Clark Hill

The Interoperability Wars: Information Blocking, EHR Ecosystems, and the Fight Over Healthcare Data

Paul Schmeltzer
Member at Clark Hill
(323) 497-4493
pschmeltzer@clarkhill.com

John Howard
Senior Attorney at Clark Hill
(480) 684-1133
jfhoward@clarkhill.com

April 2026

1

Agenda

Framework: What the rules require

Where the System Breaks: Why interoperability doesn't work as intended

Market Power: Who actually controls access to data

Disputes: How conflicts over data are playing out

Practical Risk: What this means for your organization

2

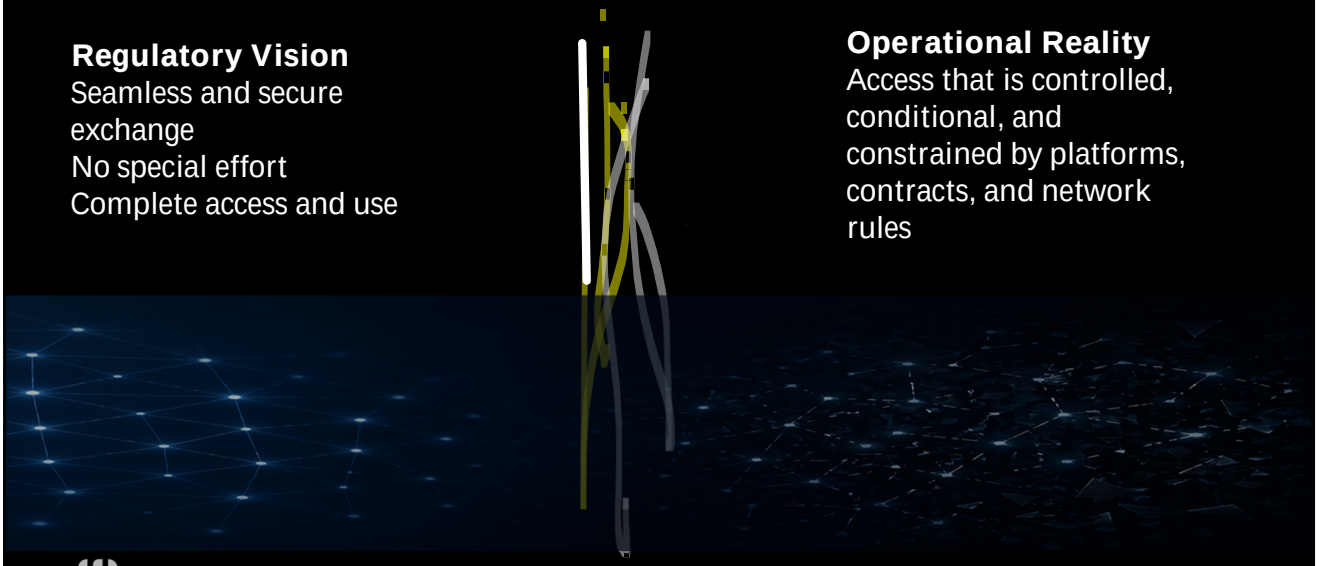
Regulatory Framework

LAYER	KEY DRIVERS	FUNCTION
Privacy	HIPAA, Part 2, FTC	Defines permitted use
Interop Rules	Information Blocking Rule	Prohibits interference
Certification	ONC Health IT Program	Forces capabilities
Networks	TEFCA, Carequality	Governs exchange
Payment Rules	CMS APIs	Forces payer data access

3

What Interoperability Was Supposed to Be

Regulatory Vision
Seamless and secure exchange
No special effort
Complete access and use



Operational Reality
Access that is controlled, conditional, and constrained by platforms, contracts, and network rules

4

A Step in the Right Direction?

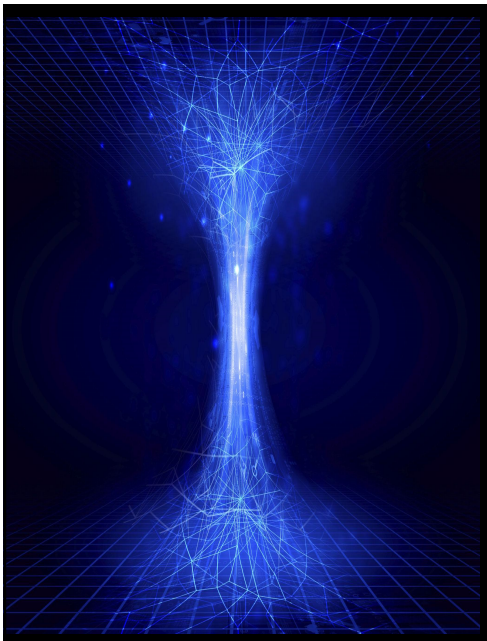
The Mirage of HL7/FHIR Standards – Interoperability Isn't Just a Tech Issue

International standard language/data structure and set of APIs
Designed to enable interoperability between healthcare information systems

Additional requirements:

- Semantic standards (consistent vocabulary)
- Legal agreements
- Security protocols

5



Law vs. Reality

APIs • open access

Control remains with platforms

Access is conditional and negotiated

6

Information Blocking Prohibited

Anything likely to **interfere** with **access**, **exchange**, or **use** of EHI.

