Data Security in Communications for the Healthcare Domain

Renuka Kulkarni

Independent Researcher
USA
Renukak12@gmail.com

Abstract

Customer communication management (CCM) software tools are designed to create and deliver personalized, multichannel communications. They provide customers with a secure, cost-effective, efficient, and reliable solution for managing customer communications. CCM tools fit into the customer engagement needs of any domain, be it insurance, banking, utility, or healthcare. This article will examine how security protocols are applied in Customer communication tools for composing and delivering communications in a secure healthcare environment.

Keywords: Customer communication, Security, Healthcare

Introduction

Customer Communication Management (CCM) platform empowers organizations to create, manage, and deliver personalized and consistent communications across various channels. It is widely utilized for generating customer-facing documents such as correspondence for healthcare communications, billing statements, invoices, marketing materials, and other types of customer-related documents. When deploying solutions within the healthcare domain, several key considerations must be considered during the design and implementation of the CCM product.

Customer Communication Management (CCM) and Data Security are closely related. Businesses must ensure that personal customer data used in communication is protected from various security threats, such as unauthorized access and misuse. Strong data security practices are essential to maintaining customer trust, regulatory compliance, and overall business integrity.

Problem statement

Healthcare organizations interact with patients and healthcare providers through various channels such as letters, faxes, email, and SMS. However, many data breaches occur in the healthcare domain, which involve incidents where sensitive and critical patient data is accessed or disclosed to unauthorized personnel. These occur when the healthcare data used for managing communications is not secured correctly. These breaches can create severe consequences for patients as well as healthcare organizations. Taking preventive measures in the context of CCM to protect sensitive data can avoid potential risks and help organizations avoid the risks of data breaches.

Solution

Data Security Measures in Healthcare

CCM tools interact with sensitive data, including Protected Health Information (PHI) and Personally Identifiable (PII) within the healthcare domain. To ensure secure data transfer, it is essential to implement robust measures for handling data at the input and output stages. CCM enforces security through a

combination of administrative controls, user authentication, data encryption, and compliance with industry standards, ensuring the integrity and confidentiality of sensitive information. The details below focus on various key security mechanisms implemented while handling healthcare data.

Real-time OnDemand processing with SSL (secure socket layer) protocol

The CCM tools are designed to facilitate the creation of personalized communications by processing input data and composing output messages by using a core processing system. This processing system, called the executable, is responsible for merging data and template skeletons to create customized communications. This processing system is referred to differently based on different communication system tools. The core processing system's flexibility allows it to operate in two distinct modes depending on the need for customer data quantity and the processing of data needs.

Batch mode and an On-Demand mode

Batch Mode: Batch mode is suitable for processing large datasets and is ideal for generating large quantities of communications that follow a scheduled or periodic processing cycle (e.g., monthly billing statements and mass customer notifications). Generally, batches are scheduled for execution from each subsystem participating in the flow; in this method, the CCM process is also takes part in execution flow and is only invoked based on the batch schedule to create customer communications.

On-Demand Mode: This is dynamic and uses real-time processing. This method keeps the composition core process running to handle ad hoc requests as data is received. The process keeps listening to message queues for incoming data. This enables real-time communications to address specific user requests or immediate events (e.g., personalized customer service replies or medical records processing). In this method, there is no batch schedule predefined by a scheduler, as processing happens in an ad-hoc manner.

In OnDemand mode, the data comes from the message queue. Secure Data Transfer is achieved with the help of the Secure Sockets Layer (SSL) protocol to complete data transfer with security. For instance, when a patient authorization is approved, data from the front end is transferred to the queues in XML format, and the CCM process, which keeps on spooling to the queue, receives customer data and generates approval communication for the patient. In this scenario, both input and output are read and written to the queues using SSL protocol to ensure that patient data is kept secure. Introducing SSL parameters in configuration provides encryption for data in transit, ensuring that sensitive information is protected. Prevents unauthorized access or tampering during data exchange. Enforces authentication between components

Using message queue connector:

CCM tools are integrated with a Message Queue Connector to facilitate secure, real-time communication without relying on a file system for data processing or storage. This setup is particularly beneficial in environments with strict data security and compliance requirements, such as federal healthcare systems. Details of workflow and benefits are explained below.

