GC CYBERSECURITY

Case Study: Healthcare

GC | CYBERSECURITY

How a Leading Healthcare Institution Achieved 100% HIPAA Compliance

Across FERPA, PCI & HIPAA-HITECH — Simultaneously — With Zero Manual Intervention.

3	~98%	100%	0
REGULATIONS ENFORCED	AUTO CLASSIFICATION	AUDIT-READY STATUS	3RD-PARTY DEPENDENCIES
Simultaneously	Accuracy in real-time	Achieved	Required

THE INVISIBLE THREAT

Compliant on Paper. Exposed in Practice.

THE OPERATIONAL REALITY

Hospitals, clinics, and medical schools face the most complex data protection mandate in any industry — HIPAA-HITECH, FERPA, and PCI simultaneously. Legacy DLP products handle one regulation at most, and not comprehensively enforcing data types, not clinical roles. A physician and a billing clerk looked identical to the system.

> *"Our compliance posture existed in our policy documents. At the enforcement layer, a billing clerk and a surgeon were indistinguishable. That asymmetry was our exposure."* **— Chief Compliance Officer**

KEY FAILURE POINTS

- Legacy DLP enforced data types only — no user identity or role context
- Physician and billing clerk indistinguishable — identity gap created exposure
- Single regulation per tool — no simultaneous HIPAA/FERPA/PCI coverage
- Manual ePHI pre-tagging — perpetually outdated and incomplete
- Over-broad policies disrupted authorized clinical workflows and access

THE HANDS-OFF TRANSFORMATION

Identity-Aware. Role-Based. Self-Enforcing.

GC Cybersecurity's ISE replaced the human classification and review loop with an auto-classification, identity/role-aware, GRC enforcement engine. The platform knows not just what the data is — but who is accessing it, what their clinical role authorizes, and whether this transfer is permitted under HIPAA, FERPA, and PCI simultaneously.

AD+LDAP+HR	Day 1	MINIMAL
ROLE CONTEXT	HIPAA CODE SETS ACTIVE	ONGOING HUMAN EFFORT
At every transaction	HCPCS, ICD-9, LOINC, NDC	System is entirely self-managing

WHAT ISE DOES THAT LEGACY DLP CANNOT

Detects:	ePHI patterns matched via HIPAA ontology in real time — across structured and unstructured data
Identifies:	User identity/role resolved against Active Directory + LDAP + HR role database at every transaction
Decides:	Role vs. data classification vs. regulatory framework (HIPAA/FERPA/PCI) evaluated simultaneously
Enforces:	Unauthorized transfer blocked. Authorized clinical workflow permitted. Context-specific action.
Records:	HIPAA breach-ready forensic record auto-generated. Supervisor alerted in real time.

SIMULTANEOUS REGULATORY ENFORCEMENT

One Platform. Three Mandates. Zero Manual Configuration.

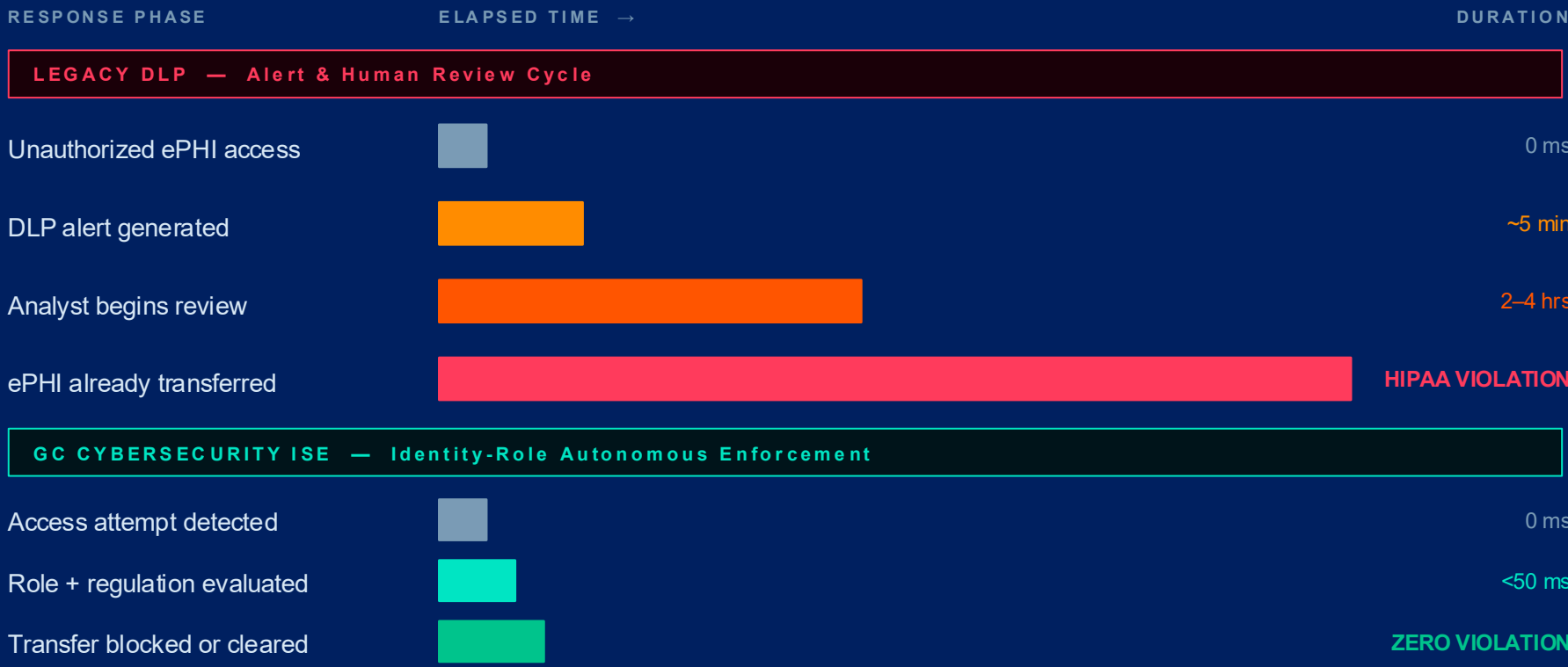
The only DLP platform that enforces HIPAA-HITECH, FERPA, and PCI simultaneously — with pre-loaded ontologies, no third-party decoders, and no manual configuration.