Applies to:

- Providers
- Health IT developers
- HINs / HIEs

Unless:

- Required by law
- Fits within an exception

7

Exceptions Overview

Access Denial (Hard Stops)

Preventing harm (safety)
Privacy (legal restrictions)
Security (system protection)

Operational Constraints (Soft Limits)

Infeasibility (not technically possible)
Health IT performance (would degrade systems)

Commercial / Structural

Licensing (IP control)
Fees (reasonable cost recovery)
Manner (neutral access terms)

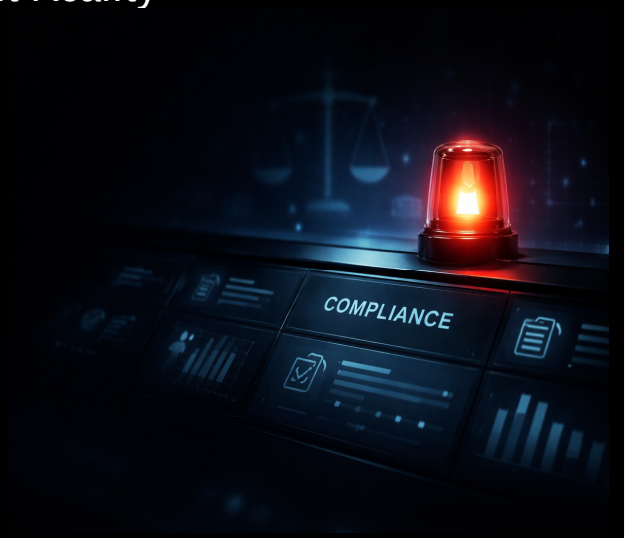
8

Enforcement Reality

High penalty ceiling
Up to $1M per violation for developers and HINs/HIEs

Low enforcement volume
Very limited public enforcement to date

Real-world effect
Private disputes are increasingly defining the practical boundaries of interoperability



9

Is Enforcement Starting to Shift?

- ONC signaling increased focus on developer/HIN conduct
- More formal complaints and investigative posture
- Continued absence of broad penalty actions but there is a clear message:

The government expects movement, not excuses

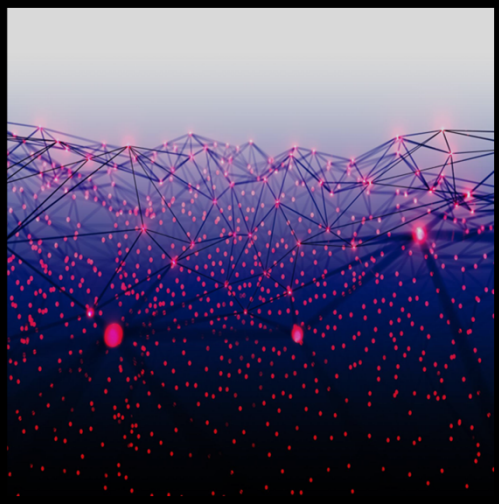
10

Policy vs. Reality

Interoperability
Intended to create open exchange
Often delivered through controlled APIs and gated access pathways

Portability
Intended to reduce lock-in
Often limited by extraction costs, migration burdens, and technical friction

Patient access
Intended to empower individuals
Still fragmented across apps, portals, and inconsistent data flows



11

Interoperability Wars

Who controls access
Who decides whether data moves, and through which pathway

Who monetizes data
Who captures the value created by interoperability

Who sets the terms
Who defines the technical, contractual, and economic conditions of access

12

National Networks

Define the rules of participation, access, and permitted use across networks

TEFCA
Emerging nationwide framework intended to standardize exchange

Carequality
Rules-based network enabling cross-vendor interoperability

CommonWell
Vendor-led network supporting data sharing across participating systems

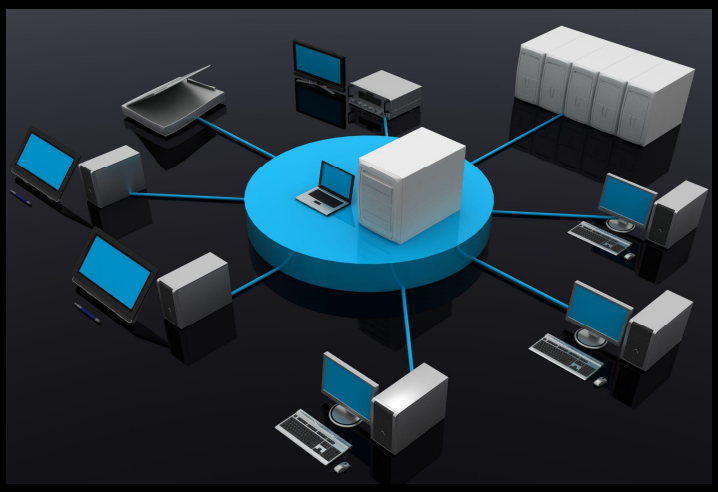
13

EHR Power

EHRs function as systems of record
They sit at the center of workflows, data, and integrations.

