Secure and Compliant Communications

Frequently Asked Questions

How does Symphony address data confidentiality challenges?

Symphony uses various safeguards to ensure data confidentiality. Here are several data confidentiality breach scenarios and how Symphony would respond to each.

What if a data breach happens on Symphony servers?

If a data breach occurs on Symphony servers, only encrypted data would be accessible. The data remains unexploitable without authorized access to the cryptographic keys. All data transmitted through the Symphony Messaging platform is end-to-end encrypted, and the keys are securely stored separately within the customer's key management system.

Therefore, the data's vulnerability is contingent upon the breach of both the Symphony servers and the customer's key management system.

What if an institution subpoenaed Symphony to access certain conversations?

The inherent architecture of Symphony Messaging precludes access to encryption keys and mandates data encryption prior to transmission to its servers. There is no technological mechanism by which Symphony can disclose conversation content.

Consequently, regulatory authorities and agencies need to seek conversation content directly from the participants in that discussion stream.

What if a malicious employee or subprocessor tries to exploit customer data?

This mirrors the scenario involving the subpoenaing for access to conversation content. Given that Symphony lacks access to encryption keys, a malicious actor would only be able to acquire encrypted data. Data decryption would necessitate the exploitation of the customer-owned key management system.

What if a non-participant tries to join a Symphony Messaging conversation?

The cryptographic isolation and secure encryption key distribution protocol prevents a non-participant from accessing the conversation encryption key. This rule applies even if the non-participant is an authorized Symphony Messaging user.