



Enterprise Random Password Manager

Maintaining HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) was introduced as a reform to the healthcare industry in 1996. It establishes security standards to ensure the confidentiality, integrity, and availability of all electronic information about patients that healthcare organizations create, receive, maintain, or transmit. HIPAA has a significant impact on Information Security departments, as well as healthcare software vendors.

It is the responsibility of IT to maintain strict control over the sensitive data on critical systems. Compliance is at risk if security measures are compromised and patient data is lost or inappropriately disclosed. To comply with HIPAA's privacy and security initiatives an organization must:

- Ensure appropriate risk management
- Protect all IT assets
- Control access to confidential data

THE SOLUTION

With Enterprise Random Password Manager, you can generate unique administrator or root passwords for every system in your enterprise at regular intervals and allow delegated users to recover current passwords on demand via an audited web interface. It locates all accounts and every place the accounts can be used in the enterprise - including services, tasks, COM objects, IIS, and more. When a password change is implemented, Enterprise Random Password Manager updates the account information everywhere it is used.

You maintain fully audited control over which local passwords a user can access and for what length of time. You also have access to a historic audit trail of password changes.

Enterprise Random Password Manager helps organizations maintain compliance with HIPAA by providing:

HIPAA STANDARD	HIPAA REQUIREMENT	ERPM SOLUTION
Password Management	Implement procedures for creating, changing, and safeguarding passwords	Automatically and frequently generate unique, privileged passwords for every account
Unique User Identification	Implement procedures for identifying and tracking user identity	Create unique administrator accounts so users do not share a common account
Encryption and Decryption	Implement procedures to encrypt and decrypt access to data	Secure privileged passwords with AES-256 encryption of data in the database, and hardware-based encryption
Audit Controls	Record and examine activity in systems used for sensitive data access	Produce audit-ready reports showing privileged password changes and recoveries, and program logons
Access Authorization	Implement procedures for granting access through systems to private data	Grant only authorized users the ability to recover current local passwords
Termination Procedures	Terminate access to data when the employment of a workforce member ends.	Access to privileged passwords is temporary and can be revoked immediately.