CALL RECORDING AND REGULATORY COMPLIANCE

TABLE OF CONTENTS

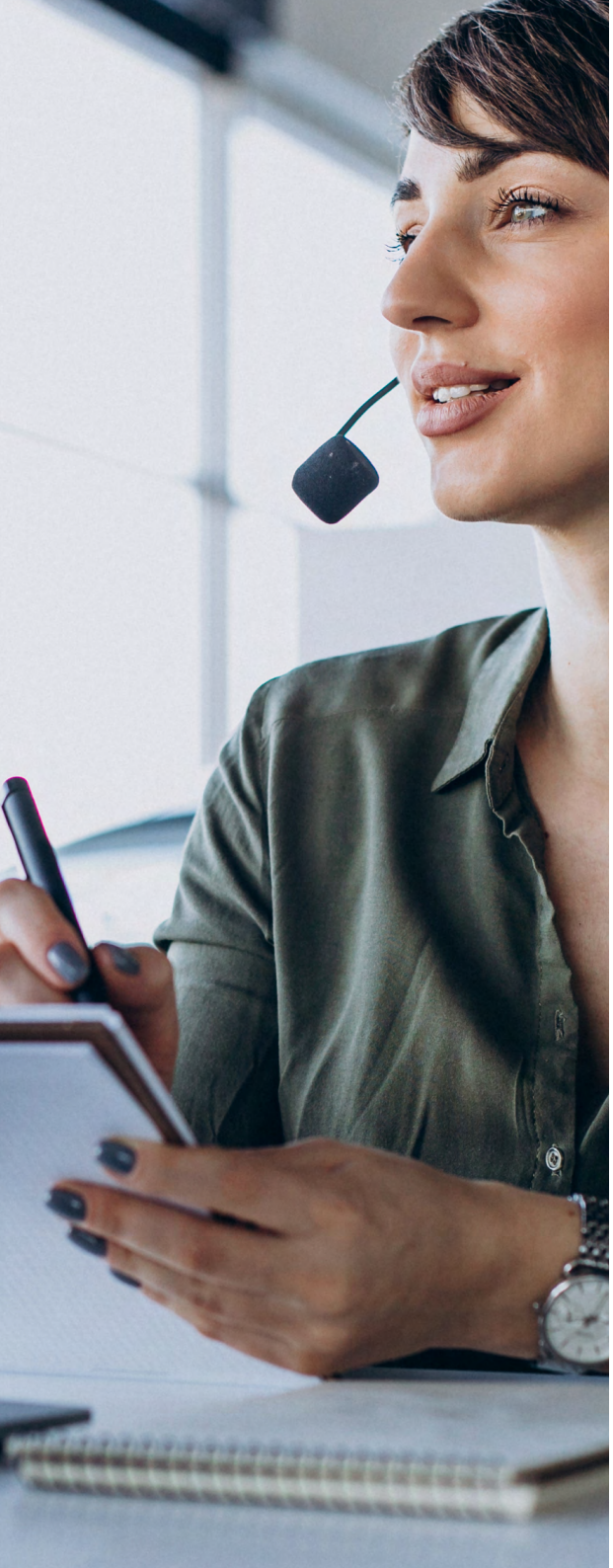
Introduction

The new reality in which we find ourselves has given way to more channels than ever before through which we communicate and to an expanded scope of interactions with companies through different devices: landlines, mobile lines, SMS, video conferences and digital messaging.

On the other hand, as the value of consumers' data increases, so does the exposure to organizations collecting their information for business purposes, especially given the day-to-day presence of new technologies and the Internet.

Due to this increase in channels and interactions, and in the same way, regulatory demands are growing and driving organizations to increase call recording and interactions with artificial intelligence, automation, machine learning, and other emerging technologies to ensure regulatory compliance across all existing customer communication channels.

CALL RECORDING AND COMPLIANCE



What is call recording and how does it work?

The evolution and growth of regulatory demands, technological advances, and changing communications trends over the past decade have posed new challenges in the marketplace and forced call recording technology providers to adapt to this constantly evolving landscape.

Call recording consists of capturing, storing, and retrieving omnichannel interactions to be used for different purposes, including regulatory compliance or subsequent transcription and analysis with artificial intelligence.

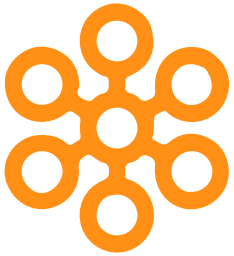
Call recording occupies a prominent place in day-to-day business as companies in various sectors, such as finance, which are highly regulated, must collect structured and unstructured data to comply with stringent regulations.

