



### **Me4Sure Enterprise For The Healthcare Industry**

- Protects your medical record databases & IT infrastructure
- Meets and/or exceeds HIPAA compliance regulations
- Secures Electronic Protected Health Information (EPHI)
- Controls who, what, where, when and how users access your environment
- Offers a low cost, quickly deployed, user friendly authentication solution

Me4Sure's revolutionary biometric authentication solution, Me4Sure Enterprise, efficiently and effectively combats unauthorized access, fraud, theft and identity theft by providing superior authentication security.

Me4Sure Enterprise strengthens the way entities protect access to Electronic Protected Health Information (EPHI). With respect to remote access to or use of EPHI, covered entities should place significant emphasis and attention on their:

- Risk analysis and risk management strategies;
- Policies and procedures for safeguarding EPHI;
- Security awareness and training on the policies & procedures for safeguarding EPHI.

Me4Sure Enterprise is a biometric, cryptographically protected, portable USB drive. Unlike other security devices, Me4Sure features a secure, multifaceted, cryptographic communication process. The multi-layered authentication process ensures accurate, instantaneous verification and authentication of all authorized parties in every access based transaction.

- Stops unauthorized access, fraud, & identity theft on all transactions
- Eliminates all keystrokes, Usernames, Passwords, or PINs
- No need for the user to load software – Plug & Play
- World-class encryption, true multi-factor authentication
- Biometric single sign-on authentication
- Meets regulatory requirements
- Never transmits or exports fingerprint data
- Organizations can customize the device to meet branding requirements

In addition to protecting access based transactions, Me4Sure Enterprise device can function like a standard USB storage device when configured with additional memory. Unlike other USB storage devices, Me4Sure protects access to the stored data with biometric technology. Only the enrolled user can access the stored data. Even if the user

loses the Me4Sure device or someone steals it, the stored data is inaccessible and remains protected.

### **Encryption and Protection of Customer/User Identity**

The Me4Sure solution provides the maximum in user protection by digitizing and encrypting the enrolled data/fingerprint(s) and by storing this information only in the Me4Sure device. Me4Sure does not use external programs, software, or hardware in the storage and encryption process. The Me4Sure device and authentication process never exposes, transmits, transfers or exports the encrypted fingerprint data. The encrypted fingerprint data only verifies the user to that particular device.

### **Multi-level Authentication Process**

Me4Sure uses a multi-level verification and authentication process to ensure that each user has connected to an authorized entity before any transaction can begin. The Authentication Gateway (AG) issues random challenges that prevent any replay of prior transactions. This ensures that each response corresponds with the current random challenge and not with one previously generated. The biometric authentication process activates Me4Sure, and the corresponding transaction verifies the enrolled user's identity and authorizes the required authentication or payment/transaction.

### **Deployment of the Me4Sure Solution**

Deployment of the Me4Sure Solution requires little if any configuration changes to the client's IT infrastructure. This enables rollouts to occur in a matter of days, unlike other authentication platforms that usually take weeks or months. Me4Sure's Professional Services Group can install either a Gateway Architecture or an Adjunct Server Architecture Model to fully conform to and comply with each organization's IT standards.