We've got HIPAA covered.

In today's connected world of healthcare, you're right to be concerned about document security and HIPAA compliance.

As the methods used by hackers mature, healthcare data is now a high-value target. The cost of any type of breach—either electronic or human—goes beyond the direct cost of data loss and includes fines (up to $1.5m for each case) and penalties related to HIPAA violations. Sfax has been working with protected healthcare information since 1998, and Sfax employees undergo HIPAA training and assessment. Our customers can rest easy knowing that we HIPAA covered, so they can work confident.

HIPAA runs through everything we do

HIPAA privacy rule

The "Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) establishes regulations for the use and disclosure of an individual's Protected Health Information (PHI) held by 'covered entities' (typically clearing houses, employer sponsored health plans, health insurers and medical service providers). Sfax may be defined as a 'Business Associate' (BA). A BA is a person or organization that performs certain services for a covered entity involving the use and/or disclosure of PHI. When PHI is transferred from one computer to another, HIPAA security measures need to be implemented by the covered entity and BA.

According to the Security Standard Final Rule, a covered entity may permit a BA to create, receive, maintain or transmit ePHI on the covered entities behalf only if the BA obtains satisfactory assurances, in accordance with **45 CFR Part §164.305(a)** that the BA will appropriately safeguard the information.

Rest easy knowing that Sfax meets or exceeds requirements of both the HIPAA Privacy Rule and Security Rule. Sfax employees undergo HIPAA training and assessment. We also insist on Business Associate Agreements with anyone handling PHI. The following pages outline how we meet the standards on HIPAA security measures.

HIPAA security rule

A component of HIPAA is the "Security Rule", which includes technical safeguards which are defined in **445 CFR Part §164.304** and their implementation:

"Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

The Security Rule's technical safeguards do not mandate a specific technology solution but rather employ the adaptable requirement that an entity uses and as many security measures as are reasonable and appropriate.

Access control

"Access" is defined in § 164.304:

"Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."

The access control standard **§ 164.312(a)(1)** requires that a covered entity must:

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

Access controls are designed to provide the appropriate privileges to user accessing data, applications and files. The HIPAA Security Rule describes implementation specifications for the access control standard:

Unique user identification § 164.312(a)(2)(i). Assign a unique name and/or number for identifying and tracking user identity. Sfax ensures each user a unique identification name, allowing it to route information appropriately and track user activity. Identity is established during registration by requiring the following fields: name, address, office phone, mobile phone, industry, email address and password.

Automatic logoff § 164.312(a)(2)(iii). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Users of Sfax products have to enter their password (and PIN or other factors) after set periods of inactivity set by the admin, and every time the application is reopened.

Encryption and decryption § 164.312(a)(2)(iv). Implement a mechanism to encrypt and decrypt electronic protected health information. To protect sensitive health information from unauthorized access, we use industry-leading data protection and military-grade security policies combined with full 256-bit TLS encryption and 2048-bit private keys and AES multi-layered encryption for all documents and data, both at rest and in transit. In fact, we force the https:// standard for all desktop, mobile, web and API communication features, protecting from unauthorized access over wireless and wired networks.

Person or entity authentication

The person or entity authentication control standard **§ 164.312(d)** requires that a covered entity must:

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

To verify identity upon website access or mobile installation, Sfax authenticates with either login or registration. Existing user login requires a username and password. Access to secure messages can be further protected by a multi-factor authentication. During registration, identity is established by requiring the following fields: name, address, office phone, mobile phone, industry, email address and password.

Transmission security

The transmission security standard **§ 164.312(e)(1)** requires that a covered entity must:

"Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network."
There are two implementation specifications for the transmission security standard:

"Integrity controls § 164.312(e)(2)(i). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

"Encryption § 164.312(e)(2)(ii). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

Integrity

"Integrity" is defined in § 164.304:

"Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner."

The integrity standard **§ 164.312(c)(1)** requires that a covered entity must:

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

Sfax protects the integrity of electronic health information on its secure platform via end-to-end encryption and decryption of messages transferred over the TLS protocol. To protect against destruction, all messages are securely archived on a central server after encryption.

Audit control

The audit control standard **§ 164.312(b)** requires that a covered entity must:

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Sfax records and examines network activity to protect users, technical infrastructure and electronic health information from security violations.

We are Sfax.

© 2017 j2 Global, Inc. and affiliates. All rights reserved.
Sfax is a trademark of j2 Global, Inc. and affiliates.

For more information, please visit www.scrypt.com

Sales / Support: 1-877-493-1015