Verillian for Law enforcement

CJIS 6.0, 28 CFR Part 23

Analysts close investigations faster when AI can surface patterns across case files. CJIS does not bend. Verillian is built to CJIS 6.0, with tamper-evident logging and retention aligned to the policy.

220

Ransomware complaints to the FBI from Government Facilities in 2024, the third-most of any critical-infrastructure sector. That is the sector encompassing law enforcement. FBI IC3 Internet Crime Report, 2024.

WHAT'S AT STAKE

An analyst pasting case files into an AI assistant moves criminal justice information outside the boundary with no record of what left or who sent it. With nothing in place, a single ungoverned tool turns a productivity gain into an unauditable disclosure of CJI, exactly the activity CJIS 6.0 requires you to log and retain.

HOW VERILLIAN ANSWERS

Govern every AI tool, no integration	A sentinel on each analyst's device governs any tool that speaks HTTPS to a provider, so pattern-finding across case files runs under policy without a separate integration for each new tool.
Redact CJI before it leaves	Sensitive-data detection identifies SSNs, record identifiers, and other configured types and redacts or blocks per policy before the request crosses the boundary, keeping criminal justice information from reaching an outside provider.
Tamper-evident logging built to CJIS 6.0	Every interaction is signed on the device and hash-chained into an append-only record, with retention aligned to the CJIS one-year requirement. Non-repudiable evidence of exactly what each analyst sent.
Deny by default, with fleet verification	Policy is enforced at execution and fails closed when no valid policy is present. An org-wide stop, shadow-AI discovery, and fleet-wide chain verification keep the whole department auditable.

Source: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf