



# **New Whitepaper: Mobile Health and Security – Ten Questions you Should ask Before Implementing an mHealth Solution**

April 29, 2011

In today's healthcare regulatory climate, protecting personal information stored and shared through mobile healthcare (mHealth) solutions is becoming a big issue for healthcare providers, payers and vendors.

Diversinet Corp. has released an interesting white paper titled [Mobile Health and Security – Ten questions you should ask before implementing an mHealth solution](#). The document can help healthcare organizations better understand the rapidly evolving security requirements by outlining the most relevant HIPAA security rules and providing recommended best practices to address them.

*(Note: The whitepaper does require registration information to download.)*

The white paper starts with an executive overview that outlines the contents of the white paper beginning with:

This Mobile Health and Security white paper analyzes HIPAA security requirements and mobile health security best practices to assist healthcare organizations in evaluating and implementing secure and fully compliant mobile health solutions. The section on "HIPAA Security Requirements: Implications for Protecting Mobile PHI" reviews the HIPAA Security Rule Technical Safeguards for Protected Health Information (PHI) and discusses the mobile security best practices that directly relate to each Technical Safeguard.

[Diversinet Corporation](#) provides a patented and proven secure application platform that enables healthcare organizations to rapidly deploy HIPAA-compliant mHealth applications on mobile devices.