Ten Questions to Consider When Implementing a Secure Message Center Within Your Customer Portal

The insurance, financial services and healthcare industries work with regulated information as part of their core business process. Because of this, customer portals and support services for members, account holders or patients are more complicated than other industries due to security and privacy regulations surrounding the sensitive information, be it identity, financial or health information. Support services delivered via web and app-based messaging and email channels must be encrypted, logged and tracked for compliance purposes.

For that reason, organizations in these sectors should implement a Secure Message Center on their web properties. When implementing a secure message center (SMC) for a website or customer services portal, what questions should you be asking yourself? In our experience – it's all about understanding the support inquiry workflow end-to-end. Below are 10 questions to consider, and some insight based on our experience implementing them. For simplicity in the guidance provided, we use 'customers' to describe all prospective and current financial services clients, insurance subscribers, patients, clinicians etc. Likewise, anyone in your organization supporting or communicating with customers are labeled 'employees'.

Question Number One

Who needs to use the secure message center and why?

Customers visiting your web properties to get information or utilize self-service resources should be provided various ways to contact your employees when they need help. That's an obvious statement, yet many organizations limit the support options to telephone contact and snail mail or restrict email correspondences to non-sensitive topics (thru disclaimers and warnings). To provide a better level of service and support, a SMC should be implemented to enable the exchange of

sensitive information throughout the message string with the employee using encryption and access permissions.

Question Number Two

Where should the secure message center be located?

The SMC should be readily accessible (and easy to use). If customers visiting your public website(s) need to engage your employees and share regulated information, you may need to provide access points from a public webpage. For customers with login credentials to a secure customer services portal, locating the SMC where it can be accessed from anywhere inside the portal is best. In other cases where high volume, specific requests or service issues are handled, customized SMC fields or forms specific to content on a webpage can be more effective and provide structured data to your backend enterprise applications.

Question Number Three

How should secure message center users authenticate themselves?

A SMC requires customers to identify themselves, and password protect the information exchanged for security and compliance purposes. If the customer is a new visitor on a public webpage – they will need to authenticate by creating an account (email and password typically), or you could leverage their public ID providers to make it easier for them (ex: Google, LinkedIn, Facebook, Microsoft). If the customer is already logged into a secure portal with existing credentials, the secure message center should leverage those credentials through enterprise SSO techniques such as OAuth, or other IdP techniques, eliminating the need to re-authenticate or create separate credentials for your SMC. No one wants to log in twice or maintain separate credentials to access secure messaging for support.

Question Number Four

What type of inquiries are expected?

Secure message centers are meant to provide a safe and secure method of transmitting sensitive information and should be advertised as such. Awareness of SMC functionality is important to user adoption. Once the customer knows that it's meant for sensitive communications, then all types of inquiries are to be expected—such as customer support inquiries to issues with mobile finance/banking to questions about a customer's account. You should expect the same variety of inquires that come through your current support or service channels.

Question Number Five

Do customers or employees need to share files or other message attachments?

Depending on the type of inquiries, file attachment features may be needed to support the inquiry or resolve an issue. Sharing smartphone photos and screenshots is often required. In some cases, you may need the ability to handle very large file attachments such as videos or diagnostic images.

Question Number Six

Can the inquiries be categorized for efficient routing?

If a customer exists in your database, routing their inquiry to a specific employee tasked with managing their account may make sense. In other cases, you may want to route the inquiry to your subject matter experts, or groups tasked with specific business processes, product or services. Here are various ways you can route inquiries from the SMC:

- Customer – by email address, name or an account number

- Topic – by picklist in the SMC webmail user interface
- Topic – by content filter once the message is sent (keyword routing)
- SMC – unique SMCs can be placed on different areas of the website or portal and messages can be routed to responsible employees accordingly

Question Number Seven

Who will respond to the inquiries and what application will they use?

Routing techniques above help distribute inquiries to the appropriate teams as needed, and backend applications should identify available employees within teams. Is it a support issue? Send it to customer service/support team. Is the customer asking about their account? Send it to an advisor. Asking about a specific product or service, send them to appropriate sales team.

It's important to consider the backend application your employee uses to receive and respond to the inquiry. Depending on their role, they may work in a CRM system, a contact center application, a support ticketing system, or a standard email client like Outlook. In some environments, there may be a custom database application specific to the business process.

Regardless of the application they use, a secure messaging solution should integrate the messaging workflows into the UI and application for best results. Generally, if the application supports standard email protocols, your SMC solution should enable your employees to send and receive easily, often with case tracking and archiving for the entire message string. In some cases, APIs can be used to improve the integration and seamless handoff of the message, files and metadata.

Question Number Eight

What type of reply notifications do customers need?

When an employee responds to a customer inquiry from a SMC, how should the customer be notified? In most cases a simple email notification with a link to the message center inbox will suffice. In other cases, and where other contact information is available, (phone numbers, mobile phone numbers), that may be supplemented with notification types such as a text messages or an automated voice message. These supplemental techniques ensure the customer gets a timely notification of the employee response.

With advanced SMC response techniques – the reply, including related file attachments as needed, can be sent securely right into the customer's personal email inbox. This simplifies the messaging process and enhances satisfaction with the inquiry engagement and resolution.

Question Number Nine

Is a custom user interface desired, or is a standard webmail interface sufficient?

Depending on your specific use case, the SMC may benefit from your own web design and UI implementation, specific features exposed or hidden, or structured data fields beyond the tradition 'to' 'from' and 'subject' lines. In this case you'll need an SMC platform with a robust set of secure messaging APIs, including runtime functions, provisioning and management of the message center functions. APIs are also required if a SMC function is implemented in a corresponding mobile app for customers.

If a standard webmail interface is sufficient, your SMC provider can likely provide you an interface with your own branding at a minimum, and some other 'on/off' feature selections such as drop-down 'to' fields for routing, file

folders and other minor send/receive features enabled or disabled. This approach minimizes web development and accelerates the implementation time for the SMC.

Question Number Ten

What type of management and reporting tools are needed?

When it comes to a SMC solution, the message traffic must be logged and tracked to support a compliance audit or other inquiry to prove that a message and file exchange has met security and compliance policies and laws. Detailed message metadata can also be used to identify usage trends by any field (sender, recipient, date, time, subject, attachment name, etc.). Optimally, the content of messages and file attachments should be inaccessible to anyone outside of the sender and recipient also to support security and compliance policies. If e-discovery is needed, a separate (and secure) archiving solution can be used with the SMC.

For reports on message handling rates, inquiry resolution and other employee productivity levels, corresponding CRMs, ticketing systems or contact center solutions are designed specifically to deliver this data and should be leveraged for those type of reports.

About DataMotion

DataMotion provides secure data delivery solutions such as encrypted email, file transfer, forms processing, customer contact and Direct Messaging. By using DataMotion, businesses can safely and easily exchange email, files, and other information with partners and customers from anywhere to anywhere. Our easy-to-use solutions leverage a core, secure platform for unified data delivery that can also be integrated into almost any workflow or system. All our solutions apply military grade encryption to your data in motion, including those sent from mobile devices, allowing them to remain secure, and to support your regulatory compliance objectives.

www.datamotion.com 200 Park Place Suite 302 Florham Park New Jersey 07932 800-672-7233