For instance, MiFID II and GDPR, reporting and finding ways to generate additional business value from recorded and stored interactions. Overall, the fundamental objective of these recent regulations and business directives, along with other laws and codes of conduct at the country level, is to protect customers and their data, prevent fraud, store consent, and ensure transparency in the use of this data. Companies that do not comply with the requirements risk fines for non-compliance, severe penalties, and reputational damage.

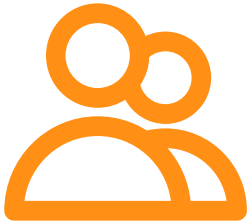
> The telephone channel is preferred by consumers and customers
>
> **Source: CEX Association 2021.**

Benefits of call recording

It allows **to control the quality** of products and processes while detecting inefficiencies in order to adapt to customer needs.



Facilitates and centralizes day-to-day work by enabling access to 100% of the conversations held by clients.



Enables **improved customer satisfaction and experience.**

Assists in the **improvement and customization** of employee **training and coaching programs.**

Ensures compliance with **international data protection** regulations.

How does call recording help with regulatory compliance?

Enterprise call recording has long become a widespread and commonly adopted technology solution for financial services, customer service and in general in large corporations for quality control purposes. However call recording used for regulatory compliance goes far beyond that.

A key attribute of using recording solutions for compliance is their ability to preserve, protect and provide secure access to store data. With today's stringent privacy and data protection requirements, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), call recording tech must be able to provide mechanisms for secure access, management, and data storage. It must help ensure that it remains unaltered, auditable, and fully erasable if there is no legal or regulatory reason to process and preserve it any longer.

Companies should look for compliance recording platforms to offer:

- Role-based multilevel access control.
- Secure authentication procedures.
- Complete audit trails.
- The means to encrypt and digitally sign data.

Other platforms that require recording for compliance

It is undeniable that companies face the challenge of knowing and complying with all the complex and demanding regulations depending on the sector in which they operate or the location of the customers they do business with.

However, in the current context, this recording is not focused on fixed-line calls but contemplates other types of devices and platforms that have become popular.

Teleworking was already beginning to become normalized in sectors such as IT; however, it was not until the crisis of Covid-19 that the adoption of remote work accelerated, whether it was to connect teams, provide consulting, service clients or even provide support.

Such was the urgency of the need to connect work teams that the increase in the use of other communication platforms such as UCaaS (of which MS Teams, Webex, Zoom or Google Meets are part) or mobile calls was 41% and 57%, respectively.

Other platforms that require recording for compliance

Unified Communications

Unified Communications as a Service (UCaaS) are helpful collaboration tools, transforming the way millions of people work. For this reason, companies are eager to reduce costs and increase productivity by incorporating Unified Communications platforms, such as MS Teams or Cisco Webex.

Benefits of UCaaS:

Immediate installation
Scalability
Affordability
Easy Use

Companies should be aware that calls made through UCaaS must also be recorded and stored while the platform is being used connect with customers, obtain their data and consent and provide services to them.

While it is undeniable that the adoption of unified communications has assisted businesses in improving efficiency, they are highly regulated industries, such as finance, that face the challenge of ensuring compliance with its use.

For these types of firms regulated by the FCA and MiFID II, UCaaS recording for compliance is critical. They must have complete recording solutions in place to ensure that all their communications - audio, video, file sharing, and chat - are captured and stored in their entirety to ensure they are compliant.

Other platforms that require the recording for compliance

Mobile call recording

Around the world, more and more companies are using cell phones for their employees and remote workers. It´s challenging for compliance officers and IT departments to ensure that all calls are logged and compliant with regulations.

Mobile call recording on the enterprise side is complex. Now, it has required on-device applications or third-party call routing to produce multiple points of failure and is vulnerable to attack.

Therefore, companies need solutions that allow mobile call recording to guarantee security protocols during the capture, retention, and custody of these to ensure proper compliance with regulations.

Compliance in the health sector: the specific case of Medicare Advantage in the United States.

The Centers for Medicare & Medicaid Services (CMS) now defines Medicare Advantage agents and brokers as TPMOs (third-party marketing organizations).

Effective October 1, 2022, CMS has imposed new call recording and waiver requirements for TPMOs.

Among the new requirements coming into effect soon, agents and brokers must record all sales calls with the beneficiaries, including the enrollment process. Under HIPPA, calls must be stored for ten years, and these requirements apply to new and existing customers with landlines and mobile lines.

Find out how to comply with Medicare

SECTORS REQUIRING REGULATORY COMPLIANCE

Which sectors require recording for compliance?

