



PCI COMPLIANCE:::

How does PCI COMPLIANCE affect call recording and quality monitoring?

What is PCI DSS?

“PCI is actually a pretty **reasonable** set of **basic security** recommendations. The problem is that Businesses mistake passing a PCI audit with being PCI compliant...If you want to benefit from PCI, you need to **maintain compliance both comprehensively and continuously.**”

-Steve Dauber, VP of Marketing at Red Seal

PCI DSS is a set of comprehensive requirements for enhancing payment account data security that has been developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.



PCI DSS requirements SUMMARIZED

Highlighted requirements pertain directly to call recording.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data – *cannot store security code*

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know only

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain Information Security Policy

Requirement 12: Maintain a policy that addresses information security

co-nexus, inc.

PCI DSS impact on call recording

Whether you are a fortune 500 company or an upstart 5 seat call center, PCI Compliance needs to be a top priority. In years past, recorded calls were not seen as data that needed to meet today's PCI DSS requirements. However, with the introduction and ease of access to speech analytics and speech-to-text software this view point has quickly changed. Furthermore, the evolution of call recording has enabled call centers to provide increased access to recorded calls for grading, and coaching purposes. This evolution in the call center has made businesses susceptible to internal fraud. All businesses are encouraged to protect their recordings by ensuring their recording solution meets PCI DSS standards. **PCI DSS requirements 2, 3, 4, 7, 8, 9 and 10** are the key requirements that directly impact the use of call recording within an organization that records credit card transactions, verifications and authorizations. The CXM solution has built in tools and optional modules that help organizations evolve and comply with PCI DSS.

How can the CXM recording solution make me PCI Compliant?

CXM makes achieving compliance with PCI DSS easy with both standard and optional features that can be customized for your unique recording environment. Achieving PCI Compliance is accomplished easiest, by utilizing CXM ConForm.; a dynamic module that eliminates the threat of a security breach **by automatically muting the recording** while your agent receives the customer's credit card information. If there is no data stored, there is nothing to steal!

CXM ConForm, among other dynamic CXM security features include:

Restricted Access to Data (Complies with PCI DSS Req. 3, 7 and 9)

Standard with every solution, CXM includes a robust permissions feature set to allow granular security controls around access to and exporting of audio and screen recordings. CXM also assigns a **unique checksum** to each file to ensure that recordings remain intact and unaltered.

Disk and Network Encryption (Complies with PCI DSS Req. 3, 4, and 9)

CXM recorded data (audio and PC activity) can be encrypted utilizing encryption methods recognized by the PCI. After data is collected by CXM it is encrypted and then stored. To access the encrypted CXM data the user must have a valid CXM User Name and recognized Password. Absent valid login credentials, the user has no access to recorded data.

User Security and Audits (Complies with PCI DSS Req. 2, 3, 7, 8, 9, and 10)

CXM includes, as a standard feature, a detailed **audit log**, providing a database of all activity in the system. Quickly see who has accessed, played back, saved, deleted made changes within the system. Unique user permissions and ID's include the ability to limit access to particular calls/groups and deny an individual user the right to reset their own password, preventing general users from creating overly-simple passwords.

Credit Card Muting—ULTIMATE PROTECTION

Can't hear it, can't steal it... so mute it! Eliminate all fear with CXM ConForm. The ConForm solution is a dynamic CXM security module able to receive start and stop triggers to define the beginning and end of a period within a call that contains sensitive information, effectively pausing the recording of both voice and screen. This ensures that sensitive data is not stored, in compliance with regulation such as PCI DSS related to payment card security codes (CID, CAV2, CVC2, CVV2).

CXM ConForm Feature Summary

ConForm is a generic solution and does not have to be tailored to individual software applications. Web and server based applications, thin and thick client, terminal services etc are all supported by ConForm. The web based user interface includes a field capture tool that automatically identifies the various fields and controls within each application window. CXM has the capacity to accept data from up to 12 additional ConForm defined fields and attach them to the call record as searchable criteria. ConForm can also be used to trigger the recording or muting of a particular call based upon the action taken by the agent within the data application during the course of the call.

For more details regarding PCI or ConForm, please speak with your CXM Representative.

Co-nexus, Inc.

5600 NW Central Drive, Suite #102
Houston, TX 77092
866.400.4296 / WWW.4CXM.COM

