FixMe.IT
by Techinline

FixMe.IT HIPAA Compliance Guide

Remote Support & HIPAA Regulations

In today's era of technology, remote support software has become essential in many industries, including healthcare. The healthcare industry can benefit greatly from using remote support tools to maintain technical resources, however, like any other industry that involves transmitting sensitive data over the Internet, every healthcare organization should make the necessary steps to ensure that private patient information is kept and/or transmitted in a secure way.

For that, the Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, requires all healthcare organizations that store or transmit patient data to comply with specific technical, physical and administrative safeguards to ensure that this information is fully protected from unauthorized access.

About this Guide

The following guide is based on the HIPAA Security Standards rule (Technical Safeguards, section 164.312), which applies to remote support software, and is aimed at demonstrating how the FixMe.IT remote support application can help healthcare providers achieve HIPAA compliance. To view the complete list of HIPAA requirements with regard to privacy and security, visit the official website of the U.S. Department of Health and Human Services at https://www.hhs.gov/hipaa/for-professionals/index.html.

Please note that this document is for informational purposes only and is not to be considered as a legal advice regarding FixMe.IT's compliance with HIPAA regulations. We recommend that you seek the guidance of the appropriate legal counsel before relying on any of the statements contained below and making a purchase decision.

Terminology

Expert: A technician using FixMe.IT to provide remote technical assistance to clients.

Client: A remote user requesting technical assistance from a support technician.

Client ID: A unique 6-digit number generated by the FixMe.IT Client application that allows the Expert to send a connection request to the Client.

Addressable: A certain level of flexibility in taking steps to comply with the regulation is allowed.

FixMe.IT & HIPAA Security Standards

§ 164.312(a)(1) – Access Control

HIPAA requirements:

- *Required:* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.
- *Required:* Assign a unique name and/or number for identifying and tracking user identity.
- *Addressable:* Implement a mechanism to encrypt and decrypt electronic protected health information.

Support in FixMe.IT:

- All FixMe.IT remote support sessions must be initiated by the Client. The Expert cannot establish the remote connection until provided with a unique Client ID generated by the FixMe.IT Client application.
- Permission-based access control model ensures that the Client always stays in control of what's happening on their side and can override remote control or terminate the session at any point.
- The Expert must log in using a strong password and email address to access the Expert Console of the FixMe.IT application.
- The optional two-factor login process requires the account holder's username and password as well as a virtual token sent via email, which must be provided upon login, and thereby provides an additional layer of account security.
- All sensitive data transmitted during the FixMe.IT remote support session is fully protected with the RSA public/private key exchange and 256-bit SSL/TLS encryption technology.
- A unique encryption key is generated through the server handshake at the start of each session. The FixMe.IT servers route only encrypted data packets and do not have the session encryption key. This means that the data transferred between the Client and the Expert cannot be altered or intercepted by any third party.

§ 164.312(b) – Audit Controls (Required)

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

Support in FixMe.IT:

- Session activity (including start/end time of session, IP addresses of participants, the amount of transferred data) is logged for security and auditing purposes. All session logs are securely stored in an encrypted database.
- Every remote support session can be recorded for security and quality-of-service purposes.
- The Expert Console of the FixMe.IT application provides IT administrators with quick access to both session logs and video recordings.

§ 164.312(c)(1) – Integrity Policies & Procedures (Addressable)

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

Support in FixMe.IT:

- Permission-based access control model ensures that the Client can terminate the session at any point.
- If the remote control operation has been authorized, the Client can always see what's happening on their screen and override remote control at any time.
- In case unattended access is installed on the Client's computer, the Client can always abort the unattended connection by clicking on the FixMe.IT icon in the Windows system tray and choosing the corresponding option.

§ 164.312(c)(2) – Integrity Mechanism (Addressable)

Implement methods to corroborate that information has not been destroyed or altered.

Support in FixMe.IT:

- All data transmitted between the Expert and the Client during the remote session is fully protected with the RSA public/private key exchange and 256-bit SSL/TLS encryption technology.
- All data is transferred only between the Expert and the Client and leaves no footprint anywhere in the middle.
- Session video recording can show if any data on the Client's computer was affected during the session.

§ 164.312(d) – Person or Entity Authentication (Required)

Verify that the person or entity seeking access is the one claimed.

- All FixMe.IT Experts are authenticated using an email address and a strong password, which is protected with salted cryptographic hashing and stored in an encrypted database. The use of individual salt characters eliminates the risk of common password theft even in the event of a major attack.
- The optional two-factor login process requires the account holder's username and password as well as a virtual token sent via email, which must be provided upon login, and thereby provides an additional layer of account security.

§ 164.312(e)(1) – Transmission Security

HIPAA requirements:

- *Required:* Protect electronic health information that is being transmitted over a network.
- *Addressable:* Ensure that protected health information is not improperly modified without detection.
- *Addressable:* Encrypt protected health information whenever deemed appropriate.

Support in FixMe.IT:

- All data transmitted between the Expert and the Client during the remote session is fully protected with the RSA public/private key exchange and 256-bit SSL/TLS encryption technology.
- At the end of the session, no data or software is left on the Client’s computer.
- The information transferred between the Expert and the Client leaves no footprint anywhere in the middle, which means that there is no risk of transferring sensitive information to a third party, as it will be entirely disregarded from all points at the end of the session.

FixMe.IT HIPAA Compliance FAQ

Q: Is FixMe.IT HIPAA compliant?

FixMe.IT is not directly subject to HIPAA compliance. Health Insurance Portability and Accountability Act implies that healthcare organizations are the only entities that must comply with the regulations, however, any software tools (including remote support applications, such as FixMe.IT) should be thoroughly checked for compliance in the context of their security capabilities prior to deployment.

FixMe.IT's extensive set of communication security features along with its permission-based access control model and optional two-factor authentication make it suitable for remotely supporting clients in organizations subject to HIPAA compliance.

Q: What personal data does FixMe.IT collect and/or store?

FixMe.IT only collects Personally Identifiable Information (PII) and information required for accounting, billing, and reporting purposes such as session start/end time, IP addresses of session participants (Expert and Client), and the amount (in bytes) of transferred data.

All temporary information used or transferred during the session is temporarily stored in the server's operating memory without anyone having access to this information. Once the data is transferred from one session participant to another, it is entirely disregarded from the operating memory. Once the session is terminated, all temporary data is entirely disregarded.

No other personal data, including any personal health information related to the session participants, is stored by the FixMe.IT application.

Q: What is Techinline doing to help customers meet HIPAA requirements?

Techinline is providing customers with extensive information about the security capabilities of the FixMe.IT remote support application. To see the complete list of the product's security features, download the FixMe.IT Security white paper. Besides that, Techinline's sales department is always available by phone or email to provide assistance regarding HIPAA compliance.

Q: How can two-factor authentication be enabled within FixMe.IT?

Two-factor authentication is an optional, free feature that comes with any purchased FixMe.IT license. To enable two-factor authentication for your account, simply send an email request to the Techinline sales or support team, and it will be set up within 24 hours or less.

Contact information

Please forward any questions or concerns to the appropriate email address:

For general enquiries and suggestions, website, feedback and other proposals: info@techinline.com

For order quotes, pricing information, product enquiries and personal demos: sales@techinline.com

*You may also contact the Sales Department to learn more about the FixMe.IT remote desktop application. We will be happy to answer any of your questions, as well as provide a personal demo of our software.

For any technical issues: support@techinline.com

For questions or concerns about an existing FixMe.IT account: orders@techinline.com
We guarantee to respond to your request within 24 hours!

You can also contact a live representative regarding any issue:

Phone: US & Canada: 1-617-934-2771

United Kingdom: +44 (0)20 8144-7131

Skype: techinline

Useful links

Official website: https://www.techinline.com/

Overview of FixMe.IT security features: https://www.techinline.com/Security

FixMe.IT Support Center: https://docs.fixme.it