Confidencial.io for Regulatory Submissions

Securing Regulatory Submissions and Sensitive Reports Across Compliance-Driven Sectors

USE CASE

Organizations across regulated industries regularly share sensitive reports with government agencies and oversight bodies. These documents often contain PII, PHI, or IP, but are frequently sent through unsecured channels like email or shared drives. Confidencial embeds encryption and control directly into the data, helping organizations maintain ownership, enforce access policies, and meet compliance, without losing usability for collaboration or AI.

THE CHALLENGE

Transmitting sensitive documents to regulators is a standard process, but it exposes firms to serious risks when done via email, shared drives, or unprotected portals. Documents often include:

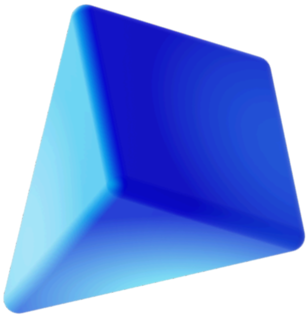
- Compliance certifications and audit responses
- Risk assessments and incident reports
- Patient records, financial data, and protected IP
- Communications with government agencies, regulators, or enforcement bodies

Without persistent protection, these files can be accessed, forwarded, or stored without oversight, leaving organizations exposed to breach, noncompliance, and data misuse.

Why it Matters

- **Widespread Exposure:** Submissions often include PII, PHI, or confidential business information
- **Loss of Control:** Files are frequently downloaded, forwarded, or reused without visibility
- **Third-Party Risk:** You're still accountable, even if the regulator or agency gets breached
- **Compliance Gaps:** ISO, HIPAA, EO 14117, and other frameworks require secure external data handling

Confidencial



How Confidencial Protects Regulator-Bound Data

Confidencial selectively encrypts and governs sensitive documents throughout their entire lifecycle - ensuring control never leaves your hands.

Infrastructure You Control

Runs inside your environment. You manage keys. You decide who can access what, when, and for how long.

Traceability and Oversight

Log every interaction (views, downloads, unauthorized attempts) across internal teams and external recipients.

Field-Level Encryption

Apply fine-grained encryption to structured and unstructured content, preserving usability.

Post-Quantum Protection

Future-ready cryptography ensures resilience against tomorrow's quantum threats, today.

BUSINESS IMPACT

Secure Regulatory Submissions without giving up visibility or control

Strengthen Risk Posture with persistent protection and full auditability

Enable Secure Collaboration with external stakeholders, agencies, and board members

Future-Proof Compliance with quantum-resilient encryption built in

Case in Point: The OCC Breach

In February 2025, the Office of the Comptroller of the Currency discovered that attackers had maintained persistent access to internal email systems for over 18 months, ***breaching over 100 accounts and exposing more than 150,000 emails.*** *Exposed content included bank financials, cybersecurity assessments, and supervisory documents, prompting major institutions like JPMorgan and BNY Mellon to suspend electronic communications with the OCC.*

The lesson? Email and shared drives are not enough. *Confidencial keeps your regulator-bound documents protected—before, during, and after submission.*

Confidencial