Top 8 Secure Messaging Policy Best Practices

INTRODUCTION

Text messaging via mobile devices has become a general means of communication within our culture and workplace. However, traditional text messaging methods have severe security limitations because the sender cannot be assured of the privacy and confidentiality of sent messages. This risk poses an even greater threat in business organizations where federal and state privacy regulations require that all client information remain confidential.

Secure text messaging solutions are currently implemented to help ensure that client data transmitted via text messages is done in a manner that complies with the organization's compliance standards. Accordingly, solutions may include features that delete text messages from both the sender's and the receiver's devices, authenticate users under the facility's policies, and offer a method to archive and audit all sent messages. With the implementation of a solution, facilities should maintain a Secure Messaging Policy to oversee usage and security of their solution.

THESE BEST PRACTICES HELP ENSURE THAT YOUR SECURE MESSAGING POLICY OUTLINES:

- Staff usage of the solution
- Transmission of secure information
- Integration with company policies

RECOMMENDED GUIDELINES

In order to ensure client information is kept secure and to help oversee staff usage of a solution, facilities are recommended to implement these top 8 components into their Secure Text Messaging Policy:

1. Secure Messaging must be used by all staff members when sending text messages that contain confidential information such as social security numbers, financial records or PHI (patient health information).

2. All data transmitted via Secure Messaging is the business' sole property. Accordingly, the corporation has an absolute right of access to all of the data sent via the solution and may exercise its right whenever it is deemed appropriate by staff management.

3. Pictures, video, voice files, and other files must be sent within the Secure Messaging application. In no situation are you permitted to use the local storage on your device.

4. Company policy prohibits screen capture or sharing confidential client information with users who are not bound by the company's Privacy Policy.

5. Secure Messaging is only functional when the user's mobile device is connected to the Internet. As such, the solution may not be appropriate in emergency situations or where Internet access is inconsistent or delayed.

6. When and where you may use your mobile device is subject to the organization's general policy covering the usage of mobile devices. Use of mobile devices near certain equipment, or in certain areas of the facility, may be prohibited.

7. Use of Secure Messaging for personal purposes is subject to the facility's general policy covering the personal use of company email accounts. This includes the disposal or sale of your personal device, which should be done in a manner only after you've fully removed the Secure Messaging application from your mobile device.

8. If your mobile device is lost or stolen you must notify your supervising staff immediately so that the data stored in yourSecure Messaging account can be remotely wiped from that mobile device.

CONCLUSION

Mobile device usage in the workplace may optimize staff communication and workflows, but organizations must keep security and compliance an immediate priority. Implementing a Secure Messaging Policy allows employees to use their mobile devices while maintaining security through guidelines that monitor staff usage, security standards and best practices for integration with employee workflows. Even with a Secure Messaging Policy, businesses should make sure to regularly update their policies to parallel with technological updates and changes in staff usage. Always make sure that your policy reflects the key benefits and security concerns for your facility. If questions arise about how to properly use your solution alongside the policy, staff members should follow up with the appropriate company staff member in charge of implementing and maintaining the secure text messaging solution.

ABOUT TIGERTEXT

As healthcare's largest provider of clinical communication solutions, TigerText helps physicians, nurses, and other staff communicate and collaborate more effectively, accelerating productivity, reducing costs, and improving patient outcomes. With 6,000 facilities, 99.99% uptime, and over 10 million messages processed each day, TigerText continually delivers advanced product innovations and integrates with critical hospital systems such as the EHR, nurse call, and scheduling solutions. The company's commitment to client success is reflected in its broad support organization that works directly with clients at every stage to streamline communication workflows and achieve the highest possible ROI.

CONTACT US

Call Us:
310 401 1820

Email Us:
sales@tigertext.com

On the Web:
tigertext.com

Follow Us on Twitter:
@TigerText

Connect With Us on LinkedIn:
linkedin.com/company/tigertext