DataMotion

HIPAA-Compliant Secure Information Exchange for Salesforce®

Salesforce is the Customer Relationship Management (CRM) software of choice for many organizations that perform large-scale sales and customer support operations, claiming the top market segment share for the 3rd straight year according to market research firm Gartner. Many enterprise-class organizations rely on Salesforce to accomplish the bulk of their daily sales and customer support e-communications and workflows.

Within the healthcare and life sciences industry - health insurers in particular - Customer Services Representatives (CSRs) and other CRM users often use the email functionality built into Salesforce to communicate with subscribers for workflows such as email-to-case. This activity may involve exchanging sensitive subscriber information that qualifies as personally identifiable information (PII) and protected health information (PHI) protected by HIPAA privacy and security regulations. Any form of a breach involving this data could cause substantial and costly damages to subscribers and the healthcare enterprise.

While the need to protect PHI, PII and other sensitive information emailed in and out of Salesforce can be addressed by using the opportunistic TLS (Transport Level Security) protocol - a built-in function of Salesforce - there is no guarantee that a recipients email environment will always support TLS. This may result in delivery failures - or even worse, unprotected delivery of sensitive data with all related risks and liabilities.

Solution

The issue of ensuring HIPAA compliance when exchanging sensitive information using Salesforce is best addressed by integrating a secure messaging solution that guarantees encrypted exchange with both mobile and non-mobile interfaces. Additionally, content filtering and related features such as Data Loss Protection (DLP) and de-identification are available as needed. This document describes integrated solutions for Salesforce using DataMotion SecureMail and APIs, and illustrates some secure information exchange use cases between Salesforce users and their customers.

Integration Methods

The integration of HIPAA-complaint secure information exchange into Salesforce using DataMotion SecureMail can be accomplished via user interface (UI) or API:

- Integration into Salesforce can be provided via the Salesforce UI, or via an application written to the Salesforce SDK.
- Integration with SecureMail can be provided via the DataMotion SecureMail web portal UI, or via an application written to the DataMotion Web Services APIs.

The tradeoffs are typical: integration via UI involves less customization effort and time, but offers less flexibility, and vice versa. Both methods can be applied independently on the Salesforce and SecureMail sides, e.g. UI integration with Salesforce can be combined with API integration with SecureMail with one caveat: when it comes to mobile applications, API integration is required in order to use a mobile app on either side.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: sales@datamotion.com www.datamotion.com
DataMotion, Inc. 200 Park Ave Florham Park New Jersey 07932

The following sections provide descriptions and illustrations of secure information exchange use cases with both UI and API integration methods.

Use Case 1: Securely sending information out of Salesforce

An employee of a health insurance company needs to send a document to a subscriber using Salesforce as a CRM. Sensitive health information is contained within this document that is normally communicated via direct phone call to the subscriber for privacy reasons. These phone calls can be time consuming, and inhibit the rate at which the employee's daily tasks can be accomplished.

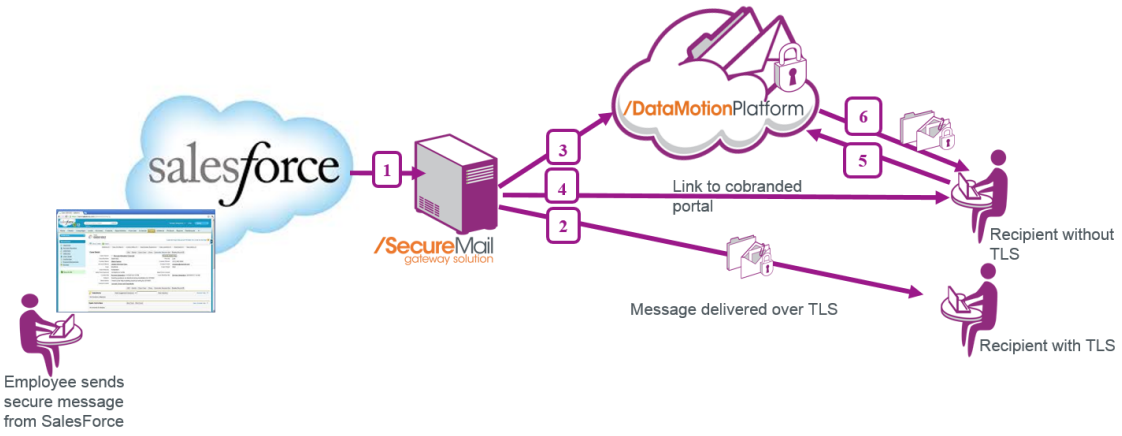

Fig. 1. Sending sensitive information from Salesforce via SecureMail

In this example, integration with Salesforce and SecureMail is accomplished via the respective web portals of both services. The DataMotion SecureMail Gateway (server software) shown in the diagram performs the role of a content filter that inspects the content of outgoing messages and determines if they need to be sent securely or if any of the data inside the messages needs to be de-identified. All outgoing messages are routed through the SecureMail Gateway, which is deployed in a private or public cloud as virtualized server software.

When the employee (CSR) sends a secure message via the Salesforce web portal (step 1), a check is performed by SecureMail to determine if the intended recipient of the message accepts TLS delivery. If the recipient does accept TLS, then the message sent by the CSR arrives in the recipient's inbox protected via TLS encryption (step 2). If TLS delivery is not an option, the message is routed for encryption on the DataMotion SecureMail platform (step 3) and the recipient receives a notification email with a link to the DataMotion SecureMail web portal (step 4), where they can securely retrieve the message with a simple login (steps 5&6).

Use Case 1 requires the least amount of customization of both Salesforce and DataMotion SecureMail.

