



MOBILE DATA COLLECTION FOR HEALTH CARE

Ensuring HIPAA Security Compliance in Mobile Environments

Introduction

Any HIPAA covered entity has the responsibility to be in compliance with the **HIPAA** Security Regulations for Electronic Protected Health Information (**EPHI**) for all aspects of EPHI; access, storage and transmission. As part of the HITECH Act provisions of the American Recovery and Reinvestment Act (**ARRA**) signed by President Obama on February 17, 2009, transmission security is an addressable implementation meaning any HIPAA entity must use reasonable and appropriate measures to meet the standard (**§ 164.312(e)(1)**). Further, covered entities and their business associates will be required to meet this standard by February 17, 2010.

Overview

HIPAA's *Privacy Rule* requires that EPHI is properly protected and prohibits covered entities from transmitting EPHI over open networks or downloading to public or remote computers without encryption. The *Security Rule* requires covered entities to put in place detailed administrative, physical and technical safeguards to protect EPHI. To do this, covered entities are required to implement access controls, encrypt data and set back-up and audit controls for EPHI in a manner commensurate with the associated risk, including making certain that vendors (Business Associates) supplying technology that touches EPHI are in compliance with HIPAA Privacy and Security Rules.

Field2Base in HIPAA Environments

Field2Base software meets or exceeds all HIPAA Privacy and Security Rules for all aspects of Electronic Protected Health Information (**EPHI**) as standard, commercial off the shelf software (COTS). Specifically, Field2Base as a Business Associate to any covered HIPAA entity meets these requirements as part of an overall HIPAA compliance plan by the following:

Access Security

Access to Field2Base software requires two level password protection regardless of hardware device (Tablet PC, Laptop, Handheld) which is part of the HIPAA Security Standard.

Storage Security

All information stored in Field2Base, including any EPHI, is encrypted at 256 bit encryption to the AES / RIJNDAEL Standard. (Note: AES encryption is recommended by the National Institute of Standards and Technology (NIST) and the 256 bit AES / RIJNDAEL standard has been approved by the National Security Agency (NSA) for encryption of Top Secret documents.)

Transmission Security

Field2Base provides a unique, patented level of security on all transmissions regardless of modality: LAN/WAN, Internet, or Commercial Wireless. Any information (data) transmitted from Field2Base software is encrypted at 256 bit certificate to AES / RIJNDAEL standard (see above).

Summary

As the need for mobile availability of EPHI increases dramatically, it is important that HIPAA covered entities utilize Business Associates whose mobile technologies are compliant with HIPAA standards. Field2Base software is fully compliant with HIPAA Security and Privacy rules especially in the difficult area of transmission security utilizing commercial wireless systems, where all EPHI is encrypted to NSA Top Secret Standards.

Questions?

Any HIPAA entity concerned with meeting the February 17, 2010 HIPAA transmitting security requirement for mobile EPHI or for more detailed information on HIPAA compliance please contact one of our Sales Executives today.

Field2Base, Inc.
101 J Morris Commons Ln.
Morrisville, NC 27560

Phone: (919) 462-8500 Ext. 154
Fax: (919) 882-9980
Email: Sales@Field2Base.com