5 Key Questions to Address for a Successful Secure Text Messaging Implementation

Intro

With the growth of BYOD in the workplace organizations have turned to Secure Messaging to solve the security issues surrounding the use of personal devices in the workplace. Healthcare facilities turn towards the same solution, with HIPAA regulations in mind, to readily provide an optimized form of communication without risking patient information. With the selection of a solution, healthcare organizations will need to clearly outline their goals and implementation steps to ensure efficiency.

The purpose of this document is to help healthcare facilities ensure a well-organized and successful implementation. Evaluate your Secure Messaging solution and your implementation process with these key steps in mind:

1. Know who will lead the implementation process
2. Define why Secure Messaging benefits your facility
3. Determine how the solution will integrate with existing procedures
4. Plan what the key implementation goals and dates are for your facility
5. Identify your facility’s next steps after implementation is complete

1. Who will lead the implementation process?

Identify the key members of the Implementation Team to ensure a smooth transition for key departments:

- Who is the ideal Project Manager?
- Who will be the clinical lead for implementation?
- Who will be the point of contact for IT integration?

2. Why will Secure Text Messaging benefit your facility?

Outline the goals of this solution to prioritize the implementation process:

- What drivers brought Secure Messaging to your organization?
- What needs does this solution meet?
- What is your ideal activation date?

Describe how the solution will optimize current hospital workflows:

- How are you currently communicating?
- Who needs to communicate or will use the solution?
- How can Secure Messaging benefit and enhance your current workflows?
3. How will Secure Text Messaging integrate with existing procedures?

Discuss how the solution will synchronize with current hospital technologies:

- What Wi-Fi Networks will be accessed?
- Which Ports will be opened?
- Is Firewall access necessary?
- How will application support be coordinated?

Distinguish how Secure Text Messaging will be provisioned:

- What types of messages will staff send with Secure Messaging?
- Who will be using the solution?
- Who needs access to a Secure Messaging solution?
- Will there be restricted access for specific users or departments?
- What resources are available to create awareness of the solution?

Incorporate applicable policies or regulations:

- Which compliance standards should the solution follow?
- How are personal devices currently managed in the workplace?
  - Does the organization use a Secure Messaging Policy?
  - Does the organization use a BYOD Policy?

Tip: If you do not currently have a BYOD or Secure Text Messaging Policy, we recommend implementing these guidelines to ensure proper use of personal devices.

4. When are the ideal dates for implementation and Key Goals?

Map out timeline leading to integration of the solution:

- What are ideal milestones leading to completion?
- How long will it take to get all users on board?
- What training materials will staff utilize?
- What is the Training Schedule and Plan?
- How is the support model determined? Is there Help Desk training?
5. What will happen once implementation is complete?

Answering these questions will help healthcare organizations prepare for the integration of Secure Text Messaging at their facility. Once this road map is complete, the implementation team should collaborate with their solution’s Point of Contact to discuss time frame to launch and next steps. Even after installation is complete, facilities should continue to provision users and schedule a post-activation review and revisit to keep staff up to date and their provider aware of their usage.

Ensure that there is always a line of communication between your organization and your solution provider. This will increase the ease of use and allow for additional assistance if needed.

Company Profile

TigerText is the #1 leader in secure, real-time messaging. TigerText allows enterprises to create a private and secure mobile messaging network with their employees’ smartphones. This controlled platform is HIPAA compliant and replaces the unsecured SMS text message that leaves protected health information and other confidential data at risk. The speed, compatibility, and ease of TigerText increases workflow and employee satisfaction. Users can communicate from any computer or smartphone with key features that include an integrated company directory, delivery and read notifications, user controlled message lifespan, group messaging, and file sharing. For more information on how to get TigerText set up with your enterprise.

Contact Info
Phone: 310-401-1822
Email: sales@tigertext.com
www.tigertext.com

For more information visit us at:
http://www.tigertext.com or
http://developer.tigertext.com

Like us on Facebook
facebook.com/TigerText

Follow us on Twitter
twitter.com/tigertextapp