Use Case 2: Email-to-case from a mobile app into Salesforce UI

An insurance company subscriber is on the road and needs to make a quick request regarding a recent claim. The subscriber only has access to a smartphone at the time.

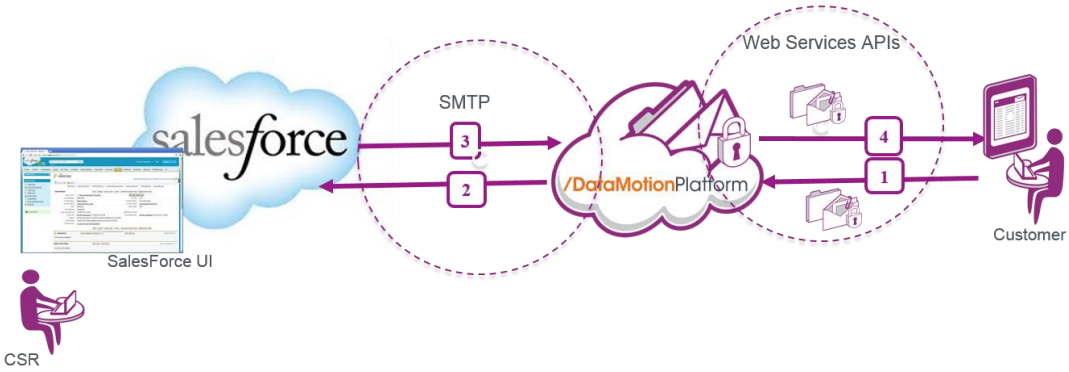

Fig. 2. Salesforce email-to-case integration with a mobile app using SecureMail APIs

In the use case illustrated in Fig.2, the subscriber initiates an email-to-case transaction with a insurance company CSR from the insurers mobile app (step 1). Driven by DataMotion Web Services APIs, the message gets delivered securely via the DataMotion Platform into Salesforce (step 2), where the message is replied to by the CSR with the Salesforce Thread ID embedded in the message (step 3). The message is then delivered securely to the customer's mobile device via the DataMotion platform (step 4). In all subsequent correspondence, the Thread ID is preserved inside the message so Salesforce can track it.

In Use Case 2, integration with Salesforce is accomplished via its web portal UI because it provides all the required functionality. In order for the subscriber to use the insurers mobile app to exchange claim information securely, integration with SecureMail is accomplished via the DataMotion Web Services API – it's an encrypted connection so there is no concern about TLS delivery into the customer's mailbox.

Use Case 3: Email-to-case from a mobile app into Salesforce app

This use case is similar to the one described above, except that the insurance CSR is provided with a custom application developed to the Salesforce SDK due to specific requirements that cannot be addressed by the Salesforce UI.

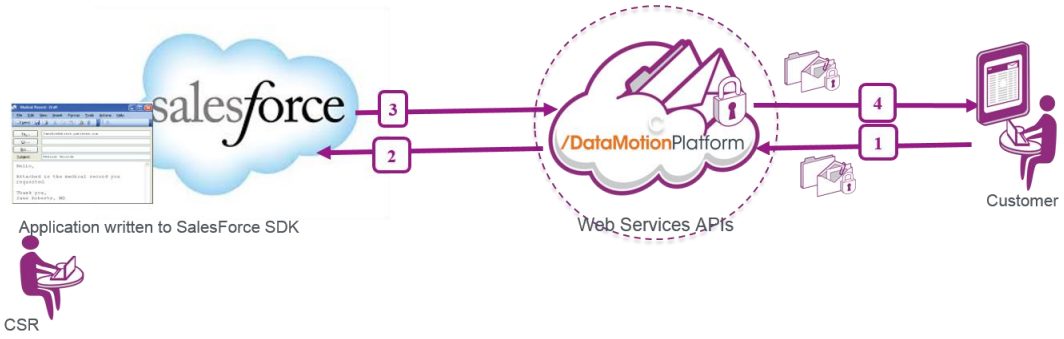

Fig. 3. Salesforce email-to-case integration with a mobile app using SecureMail APIs and Salesforce SDK

The sequence of steps for this use case is similar to the one described in Fig. 2, except that the Salesforce integration is handled by the application developed to the Salesforce SDK to satisfy the CSR workflow and client requirements.

Summary

The need for HIPAA-compliant secure messaging integration with Salesforce is driven by the ever-increasing demand for compliance with HIPAA privacy and security regulations for protecting PHI, PII and other sensitive subscriber information. Such integration is easily achievable in a variety of ways via DataMotion SecureMail and DataMotion Web Services APIs. The available integration methods can satisfy the needs of Salesforce healthcare and life sciences customers to facilitate the workflows and enable interactions on subscriber mobile or desktop endpoints.

ABOUT DATAMOTION

Since 1999, DataMotion secure data delivery technology has enabled organizations of all sizes to reduce the cost and complexity of delivering electronic information to employees, customers and partners in a secure and compliant way. Ideal for highly regulated industries, the DataMotion SecureMail portfolio offers easy-to-use encryption solutions for email, file transfer, forms processing and customer-initiated contact. In the healthcare sector, DataMotion is an accredited HISP (health information service provider) of Direct Secure Messaging. The DataMotion Direct service enables efficient interoperability and sharing of patient data across the continuum of care. DataMotion is privately held and based in Florham Park, N.J. For the latest news and updates, visit http://www.datamotionhealth.com, follow DataMotion on LinkedIn or Twitter® @datamotion.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: sales@datamotion.com www.datamotion.com
DataMotion, Inc. 200 Park Ave Florham Park New Jersey 07932