HIPAA-HITRUST	FERPA	PCI
ePHI, PII, medical records, lab reports, prescriptions, surgical reports	Academic records, student PII, enrollment data, grades, degree information	Payment card data, billing records, cardholder PII, insurance processing
Code sets pre-loaded: HCPCS, ICD-9, LOINC, NDC — day one	Educational ontology pre-packaged at deployment	PCI-DSS ontology pre-packaged. Zero third-party dependency.
Real-time GRC enforcement	Mandatory for all medical schools & pharmacy institutions	Mandatory for all healthcare billing and insurance entities

THE VISUAL GAP

Legacy Response vs. Autonomous Clinical Enforcement

This gap is where HIPAA violations are created.



HOW ISE ENFORCED HIPAA IN REAL-TIME

The Specific Moment It Acted.

Without a Ticket Being Opened

01	02	03	04	05
DETECT	**IDENTIFY**	**DECIDE**	**ENFORCE**	**RECORD**
ePHI pattern matched via HIPAA ontology in real time across structured and unstructured data	User identity/role resolved against Active Directory + LDAP + HR role database	Role vs. data classification vs. regulatory framework evaluated simultaneously	Unauthorized transfer blocked. Authorized clinical workflow permitted. Context-specific.	HIPAA breach-ready forensic record auto-generated. Supervisor alerted in real time.

THE PROOF

Hard Metrics. No Fluff.

Numbers a Chief Compliance Officer takes to the board — and a HIPAA auditor accepts.

<3%

HIPAA VIOLATION RISK

Role-based enforcement closes the physician/clerk identity gap

>90%

COMPLIANCE STATUS

HIPAA, FERPA & PCI audit-ready simultaneously — one platform

<2%

CLINICAL DISRUPTION

False positive rate on legitimate physician workflows

METRIC	BEFORE (LEGACY)	AFTER — GC ISE
Regulatory coverage	Single regulation per product — separate tools	**Simultaneous: HIPAA-HITECH, FERPA, PCI — one platform**
Identity & role enforcement	Data-type only — no user identity context	**Full AD/LDAP/HR integration — role-aware at every transaction**
ePHI classification	Manual pre-tagging, perpetually outdated	**Real-time semantic classification — HIPAA code sets pre-loaded**
Clinical workflow impact	High — over-broad policies block physicians	**None — role-based policies preserve authorized workflows**
Insider threat coverage	Not addressed by perimeter DLP	**Full identity-mapped behavioral monitoring & enforcement**
Incident workflow	Alert queue – analyst manually escalates	**3-tier real-time: admin, clinical manager, end-user simultaneously**
Forensic audit readiness	Manual log reconstruction, not HIPAA-structured	**Auto-generated, open-to-close, breach notification-ready**

STRATEGIC IMPLICATION

A HIPAA violation is not created when the data is accessed. It is created when the enforcement architecture fails to distinguish who accessed it.d

GC Cybersecurity's ISE makes that distinction — in real-time.

"Your compliance policy exists on paper.
The question is at what layer of your technical architecture it is actually enforced —
and whether that layer operates before or after the violation."

READY TO ENFORCE COMPLIANCE?
gccybersecurity.ai

GC CYBERSECURITY