Message Queue Connector acts as a bridge between external data sources and the CCM tool. It utilizes JMS (Java Message Service) for secure, asynchronous, or synchronous data transfer. Data from external systems is pushed into input queues, where the system retrieves and processes input data, creating customer communication outputs. The processed communication is sent back to output queues for further distribution. This architecture provides Security; it ensures data is transferred securely through JMS with support for encryption, authentication, and reliable message delivery. Data transfer through the Message queue connector reduces the security risk associated with file storage and unauthorized access. JMS can handle

high volumes of data, providing reliable communication. This transfer enables seamless integration with diverse IT infrastructures and platforms.

Supported Platforms:

Linux (Red Hat): Common in enterprise environments for stability and performance.

Mainframe (z/OS): Essential for high-throughput, transaction-heavy systems.

UNIX (AIX, HP-UX, Solaris): Known for reliability in mission-critical operations.

Windows: Provides flexibility for development and deployment in mixed environments.

In the case of the Federal healthcare domain, On-demand processing is preferred to add an extra layer of security.

Web services with HTTPS protocol:

CCM references data outside the organization or network to access customer information that is unavailable on the primary input. These optional data file objects are indexed, which enables retrieving supplementary customer or external data from systems outside the immediate environment.

Reference file objects are particularly advantageous when managing frequently changing information. Rather than updating each customer's details within the input or modifying application logic, data can be updated in a single location, automatically applying to all customers who meet the specified criteria.

CCM tools rely on the HTTPS protocol to ensure secure and encrypted data transfer when accessing reference files stored on external systems. CCM sends a request to the website using a request in Web Services Description Language (WSDL), which contains key parameters to access the required data for referencing external content and, as a response, if a valid request is made, receives the data needed as a response in the reference file. Using HTTPS protocol for such APIs provide secured data transfer.

Using the Security group to access documents

Newer versions of CCM tools provide editing functionality for business users. This feature allows business users to focus only on areas of communication they have permission to edit, ensuring the right message is delivered and communications stay compliant with company and legal guidelines for sophisticated document editing requirements. This facility allows business users to add last-minute updates to communication, making it more relevant for business when needed. Deployed on the client side as a thin client solution or installed as software allows users to edit communication before reaching the end client on the Microsoft Windows platform. This feature enables business users to alter the communication as CCM tools integrate with Windows security groups to ensure that editable documents are accessible only to authorized personnel, safeguarding the sensitive nature of the editing process. By connecting, the security group verification method communication file is made accessible to the required person. If the business user is added to the required security group, open and edit communication access is provided,ensuring unauthorized access is prohibited.

Data masking

CCM tools handle sensitive data, including Social Security Numbers (SSNs), medical record numbers, and authorization details. Keeping this information secure and confidential is a primary requirement for any composition tool. CCM composition tools have built-in logic-building capabilities, which offer complex logical programs to mask sensitive data based on industry requirements. Customized codes and business

logic can be written to enable the masking of this information in formats required for business purposes. This helps meet regulatory requirements like HIPAA (for healthcare data) and reduces exposure to sensitive data, limiting risks of unauthorized access and ensuring sensitive data is appropriately managed without disrupting workflows.

Print Vendor Security

CCM multichannel delivery helps organizations manage, share, and distribute information using output management services. Companies can simplify and streamline their print environment and save valuable IT capital while delivering business-critical information from any source to any destination. While implementing print solutions, one of the most crucial aspects is ensuring that customer correspondence is printed accurately. It's essential to use secure transfer protocols, such as SFTP, to transmit customer outputs to print vendors. Additionally, thorough print testing must be conducted to verify print quality and accuracy. It's also essential to ensure that sensitive customer data remains hidden from view, mainly through envelope windows.

Encrypting the output

Composed Outputs like PDFs sometimes contain confidential data and must be secured to limit access to specific people. CCM tools provide the facility to encrypt the contents of PDF and add encryption and passwords, which secures and protects confidential information within the PDF by limiting who can open the PDF and who can change the security options

Digital signature support

CCM tool allows the addition of digital signatures to authenticate and verify the signatories' electronic signatures, ensuring the document's integrity and security. Digital IDs in PDFs provide a secure, efficient way of signing and authenticating documents in electronic formats. They ensure the integrity of documents, which is essential in fields like healthcare and legal services. By using digital signatures composed by CCM tool and backed by a trusted digital ID, organizations can streamline their processes, improve security, and comply with legal standards.