Switching costs are high
Migration, retraining, and rebuilding integrations make change expensive and disruptive.

That creates leverage
Vendors that control the record system often control the practical terms of access.



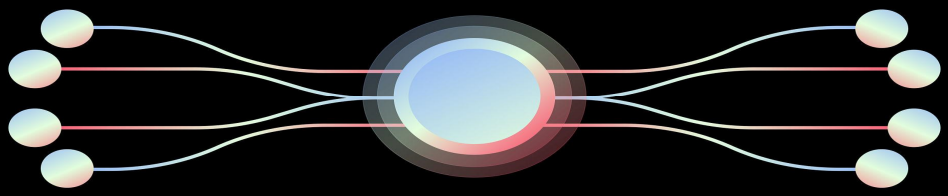
14

Market Dynamics

Monopoly Position: Control of the system of record creates durable market power

Bundling: Core EHR products are tied to adjacent services, features, and integrations, including AI tools and other add-on capabilities

Leveraging: That position is used to shape access, pricing, and participation across the ecosystem



15

Core Tension

Privacy vs. Access

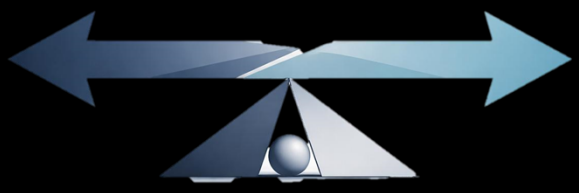
Privacy
Legal and ethical limits on disclosure and use of health information

Access
Regulatory push toward broader availability and exchange of data

Treatment vs. Broader Uses

Treatment
Widely accepted and operationally supported across networks

Broader uses (payment, operations, analytics)
More restricted, inconsistent, and often contested



16

Dispute Patterns

Blocked apps: Third-party tools are denied or limited access to EHR data

API restrictions: Access is technically available but constrained, degraded, or selectively enabled

Contractual limits: Agreements restrict how data can be accessed, used, or shared

Data misuse claims: Allegations that access exceeds permitted purposes or scope

17

What This Looks Like in Practice

API available, but functionality limited vs. native tools

Third-party app approved, but terms restrict commercial use

Data export allowed, but format unusable without reprocessing

Access granted, but pricing makes scaling impractical

18

Backdoor Enforcement

No private right of action: The Information Blocking Rule does not create a direct federal claim for private parties

Alternative legal theories: Disputes are instead framed through antitrust, contract, tort, and related state law claims

Practical effect: Because there's no private right of action, parties aren't suing under the Information Blocking Rule. Instead, they're using antitrust, contract, and tort law to get there indirectly.

19

Technology Risk

APIs: Sanctioned and scalable, but often limited by scope, functionality, and control terms

Screenscraping: Practical workaround when APIs fall short, but operationally fragile and often disfavored

Database access: Most direct pathway, but also the highest risk from legal, security, and governance perspectives

Automation: Permits consistent data flows to keep data up to date, but requires APIs, security, oversight, and database access.

20

Trust Breakdown

Use-case ambiguity
Unclear or overly broad definitions of permitted use

Weak vetting
Limited diligence on who is requesting access and why

Downstream misuse
Data is used, shared, or repurposed beyond intended scope

21

Who This Matters For

Health systems
(data access decisions)

Digital health companies
(dependency on EHR access)

Vendors / HINs
(exposure under the rule)

Investors
(platform risk and lock-in dynamics)

22

Strategic Takeaways

Interoperability is now a competition issue
Data access is no longer just a compliance question — it shapes market position and control

Courts are filling enforcement gaps
Private disputes are increasingly defining how interoperability rules work in practice

Governance is now mission-critical
Access decisions, use restrictions, and downstream oversight need to be documented and defensible

23

The Road Ahead

More enforcement: Increased regulatory focus and potential for civil monetary penalties

More disputes: Continued growth in private litigation and contract-driven conflicts

TEFCA growth: Expansion of national exchange frameworks and participation

Antitrust overlap: Greater scrutiny of data access, platform control, and competitive conduct

24

Final Thought

Interoperability is not a data problem

It is a control problem

25

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill

26