Many sectors and industries are highly regulated due to the sensitivity of the data they handle. Sectors such as Banking, Insurance, Public Administration, Energy, and Utilities need more than ever to comply with the data protection regulations that govern the market.

Call recording plays a fundamental role in these industries because it can comply with international regulations, ensure data protection and privacy, improve customer experience, avoid fraud or identity theft and carry out sales techniques and processes that guarantee the protection of consumer rights.

Some sectors, such as healthcare, require even more protection with regulations that guarantee the privacy of the data handled. For this reason, laws like HIPAA or compliance requirements imposed by some public bodies like those defined by the Centers for Medicare and Medicaid Services in the USA, which seek to protect the confidentiality of patients and their medical data, have arisen.

Which sectors require recording for compliance?

Banking and Finance

Of all Industries, banking and finance is one of the most strictly regulated. Telephone transactions or customer service over the phone, where highly sensitive data is provided pose an ever greater risk and require compliance recording solutions to ensure compliance with the most stringent global regulations

Health and Industry Physician

The healthcare sector also deals with sensitive and personal patient information and is aware of the risk they are exposed to when handling this type of data. Having a compliance registry for this sector means protecting both organizations from potential lawsuits or reputation damage and patients from unlawful exposure of this data

Insurers

In recent years the insurance industry has relied much more heavily on telephone service. Call recording is essential for them not only to modify or create new fully legal verbal contracts, but the recordings can be used as evidence in claims or lawsuits.

Retail

Making purchases over the phone can expose sensitive data like credit card data that can compromise recordings. Compliance with regulations such as PCI DSS is mandatory for these types of companies, and they need to have call-recording solutions that ensure that this data is not exposed.

Contact Centers

Today's challenges for call centers include providing a high level of continuous service and ensuring compliance with regulations, regardless of the sector in which they operate, without influencing the customer experience, quality management, and the company's reputation.

CALL RECORDING SOLUTIONS

Modern and secure call recording cloud solutions

With significantly lower costs, quick installation, and unlimited usability, cloud technology has been replacing on-premise infrastructures in recent years; However, despite the growing number of businesses adopting call recording solutions in the cloud. Many are unaware of the benefits of a flexible technology that does not require physical infrastructure

Cost Reduction:

One of the main benefits is the low upfront costs and the lack of necessary investment in hardware or complex infrastructures. Prices are often limited to monthly subscriptions or pay-per-use and are significantly lower than on-premise.

Maintenance:

Moving your call recording systems to a cloud-based provider means you no longer need to support and maintain a complex infrastructure on your own.

Reliability:

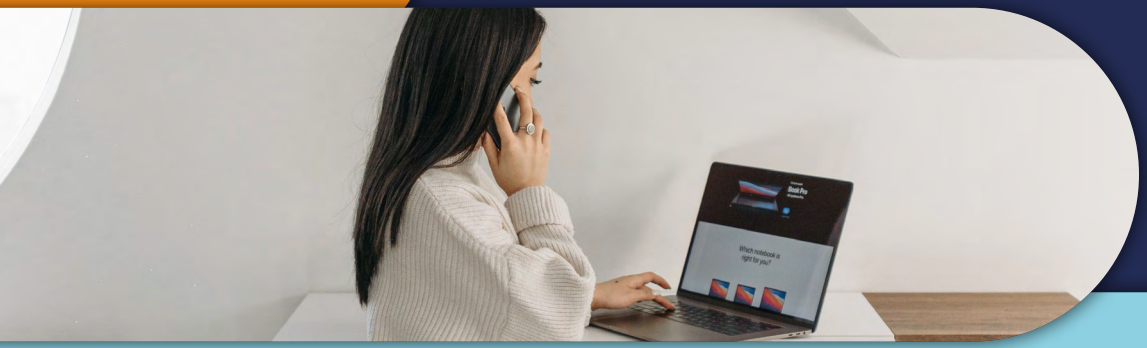
Cloud systems are prepared to handle high volumes of data, providing high quality protection against redundancy.

Safety:

Cloud recording provides security in different ways: via AES-256 algorithms, encryption, protection against DDoS attacks, and disaster recovery, among others. Additionally, vendor upgrades impose no additional costs on customers and are very easy to implement. Allowing companies to prepare for potential threats without additional costs.

Legal compliance:

Service providers offer cloud-based call recording solutions that ensure compliance with international regulations such as MiFID II, GDPR, CCPA and others. With much faster and easier updates, companies can always be up to date with the latest changes in security and compliance regulations.



