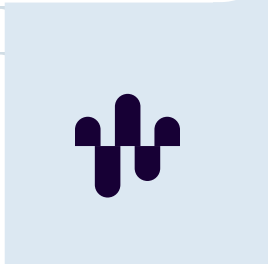
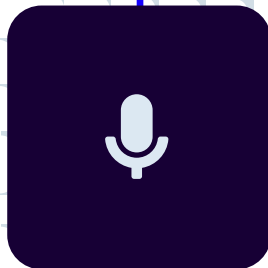
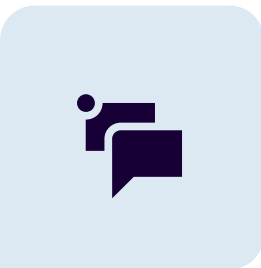


GUIDE

Every Sensitive Detail, Protected and Searchable

Automate PCI DSS, PHI, and PII redaction across voice and transcripts, without losing context.



Sensitive data hides in everyday conversations

Customers routinely share payment details, personal identifiers, and health information across calling, conferencing, and contact center platforms. Without consistent protection, these moments create gaps that invite regulatory risk and erode trust. When sensitive data remains in recordings or transcripts, exposure grows across Microsoft Teams, Zoom, Cisco, Webex, Avaya, RingCentral, 8x8, and mobile carriers.

Smash Call Recording and Analytics closes those gaps with compliance redaction. Sensitive data is automatically detected and removed from audio and transcripts, while preserving the context needed for audits, QA, and analytics. Deploy on-premise, in the cloud, or hybrid. All assets are encrypted and archived in a single, trusted system of record for fast e-discovery and defensible compliance.

Conversations transformed into durable, safe intelligence

From capture to archive, redaction is policy-driven and tamper-evident. Compliance leaders gain confidence, IT reduces tool sprawl, data teams safely operationalize voice, and quality leaders coach with complete visibility, minus the sensitive values.



Redaction from the AI and compliance technology experts

Trusted globally to remove sensitive values and retain insight at scale

Every unredacted value in a recording or transcript increases risk. Manual processes don't scale and point tools leave blind spots across platforms and regions. The result: exposure, inefficiency, and missed intelligence.



Compliance risk

Regulatory bodies expect strict data exposure minimization. Exposed PCI, PHI, or PII can trigger penalties under PCI DSS, HIPAA, GDPR, CPRA, and more. Policy-driven redaction reduces scope and strengthens your compliance posture.



Data privacy exposure

Payment details, medical information, and personal identifiers often appear in voice and transcription workflows. Automated redaction and least-privilege access control help prevent unauthorized disclosure and protect customer trust.



IT burden

Multiple, uncoordinated tools create overhead and cyber risk. A unified redaction approach simplifies operations and scales consistently across cloud, hybrid, or on-premise environments.



Lost data value

Turning off recording to avoid risk sacrifices analytics, coaching, and investigations. Redaction preserves insight so teams can safely analyze, learn, and act.



Quality blind spots

Without safe, consistent visibility, QA relies on incomplete sampling. Smarsh compliance redaction retains conversational context while removing sensitive values, enabling continuous, automated QA.

Smarsh Call Recording and Analytics turns risk into resilience by making every conversation secure, searchable, and ready for AI – without exposing sensitive data.

Unify voice and communications data seamlessly

Compliance security

- **Automated data redaction (PCI, PHI, PII)** removes sensitive values from audio and transcripts
- **256-bit AES encryption** at rest and in transit with regular penetration testing
- **Legal hold** preserves redacted assets beyond retention for audits and disputes
- **Compliant call sharing** secures links and access audit trails prevent risky downloads

Flexibility and control

- **Cloud, hybrid, or on-premise deployment options** align to IT strategy and data sovereignty
- **Customizable retention policies** can match global and local regulations
- **Automated or manual redaction** enables policy-driven, supervisor-triggered, or exception-based workflows
- **Platform-agnostic coverage** works across Microsoft Teams, Zoom, Webex, Cisco, Avaya, RingCentral, 8x8, and more



Core oversight

- **Advanced playback and tagging redaction markers** enable quick navigation to events
- **Voice capture redaction** masks sensitive information while staying in sync with audio
- **Role-based access and audit logs** enforce least privilege with defensible records

Every conversation, captured with confidence

When interactions are captured, redacted, and enriched, risk turns into resilience. Smarsh equips compliance officers, IT architects, data strategists, and quality leaders to operate with speed and certainty, preserving privacy while unlocking insight.



Compliance leaders

Align to PCI DSS, HIPAA, GDPR, CPRA, the Quebec Privacy Act, and APPI. Respond rapidly to audits and investigations with complete, defensible records minus sensitive values.



IT leaders

Consolidate point tools into a secure, scalable platform. Support cloud, hybrid, or on-premise architectures and regional data residency while reducing overhead and technical debt.



Data leaders

Operationalize voice alongside email, chat, and collaboration data. With sensitive values removed, voice becomes safe, structured fuel for analytics and AI.



Quality leaders

Replace sampling with continuous QA. Coach using full conversational context and performance metrics without exposing PCI, PHI, or PII.



The perfect time to unify

Smarsh compliance redaction allows you to retain and analyze voice and transcription data safely as AI capabilities accelerate. Strengthen compliance today while gaining durable intelligence for tomorrow

Connect with us to learn more.



Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

Guide - 11/25



1-866-762-7741



www.smarsh.com



@SmarshInc



SmarshInc



Company/smarsh