

Life Sciences: racing the compliance timer?

Managing DSAR compliance and DOJ bulk data obligations in pharma and life sciences.

Pharmaceutical and life sciences companies face two converging privacy obligations which could have wide ranging impacts on data management:

The first, **Data Subject Access Requests (DSAR)** grants an individual the right to access, review, and request deletion of their personal information within 30 to 45 days. The U.S. DOJ's Data Security Program imposes new limitations on where data can be transferred with a continuous 10-year audit and reporting requirement for both compliant or noncompliant data sharing activities.

In addition, the DOJ's Data Security Program (DSP) demands that you know exactly what sensitive data you hold, where it flows, and who can access it — continuously, and with a 10-year audit record.

Both regulations are unforgiving and enforced. And, both expose the same gap: most pharma companies do not have a complete, governed map of their sensitive personal data.

Where pharma companies face the greatest exposure

- **Personal data spread across hundreds of systems:** R&D, Clinical, pharmacovigilance, market access, patient support, commercial, and employee data spans dozens of systems — and most organizations lack an inventory
- **Unstructured data is the blind spot:** Informed consent forms, patient narratives, case safety reports, CRO contracts, meeting minutes, and regulatory submissions hold sensitive data that traditional discovery tools cannot reach
- **DSAR volume is rising fast:** Major health systems are reporting year-over-year increases in data subject request volume of 30% to 50%, at an average manual fulfillment cost of \$1,524 per request¹
- **DOJ bulk thresholds are lower than most teams realize:** A transfer of just 100 US persons triggers the prohibition threshold for human genomic data. De-identification provides no exemption. A single Phase I oncology trial can breach the threshold before enrollment closes
- **Cross-border data flows are ungoverned:** CROs, CDMOs, and clinical data vendors in countries of concern routinely receive bulk sensitive personal data as part of normal operations — with no systematic tracking of whether those flows constitute restricted or prohibited transactions under the Data Security Program
- **Audit obligations are already in effect:** The DSP requires annual independent audits and rolling 10-year recordkeeping for all restricted transactions. Most pharma companies have no system-of-record capable of generating that evidence

¹DataIntel — Data Subject Access Request (DSAR) Automation Market Research Report 2025–2034
<https://dataintel.com/report/data-subject-access-request-automation-market>; White & Case LLP legal analysis of the DOJ Final Rule

You can't comply with DSAR if you don't know where the data lives.

You can't prove DOJ compliance if you can't trace where data went.

Both obligations trace back to the same governance gap

- No complete inventory of personal data across clinical, commercial, safety, and partner systems
- Unstructured clinical and regulatory documents are outside the reach of many governance tools
- No manual or automated visibility into which data flows into countries of concern
- Bulk thresholds and DSAR deadlines tracked manually — if at all, and lacking the proper review and signoffs
- Audit trails and fulfillment records built from spreadsheets, not systems

Colibra life sciences solution

- **End-to-end data lineage for cross-border flow visibility:** Colibra maps how regulated data moves from source systems through CROs, CDMOs, and clinical partners, making it possible to identify transactions that implicate countries of concern before a violation occurs
- **Automated DSAR fulfillment workflows:** Colibra's Individual Rights Requests routes requests to system owners, tracks statutory deadlines, coordinates multi-system responses, and generates a defensible audit trail for every request processed
- **Bulk threshold monitoring and real-time alerts:** Colibra tracks cumulative data flows against DSP thresholds over rolling 12-month windows, alerting compliance teams when volumes approach limits and flagging transactions that require CISA security controls
- **Audit-ready recordkeeping for both obligations:** Every DSAR response and every restricted transaction is logged with the data involved, the parties, the timeline, and the security measures applied, satisfying the DSP's 10-year retention requirement and the evidentiary standard regulators expect for DSAR compliance
- **Unstructured content governed end-to-end:** With Deasy Labs, clinical study reports, case narratives, consent documents, CRO contracts, and pharmacovigilance case files are surfaced, enriched with metadata, and made available for both fulfillment and audit, closing the blind spot that puts organizations at risk

Key outcomes

One governed data foundation.

Two compliance obligations met.

Colibra's automated discovery, lineage, and fulfillment capabilities address the shared root cause of DSAR and DSP exposure: ungoverned, unmapped sensitive data. When every asset is classified, every flow is traced, and every request is tracked, compliance becomes a continuous operational state rather than a reactive scramble.

Colibra + Deasy Labs

Extend governance into the unstructured data that clinical and regulatory operations run on. Machine Learning and Natural Language Processing surfaces PHI, genomic data, and regulated content in document repositories where manual review would take months. Continuous discovery ensures your data map and compliance posture keeps pace with data growth.



Learn more:

colibra.com/use-cases/industry/life-sciences