsoft Exchange 2003 with Exchange ActiveSync (EAS) Support for PFX certificates
Person or Entity Authentication	164.312(d)		<ul style="list-style-type: none"> Windows Mobile 6.0 Messaging and Security Feature Pack Enforceable strong passwords Windows Mobile 6 storage card encryption and remote device wipe
Transmission Security	164.312(e)(1)	Integrity Controls	<ul style="list-style-type: none"> Advanced Encryption Standard (AES) Microsoft Exchange 2003 with Exchange ActiveSync (EAS) FIPS compliant cryptographic algorithms
		Encryption	<ul style="list-style-type: none"> Advanced Encryption Standard (AES) FIPS compliant cryptographic algorithms

⁴ Table based on "Windows Mobile and the Health Insurance Portability and Accountability Act (HIPAA)," July 2007, found at http://download.microsoft.com/download/c/b/d/cbdc18d1-1a01-4736-a557-08474ec73443/Windows_Mobile_and_HIPAA.pdf

Disclaimer

The general guidance provided in this document is intended to help improve awareness of HIPAA security principles and how they relate to Formotus technology. It is not legal advice. For specific questions about HIPAA security and privacy requirements as they relate to your organization, you should contact an attorney with expertise in these matters.

The information contained in this document represents the current view of Formotus, Inc., on the issues discussed as of the date of publication. Because Formotus must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Formotus, and Formotus cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is not legal advice and is for informational purposes only. FORMOTUS MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user.

© 2008 Formotus, Inc. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.