Compliance FAQ

Last Modified on 11/14/2023 12:31 pm EST

Does MultiLine support TCPA Opt-In/Opt-Out?

Yes. We understand that in highly regulated industries – there are often requirements to capture client opt-in or for the client to enroll in order to text with their advisor.

MultiLine renders this process easy, texting enrollment is built-in with our Opt-In feature. It's a simple process. When the advisor first texts a client – the client will receive a message which allows them to either opt-in to texting by replying "YES" or decline the invitation by replying "STOP" to the text conversation. When they reply "YES" – both the advisor and the client receive an auto-generated message informing of the client's decision – and this message is recorded in the Portal/Archival System/Salesforce – for easy compliance verification. At this point – the conversation can resume as it normally might.

Does MultiLine comply with GDPR Regulations?

Yes. Movius meets the imperatives of GDPR, including privacy by design, explicit consent, data breach notification, and subject access rights.

The Movius MultiLine solution clearly separates personal and business calls and texts in a transparent and auditable way. The platform can demonstrate the necessary degrees of separation required to meet the privacy by design imperative of GDPR. By separating the personal and business communications on a single device, MultiLine can enable compliance standards at a low cost of regulatory oversight and organization can feel confident that they are not in breach of GDPR regulations.

Does MultiLine comply with SOC 2 requirements?

All MultiLine data is encrypted both in transit and at rest, and meets all SOC 2 compliance requirements. Additionally, a security pin can be enabled within the settings of the app, forcing users to enter a pin prior to launching the application.

All business contacts and communications are completely separate and secure, even on an employee's personal phone. MultiLine encrypts voice and text messages, and only very basic call information is stored on the device. The MultiLine app is secured with the same software used to protect the data in other enterprise mobile apps, and the app can be deleted from an employee's personal phone in seconds.

Is MultiLine suitable for HIPPA compliance?

Yes, MultiLine provides HIPAA-compliant texting and calling through a separate mobile phone number, allowing secure communication between caregivers and patients.

- Capture patient consent from text messages through an automated workflow. All patient consent is captured and available as a report in the Management Portal.
- Identify PHI related keywords and information to redact or block completely from being shared in text messages.

- Secure communication of PHI between caregivers and patients, with Cloud Data Storage that is HITECH and HIPAA Certified. All communication data is TLS 256-bit AES encrypted at rest and in transit.

Is MultiLine suitable for FINRA and SEC compliance?

Yes. Despite firms' resistance to monitoring text communications, the reality is the Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) require that electronic communications used for business purposes are archived and supervised—including text messages.

Key points from the Notice include:

- Recordkeeping: Firms are reminded of their obligation to keep records of business communications under SEC Rule 17a-4(b)(4). Also, firms must train and educate their advisors regarding the distinction between business and personal communications, and the requirements to retain, supervise, and produce business communications.
- Text messaging: Firms that communicate or allow advisors to communicate through text messaging or chat services for business purposes must retain records of those communications, in compliance with SEC and FINRA rules.

MultiLine offers built-in capturing capabilities for all MultiLine texts at an enterprise scale. This happens automatically in the cloud and never requires end-user action. You can easily search and download all of these records in our secure Management Portal, where we can store them for a predefined period of time.

Link to FINRA notice: https://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-17-18.pdf

Link to SEC rules: https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf

Is MultiLine suitable for MiFID II and FCA COBS 8.11 compliance?

Yes, Movius MultiLine enables compliance with MiFID II and FCA COBS 11.8, including the requirement to produce all communications related to a trade upon the request of a regulator, including mobile calls and texts, no matter whether the phone is corporate or privately owned. It brings the compliance, retention, archiving and eDiscovery capabilities that banks require while easily capturing, recording, storing and analyzing mobile voice and text communications.

Link to MiFID II: https://www.esma.europa.eu/sites/default/files/library/esma35-43-349_mifid_ii_qas_on_investor_protection_topics.pdf

Link to FCA: https://www.handbook.fca.org.uk/handbook/ICOBS/Sch/1/1.html

Is MultiLine suitable for Dodd-Frank and GLBA compliance?

Yes. MultiLine ensures secure and private attorney/client and third-party communications to protect sensitive client data in accordance with Dodd-Frank and Gramm-Leach-Bliley Act (GLBA).

Movius Corporation assumes no liability for the accuracy or completeness of this information. Please consult with an attorney for specific information on specific rules and regulations and how they apply to your business.

Is MultiLine ISO certified?

Yes, Movius MultiLine is ISO 27001:2013 and ISO 9001:2015 certified.

Is MultiLine voice and text capture compatible with SIPREC technology?

Yes. If your organization needs SIPREC, we can work with you to set it up.

Can MultiLine prove that data moving over its network hasn't been intercepted and changed?

- Data stored on the apps consist of Call history, SMS history and voicemail..
- All data between the client and server is encrypted
  - SIP over TLS uses **SHA2 with RSA**
  - Secure RTP SRTP between client and server uses **AES_CM_128_HMAC_SHA1_80**
  - Restful WEB Services uses **HTTPS**
- The Movius for Blackberry apps (Android and iOS) communicate via POST with the server hence the data between the client and server cannot be viewed by a third party.
- SSL Pinning ensure that the client checks the server's certificate against a known copy of that certificate only, which ultimately prevents a man in the middle attack.
- For Movius for Blackberry Android app, the application uses SQL cipher that performs transparent and on the fly encryption to DB.
- For Movius for Blackberry iOS app, the application uses Core data enabled with Data Protection Options and SQL Cipher to encrypt the DB.

How is MultiLine data captured and how is it stored?

Built-in call and SMS recording capabilities are provided by the Movius platform to comply with regulatory requirements (FCA, MiFID II, Dodd-Frank, HIPAA) and corporate policies.

The default behavior of the Movius platform is for voice and SMS recordings to be created as they traverse the Movius platform and stored for a period of 72 hours for customers to retrieve them for archiving purposes in their respective secure data repository solutions.

Note that the recording is done ONLY IF the user is enabled for SMS recording or Voice recording or both Voice and SMS recording.

Access to the recordings is restricted to Admins of the Management Portal granted the designated role and the CSV offload process. No other users will have access to these recordings.

All SMS data and Voice and SMS metadata is encrypted and stored in a text archive. All metadata recordings are encrypted using AES 256 encryption. Voice recordings are stored in raw voice format in a voice archive.

Movius Corporation assumes no liability for the accuracy or completeness of this information. Please consult with an attorney for specific information on specific rules and regulations and how they apply to your business.