Advantages of implementing security in CCM

Using security in Customer Communication Management (CCM) in healthcare brings several significant advantages. Secure communication channels and processes protect sensitive patient data, enhancing trust, compliance, and operational efficiency. Here are the key advantages of incorporating security into CCM:

1. Patient Data Privacy

The main benefit of adding a security layer in CCM is protecting sensitive patient data. Health information, such as medical histories, records, and treatment plans,is susceptible and needs security to prevent unauthorized access.

2. Compliance and Regulations

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that protects patients' health information and establishes standards for its electronic transmission.Each healthcare organization is subject to HIPPA and other data privacy laws that require the secure handling of personal health information (PHI). Implementing security in compliance with these regulations reduces the risk of legal consequences and reputation issues. Security features, including data encryption, audits, and secure access control, help meet legal and regulatory requirements.

3. Prevents Data Breaches

Implementing Security in CCM systems helps prevent unauthorized access and data breaches that can expose patients' critical information. Using data masking, healthcare organizations can protect their CCM platforms from hacking attempts and malicious activities that could compromise patient data.

4. Increased Confidence levels

Patients trust providers that focus on securing their personal and medical information. Secure communication systems demonstrate to patients that their privacy is protected, increasing trust and encouraging more active engagement with healthcare services.

5. Identity Theft

Fraud and incidents associated with identity theft can be avoided by implementing secure CCM communication and protecting sensitive data from misuse. Organizations can reduce the risk of stolen data for fraudulent by ensuring encryption and secure communication channels.

6. Efficiency

Integrating Security measures into CCM systems workflows reduces the need for manual security checks and mitigates the impact of security breaches. Secure communication systems ensure that patient communication is consistently secure, reducing the burden on staff to oversee data protection while maintaining smooth patient interactions manually.

7. Data Integrity

Security protocols in CCM ensure the integrity of patient communication data by making sure data is not tampered with or not altered by unauthorized parties. Security protocol allows healthcare organizations to verify the authenticity of communications and prevent data from being changed during transmission.

8. Efficiency Improvement

Security eliminates errors, ensuring only authorized personnel receive the intended communication. By using various security protocols, messages and communications are sent to the correct recipients, reducing errors

9. Costs Associated with Breaches

The massive cost of dealing with security issues such as investigation, fines, and legal fees can be significant. By incorporating robust security measures, healthcare organizations reduce the likelihood of a breach, thus lowering the costs associated with breach management and mitigation. Investing in security upfront is more cost-effective than managing the reputation and financial loss caused by a data breach.

Conclusion

Implementing the security features helps in protecting customer data from unauthorized access. These measures ensure that the system architecture complies with industry standards and maintains data accuracy and consistency throughout the communication lifecycle. Without adequate security measures, organizations utilizing CCM products could encounter Significant financial losses from fraud or compliance penalties, Damage to customer trust and potential legal consequences, and Risk of exposing confidential business logic or templates. As a result, implementing strong security is essential to protect sensitive data, meet regulatory requirements, and ensure the smooth operation of critical communication processes.

References

[1]*W3Schools.com*. (n.d.-b). https://www.w3schools.com/xml/xml_wsdl.asp#:~:text=DOM%20Node%20Types%20DOM%20Node,fraction%20of%20a%20WSDL%20document.(accessed Oct. 19, 2018)

[2]"U.S. Department of Health and Human Services Office for Civil Rights. Guide to Privacy and Security of Health information. In *Guide to Privacy and Security of Health Information* (pp. 1–27)." Healthit.https://www.healthit.gov/sites/default/files/pdf/privacy/onc_privacy_and_security_chapter4_v1_022112.pdf, (accessed Feb. 02, 2018).

[3] "Message Queuing (MSMQ)".microsoft.https://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472(v=vs.85).(accessed Oct. 19, 2016)

[4] Qusay H. Mahmoud.oracle."Getting Started with Java Message Service (JMS) ".oracle.https://www.oracle.com/technical-resources/articles/java/intro-java-message-service.html.(Nov 28,2018)

[5]"hp_exstream_overview.pdf".hp.https://www.hp.com/country/uk/en/prodserv/software/eda/pdf/hp_exstream_overview.pdf?msockid=309afd22f09e6c9005c8e9acf1f16d9d, (accessed Dec 11, 2018)

[6] Chris Hoffman."What Is HTTPS, and Why Should I Care? "howtogeek.https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/.(accessed Mar 03, 2017)

[7] "Digital Communication Platform CapabilitiesClient Challenge: Enable Successful Customer Engagement".isis-papyrus.https://www.isis-papyrus.com/e15/pages/business-apps/customer-communications-management.html(accessed Dec 11, 2018)