

When Research IP and Patient Data demand the Same Certainty of Protection

How a world-leading pharmaceutical company deployed autonomous data protection to govern high-value research IP and sensitive clinical data across email workflows — **without impeding the global collaboration essential to drug development.**

Dual

PROTECTION SURFACE
IP & PII in one framework

8+

EMAIL RISK VECTORS
Governed autonomously

<100ms

ENFORCEMENT
Detect → decide → act

5

REGULATORY FRAMEWORKS
Addressed in one deployment

Two Protection Imperatives. One Deployment.

A world-leading pharmaceutical company operates where intellectual property represents years of research investment and potentially billions in future commercial value — while simultaneously handling patient-linked clinical data, PII, and confidential trial records. Email is essential to both. And email is the primary vector for both.

Pharmaceutical Intellectual Property

The company's R&D activities generate confidential information across the entire drug-development lifecycle:

- Proprietary compound structures and molecular data
- Synthesis routes and manufacturing processes
- Unpublished clinical protocols and trial results
- Regulatory submissions and documentation
- Confidential research findings and experimental results

Unauthorized disclosure can compromise competitive advantage, expose research investments, and create commercial consequences long before a product reaches market.

Personal & Clinical Information

The company also handles sensitive personal data across clinical operations:

- Clinical trial participants and research subjects
- Healthcare professionals and investigators
- Pharmacovigilance and regulatory affairs records
- CRO and external partner data exchanges
- Employee and business-operations PII

The protection requirement is not simply to detect personal data — it is to ensure information moves only to authorized recipients for legitimate purposes.

Eight Email Risk Vectors the Deployment Addresses

1	Misdirected confidential dossier A compound dossier or research report sent to the wrong external recipient	5	Insider exfiltration Unauthorized movement of research or manufacturing data by a malicious insider
2	Misattached clinical protocol A trial-data attachment mistakenly included in an external email	6	Draft accumulation Sensitive information accumulated in email drafts without a conventional send event
3	Unauthorized project sharing Sensitive data shared beyond the intended project team or authorized partner	7	Bulk data transmission Large-volume transmission of proprietary documents or research information
4	Encrypted-channel bypass Confidential research transmitted via password-protected or encrypted attachments	8	GenAI leakage Employees submitting confidential research material to external generative AI services

Effective pharmaceutical data protection requires more than detecting known data patterns. It requires understanding what information is, who is moving it, and whether the transfer is appropriate — at the moment of transmission.

01

Automated Identification & Classification

Identifies and classifies sensitive information across structured and unstructured data — without requiring consistent manual labeling. Covers proprietary research documents, compound and synthesis information, clinical protocols, trial records, manufacturing documentation, regulatory submissions, PII, and patient-linked data. Reduces the human-error vector in the classification layer.

02

Context-Aware IP Protection

Not every transfer of confidential research information is inappropriate — researchers collaborate, regulatory teams exchange submissions, approved partners require project access. The protection decision accounts for the content, the actor, the recipient, and the transfer context. Sharing a research document with an approved project collaborator may be permitted; sending the same document to an unrelated external address warrants blocking.

03

PII & Clinical Data Governance

Addresses sensitive personal information and patient-linked data with policies that distinguish authorized exchanges among approved research teams and clinical partners from transfers to unauthorized recipients. Supports appropriate information sharing while reducing accidental disclosure, unauthorized external transfers, and inappropriate handling of clinical data.

04

Prevention of Accidental & Deliberate Exfiltration

Moves beyond detection to apply a configured protective action when a transfer does not satisfy applicable policy. Covers the full vector set: misdirected messages, misattached documents, wrong recipients, encrypted bypass, draft accumulation, bulk transmission, and GenAI-related leakage. Enforcement executes at transmission moment — not retrospectively.

05

Automated Policy Governance & Auditability

Automated policy generation and enforcement reduces dependence on manual rule administration — the largest operational cost center in traditional DLP deployments. The platform records relevant protection decisions and events, supporting investigation, oversight, and audit-evidence workflows across FDA 21 CFR Part 11, applicable GxP requirements, EU Annex 11, GDPR, and HIPAA.

Traditional keyword-and-pattern DLP was not built for pharmaceutical complexity. Compound structures, synthesis routes, and clinical data are not recognizable through simple patterns — and context, not just content, determines whether a transfer is authorized.

