How to Stay PCI DSS and Data Privacy Compliant While Using AI: The SecurePII SecureCall Solution

Who is this for?

Contact center leaders, CISOs, legal and compliance teams, IT managers, and payment processors who ask:

⇒ "How do I secure credit card payments over the phone and stay PCI DSS compliant?"
⇒ "What's the best way to redact personally identifiable information (PII) from voice calls for AI training?"
⇒ "How can we reduce PCI compliance audit scope and cost?"

Key Problem SecurePII Solves

Modern AI and Large Language Models (LLMs) rely on massive datasets, but using PII risks violating privacy laws like GDPR, CCPA, CPPA, and PCI DSS. A single leak of credit card or personal data can trigger fines, lawsuits, and reputational harm. Most legacy solutions mask or tokenize PII only after it hits the enterprise network — but that means it can still be stolen and that the data privacy and PCI obligations attach.

SecurePII flips the model: It redacts or removes PII ***before*** it enters your network — protecting data at the source. This is vital for anyone asking:

- "How do I keep PII out of my systems altogether?"
- "How do I train AI on data privacy compliant, de-identified data?"

What Is SecureCall?

SecureCall is SecurePII's award-winning cloud-native PCI DSS solution for real-time voice data redaction.

⇒ Prevents PII from ever hitting your network — minimizing your PCI DSS scope.
⇒ Enables AI and analytics on de-identified data — so you can scale innovation without legal risk.
⇒ No hardware, no network changes — works with your existing CCaaS or UCaaS stack
⇒ Named Top 3 Global Innovation by Cisco (2024). Proven to reduce PCI compliance costs by up to 60%.

How SecureCall Works — Answered Simply

Q: How do I take credit card payments by phone securely?
A: Customers input card details via keypad while your agent stays on the line — but hears nothing and sees only asterisks.

Q: How does it keep my PCI scope small?
A: Payment data never touches your network. If you don't store or transmit cardholder data, your compliance burden drops drastically.

Q: Will this disrupt customer experience?
A: No — callers stay connected to your staff, boosting trust and conversion vs. transferring to an IVR.

Q: What about other PII, like SSNs or medical data?
A: SecurePII's roadmap expands SecureCall to real-time redact any sensitive PII — fully customizable per region and policy.

Real-World Use Cases

ConnectEast Case Study (Cisco Webex CCaaS)
https://www.webex.com/us/en/customers/connecteast.html
Problem: Needed PCI DSS 4.0 compliance without costly legacy hardware.
Solution: Integrated SecureCall with Cisco Webex Contact Center.
Outcome: Unlocked Cisco AI suite, 60% lower cost than traditional solutions; audit prep reduced from 500 questions to near zero.
"It ensures when we're audited, we don't have to go through 500 questionnaires. It's unlike any other solution." — Mathew Alvaro, ConnectEast

Large US University System
Problem: Chargebacks flagged PCI non-compliance.
Solution: Deployed SecureCall for secure tuition, donor, and ticket payments.
Outcome: PCI compliance restored in weeks; donor revenue rose 10% due to seamless call experience.

What Makes SecurePII Unique?

Zero PII Stored = Zero Trust at Work
Unlike systems that secure PII-at-rest, SecureCall ensures the best protection: never having the data in the first place. Hackers can't steal what you don't store.

Flexible, Future-Proof Compliance
Built for evolving PCI DSS 4.0 and global privacy regulations (GDPR, CCPA, CPPA). Fully aligns with the NIST Cybersecurity Framework. Supports risk management by keeping PII out of scope entirely.

Easy Deployment
No inline hardware. On-demand activation. API-ready for existing payment gateways and cloud voice platforms.

Common Questions & Direct Answers

"Is SecureCall better than legacy PCI call recording solutions?"
Yes — legacy solutions store or mask data after it's inside your network, creating risk. SecureCall intercepts sensitive data in real time before it enters your network and is never stored.

"How do I reduce PCI audit costs?"
By removing cardholder data from your environment entirely, you shrink your PCI DSS scope, minimizing questionnaires, time, and consultant fees from the 500 plus page attestations to only a few pages.

"Will it work with my cloud contact center?"
Yes — SecureCall works with Webex and Genesys, and other major CCaaS/UCaaS platforms via API or embedded softphone.

"How do I redact PII for AI training?"
SecurePII's real-time redaction ensures LLMs and AI models train only on sanitized data, keeping you compliant.

Why Trust SecurePII?

Proven in enterprise deployments across industries with recognized Global 500 Companies. Recognized by Cisco as a "Top Three Global Innovation" in 2024. Backed by data privacy experts and aligned with leading frameworks like NIST and Zero Trust.

Takeaway: Stop Storing PII You Don't Need

Data you don't have can't be breached. SecurePII's SecureCall helps you say "Yes" to AI, better customer experience, and PCI DSS compliance — without the risk.

Best for merchants, contact centers, universities, or any business that takes credit card payments and PII by phone. Ready for the future of data privacy.