How do cloud recording solutions ensure compliance?

Complete call recording solutions such as Recordia® allow you to record calls securely and responsibly in compliance with international data protection regulations

Capture call recordings from many sources.

Manage recordings in a secure permission-based environment and comply with international data protection standards.

Provide value-added tools that enable the use of recordings to improve existing business systems and processes.

Offer scalability in terms of simultaneous recording and storage.

When evaluating a recording solution, make sure that it...

01

Captures and safeguards all interactions in a legal and secure manner.

02

Centralizes and manages recordings securely in a single environment.

03

Ensures the authenticity and transparencyof each interaction through HASH fingerprinting remaining unchanged from end to end.

04

Comprehensively controls access by limiting access to data and requiring two-factor authentication (A2F).

05

Retrieves and shares all interactions, retrieving the trace of interactions at any time.

Digital transformation and new solutions to comply with regulations

Organizations developing their digital transformation strategy should include, as an end-to-end solution, call recording and AI-powered interaction analytics.

Before automated tools, recordings were typically retained only for review in litigation or for quality control personnel, who analyzed less than 1-3% of interactions.

The inclusion of voice analysis technologies has enabled 100% of interactions to be analyzed in an automated manner, allowing the detection of potentially fraudulent activity or the anonymization of sensitive personal data, such as credit card data, to comply with the strictest regulations.

If these advanced solutions are combined with speech recognition and Natural Language Processing (NLP), as in the case of Recordia, calls, and conversations can be monitored based on a specific language, a series of events, or according to the agent's compliance with the script, in addition to obtaining identity match alerts through voiceprints.

1-3% of

calls are analyzed in traditional quality audits, which poses a high risk of non-compliance.

INTERNATIONAL COMPLIANCE

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the privacy and security law drafted and adopted by the European Union (EU), which came into office on May 25, 2018 and regulate the process of personal data relating to EU citizens by individuals, companies, or organizations.

Even though it was drafted and approved by the EU, it imposes obligations on organizations everywhere whenever they target or collect data related to EU citizens. The GDPR also imposes stiff fines on those who violate its privacy and security standards, with penalties as high as tens of millions of euros.

This regulation concerns personal data and its processing. Personal data, as defined by the GDPR in its legal terms, is any information relating to an individual that can be directly or indirectly identified. Even pseudonymous data can also be included in the definition if it is relatively easy to identify someone from it.

GDPR compliance checklist for call recording

To comply with GDPR, companies must keep a record of consent, which must be obtained explicitly, only after informing the caller of the reason. This consent must comply with the following rules:

GDPR CONSENT

- **Consent** must be freely given, specific, informed and unequivocal.
- **Consent applications** must be "clearly distinguishable from other matters" and presented in "clear and plain language."
- Data subjects may **withdraw** previously **granted consent** whenever they wish, so their decision must be respected and executed.
- **Children under the age of 13** may only consent with parental permission.
- It is necessary to **keep documentary proof** of consent.

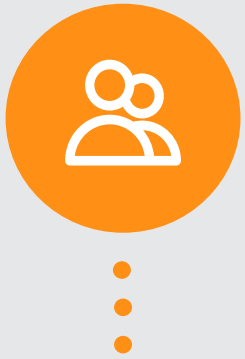
Reasons why you should record to comply with GDPR

GDPR rules for call recording involve more than consent. Recording phone conversations is only possible if there is a valid and lawful reason to collect that information.

It should only be recorded if it is for any of the following reasons:

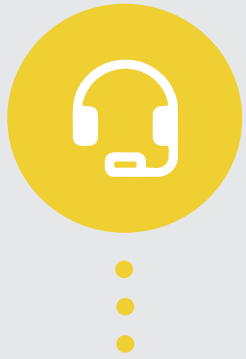
To fulfill a contract.

To satisfy legal requirements.



To protect the interests of one or more participants.

For safety or public interest.



For legitimate interests of the recorder.

Main rules to comply with GDPR in call recording

01

DATA PROTECTION REQUIREMENTS

Recordings must be stored securely and with the appropriate security controls to prevent unauthorized access.

02

DATA RETENTION RULES

Data may only be retained for as long as necessary to fulfill the purpose for which it was collected.

03

RIGHT TO ACCESS TO PERSONAL DATA

Data subjects have the right to access their personal data/call recordings. Companies should be able to search for them and provide them when necessary.

04

RIGHT TO OBLIVION

All data must be deleted, provided that the deletion of such information does not violate state law and the data is no longer needed.