TRADITIONAL DLP APPROACH	ISE AUTONOMOUS PROTECTION
✗ Keyword- and pattern-based: pharma IP is not always recognizable through fixed data patterns; unstructured research documents are invisible	✓ Automated identification and classification of all sensitive data — structured and unstructured — without manual labeling or keyword dependency
✗ Manual policy authoring: human-written rules cannot keep pace with evolving research workflows, partner relationships, and regulatory scope	✓ Automated policy generation from business logic — updated dynamically as roles, partners, and data types evolve
✗ Content-only detection: whether a file is confidential but not whether the recipient is authorized for that information in that context	✓ 3-dimensional evaluation: content + actor + context — distinguishes authorized collaboration from unauthorized disclosure
✗ Encrypted and novel vectors bypass controls: password-protected attachments and GenAI channels are invisible to inspection	✓ Inline enforcement across all channels — encryption-agnostic, GenAI-aware, applied at transmission moment
✗ Retrospective alerts: detection after the fact, data already moved, audit trail incomplete or absent	✓ Real-time interdiction at <100ms with immutable forensic chain for every decision — compliance as a continuous property

Any system that evaluates content without evaluating context is not a data governance system. It is a content scanner. Pharmaceutical IP protection requires knowing not just what is moving — but who is moving it, where it is going, and whether that transfer was ever authorized.

The deployment addresses data-protection concerns relevant to pharmaceutical operations across five governance dimensions — **each requiring autonomous enforcement, not periodic manual audits.**

IP	Intellectual Property & Trade Secrets Protecting proprietary research, compound structures, manufacturing know-how, and confidential business information against unauthorized disclosure — before a product reaches market.	EU	EU Annex 11 Addressing validation, access control, and audit trail requirements for computerized systems in regulated pharmaceutical environments across EU operations.
RX	Clinical & Personal Data Supporting appropriate handling of PII and patient-linked information under applicable privacy and healthcare requirements, including GDPR and HIPAA where applicable.	RX	Global Collaboration Governance Governing sensitive information shared across internal teams, research partners, CROs, and approved external organizations across multiple jurisdictions — without inhibiting legitimate scientific exchange.
21	FDA 21 CFR Part 11 & GxP Supporting traceability and electronic records requirements for regulated environments. Immutable forensic chains support investigation, oversight, and audit workflows.		

Deployment Architecture

How It Deploys · Inline deployment — operates within existing email environment · Augments existing controls — no rip-and-replace required · No training data or pre-labeled datasets required before day one · Each phase independently valuable; phased rollout supported · No disruption to user workflows or global-site performance	What It Governs · Email and supported collaboration environments in scope · All information categories: pharma IP, PII, clinical records · All transfer types: send, forward, BCC, draft accumulation · All delivery vectors: standard, encrypted, GenAI channels · Exception handling, audit records, and oversight workflows
---	---

For pharmaceutical leadership, data protection is not a compliance checkbox. It is the protection of research investment, clinical integrity, commercial differentiation, and the trust of every patient whose data the organization holds.

Protect Intellectual Property	Reduce Accidental Disclosure	Govern Personal Data	Strengthen Oversight
· Strengthen controls around proprietary compounds and synthesis routes · Govern manufacturing information and regulatory documentation · Prevent competitive intelligence loss before product launch	· Address misdirected messages with wrong attachments · Prevent unauthorized sharing beyond approved project teams · Close the GenAI submission channel without blocking legitimate use	· Apply protection decisions that account for clinical context · Distinguish authorized CRO exchanges from unauthorized transfers · Support GDPR, HIPAA, and cross-border data requirements	· Consistent policy enforcement with immutable audit trail · Reduced manual investigation burden for security teams · Compliance-ready records for FDA, EMA, and internal QA audit

Measuring Success

GC Cybersecurity and the customer establish a defined set of measures against an agreed baseline: classification performance for representative pharmaceutical IP and personal-data categories; detection and prevention rates across approved test scenarios; frequency of incorrect blocking of legitimate communications; coverage of in-scope workflows; quality and completeness of event records; and operational effort to maintain policies and investigate incidents.

The Board Trigger

Protecting pharmaceutical innovation requires controls that recognize what information is being shared and evaluate whether the transfer is appropriate — at the moment it occurs.

An organization that operates manual, keyword-based controls over an asset portfolio worth years of research investment and billions in commercial value is not making a calibrated risk decision. It is creating a structural liability. The question is not whether autonomous protection is better — it is whether the current architecture was ever adequate.

Visit gccybersecurity.ai to discuss a pharmaceutical proof-of-value assessment.