



Ensuring HIPAA Compliance &
Cybersecurity for Healthcare



Protecting Electronic Protected Health Information (ePHI) with Advanced Encryption

With the latest HIPAA Security Rule Notice of Proposed Rulemaking (NPRM), healthcare organizations must strengthen cybersecurity measures to safeguard electronic protected health information (ePHI). WinMagic's SecureDoc provides enterprise-grade encryption and access control solutions that help covered entities and business associates achieve compliance while securing patient data against cyber threats.

Key Benefits of SecureDoc for HIPAA Compliance

Compliance with Encryption Mandates

The proposed rule requires mandatory encryption for ePHI at rest and in transit. SecureDoc ensures:

- FIPS 140-2 certified encryption to protect patient data on laptops, desktops, and removable media.
- Centralized encryption policy management for enforcing security across all endpoints.
- Data at rest AES-256 bit encryption to mitigate unauthorized access risks in case of device theft or compromise.

Strengthening Endpoint Security & Risk Mitigation

The NPRM highlights the need for vulnerability assessments, risk analysis, and penetration testing to combat cyber threats. SecureDoc enhances endpoint security by:

- Enforcing pre-boot authentication, ensuring user identity is verified prior to OS starting and before accessing any ePHI.
- Securing network-connected devices, preventing unauthorized access to healthcare systems.
- Reducing the risk of exposure by encrypting sensitive data across all endpoints.

Identity & Access Management (IAM) for Strong Authentication

With HIPAA's new requirement for multi-factor authentication (MFA) and immediate access revocation, SecureDoc integrates seamlessly with MagicEndpoint passwordless authentication to enable:



Zero Trust security, verifying both the user and device before granting access. In fact, we uniquely create a “user on device in real time” identity assuring that only the authentic user on the authentic device is granted access to online resources including access to ePHI.



Policy-driven access control, ensuring only authorized personnel following IT policies can access ePHI. In fact, we ensure that IT policies are adhered to in order to grant access. For example, if an IT policy exists whereby endpoints need to be encrypted for users to gain access to online resources, then MagicEndpoint will enforce this policy despite an authentic user on an authentic device being used.



Automated deprovisioning, ensuring revoked access is enforced within the mandated 24-hour timeframe. In the above case—if the user is not adhering to IT policies, they will automatically be denied access to all online resources including access to ePHI.

Data Recovery & Incident Response Compliance

HIPAA's proposed rules require organizations to restore lost data within 72 hours and implement strict security incident response plans. SecureDoc enables compliance by:



Encrypting backup data files to prevent breaches from stolen or lost media.



Supporting automated policy enforcement, ensuring secure data restoration.



Allowing secure and verified access to sensitive data during security incidents.



Why SecureDoc?

- **Proven Healthcare Compliance** – Trusted by hospitals, healthcare providers, and research institutions worldwide.
- **Seamless Integration** – Works with existing IAM, EHR, and security frameworks.
- **Zero Trust & Identity-First Security** – Protects patient data with advanced encryption and authentication.
- **Centralized Management** – Enforce encryption and security policies across all healthcare endpoints.

Ensure HIPAA Compliance & Strengthen Cybersecurity with SecureDoc and MagicEndpoint.

Contact us today to learn more!

sales@winmagic.com

1.888.879.5879

www.winmagic.com