



EzIdentity HIPAA Compliance and Strong Authentication

HIPAA Rules and Specifications

As the HIPAA Security Rule goes into effect, healthcare companies are coalescing around strong authentication as a best practice for remote access users. It is increasingly clear that passwords won't be adequate for a number of reasons. EZMCOM's EzIdentity provides benefits of two-factor authentication and beyond just for remote users.

Here are the HIPAA rule sections EZMCOM's Strong Authentication can help address:

164.308(b)(1) Business Associate Contracts and Other Arrangements	Required	If protected health information is shared with a business associate, assurances must be made that the information will be safe guarded.	EzIdentity provides cost-effective two-factor authentication to non-employees. EZMCOM's software approach means you don't have to ship a Hardware token to a contract cardiologist or a visiting /Consulting specialist, for example. Our software tokens support all the major operating systems, wired and wireless.
164.312(d) - Person or Entity Authentication	Required	Best practices are strong passwords for internal access and two factor authentication for remote access. WiFi and other types of wireless access should be considered remote access, even if they are inside the facility.	EzIdentity ensures strong authentication across internal and external access systems. WiFi or wired access of resources over a network is protected with 2 nd Factor authentication tokens.
164.312 (a)(1)(i) - Unique User Identification	Required	Each user needs a Unique Identifier.	Most entities probably already have this covered. EzIdentity provides an

			inbuilt directory service that can enable Unique user identification and association. Furthermore, EzIdentity allows a user to have multiple Hardware or Software tokens (say, one running on a PC and one on their IPHONE) - two separately identifiable tokens, one unique Username.
164.308(a)(3)(B) - Access Management	Addressable	Policies and procedures for access management must be in place	EzIdentity's allows propagation of a role implemented in a directory service based organization of users. This allows access only to those network assets that are appropriate for the said user.

EZMCOM can take the pain and hassle out of two-factor authentication. EZMCOM's EzIdentity can completely automate the provisioning process of authentication tokens. Further, EzIdentity can reduce your password-reset costs and is perfectly suited to non-employee strong authentication.

For more information, please contact us at sales@ezmcom.com

About Us

EZMCOM designs, develops, markets and supports identity protection products for the financial world, business and commerce over converging wired and wireless data channels.