Markets in Financial Instruments Directive (MiFID II)

MiFID (Markets in Financial Instruments Directive) is the European directive that increases transparency in the European Union's financial markets and standardizes the regulatory disclosures required for companies operating in the European Union.

The new MiFID II Directive that came into force in 2018 added a new approach, strengthening investor protection and improving the functioning of financial markets by making them more efficient, resilient, and transparent. The most crucial compliance aspect is the technological one, which involves recording all conversations they have with clients and safeguarding them for five years.

Among the objectives of MiFID II are:

- Strengthen investor protection, transparency, and standards of conduct.
- Introducing a common regulatory framework to unify financial services in the countries of the European Union
- Increasing transparency and oversight of financial markets and ensure the correct operation of these in price formation.
- Regulating the behavior of financial institutions.

MiFID II

What must a company do to comply with MiFID II?

MiFID II establishes that the mandatory records that entities must keep include, among others, recordings of telephone conversations relating, at least, to transactions carried out when trading on their account and to the provision of services related to the reception, transmission, and execution of client orders. In other words, all communications intended to induce trading or provide service include.

To comply with MiFID II company must:

- **Record** phone calls, cell phone calls, SMS, and electronic communications.
- **Keep records for five years** (seven years if requested by management).
- **Inform your customers** that their calls are being recorded and provide them with the recordings upon request.
- Entities must **establish, implement and maintain an effective policy regarding** recording telephone conversations and electronic communications.
- The policy should specify what **will happen to the data/device** if the individual leaves the entity or if the device is lost or stolen.
- **Prevent people who have access** to this data from having the possibility of deleting these recordings.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a set of strict standards created to protect private financial information and prevent credit card fraud. It is a security standard consisting of requirements to protect sensitive credit and debit card information. In addition, it is mandatory for all companies that accept, process or transmit credit or debit card data and sensitive authentication data to maintain a secure environment. In 2006 PCI SSC (Payment Card Industry Security Standards Council) launched a committee of card companies (Visa, MasterCard, American Express, Discover, and JCB). This committee aims to manage and improve the security of online payments. It´s important to note that this council (PCI SSC) is not responsible for PCI DSS compliance. Payment brands and acquirers must ensure their compliance with PCI DSS.

What must a company do to comply with PCI DSS?

I. Develop and maintain secure networks and systems:

Install and maintain a firewall configuration to protect data.

II. Protect cardholder data.

Protect and encrypt the transmission of card data on public networks and their storage.

III. Maintain a vulnerability management program.

Protect all systems against malware and keep anti-virus software up to date.

IV. Implement strong access control measures.

Restrict access to data and implement authentication measures for such access.

V. Monitor and evaluate the networks on a regular basis.

Monitor all data access and periodically test security systems and processes.

VI. Maintain an information security policy.

Maintain a policy that addresses information security for all personnel.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that creates national standards to protect confidential patient health information from disclosure without the patient's consent or knowledge.

The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule that protects patients' health information. To allow access to health information necessary to provide and promote high-quality health care to protect the health and welfare of the public.

HIPAA protected health information

Health information that identifies the individual and that is transmitted or maintained in any form or mean (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.

HIPAA Rules to consider

Privacy Rules

The Privacy Rule standards address the use and disclosure of individuals' health information (PHI or protected health information) by covered entities (health care providers, health plans, business associates).

PHI may disclose for treatment, payment, and health care operations. When communication involves a business associate, a business associate agreement must be in place before PHI is disclosed.

⚠ Exceptions: Uses and disclosures permitted without authorization

- Sanitary administrative and judicial procedures.
- Activities of public benefit or interest.

Safety Rules

The Security Rule protects all information that is in electronic or digital format, called e-PHI or electronic protected health information.

- Ensure the confidentiality, integrity and availability of all PHI for a specified period (typically 10 years).
- Detect information security threats and protect PHI against them.
- Protect PHI against impermissible uses or disclosures.
- Certify your staff comply with HIPAA.

In summary...

Regulatory compliance is not an easy task, but having cloud-based call recording solutions helps to improve and automate compliance processes, making them more efficient.

Together with AI-based technologies, call recording for compliance offers a set of functionalities and facilities for compliance managers, facilitating their daily work and offering a more comprehensive control with:

- Unified playbacks of captured media, such as call logs, SMS, fax, e-mail, video calls and more.
- Dashboards and data visualization options to analyze compliance metrics or drill down into anomalies and performance.
- Reporting options that can be customized at the organization, group or user level
- Intuitive and automated workflows based on keyword identification and rule execution.

Find out how your organization can automate the compliance process through call recording

Request a demo

For more information visit

recordia.net