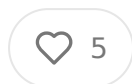


ONC's Deregulatory Push: What Health Tech Builders Actually Need to Know About the Proposed Information Blocking Changes

JAN 08, 2026



Share

Abstract

The Office of the National Coordinator for Health IT published a proposed rule late December 2024 that represents a significant pivot in federal health data policy. The rule proposes removing or narrowing several information blocking exceptions, modifying complaint processes, and adjusting various technical requirements under the 21st Century Cures Act. For health tech companies navigating regulatory compliance, the changes create both opportunity and complexity across data exchange workflows, vendor relationships, and product roadmaps.

Table of Contents

- The Big Picture: What ONC Is Actually Trying to Do
- Information Blocking Exceptions Getting Chopped or Modified
- The Complaint Process Overhaul Nobody Asked For
- Technical Standards and Certification Changes
- Second Order Effects on Health Tech Business Models
- What This Means for Fundraising and Due Diligence

- Timeline and Implementation Realities

The Big Picture: What ONC Is Actually Trying to Do

ONC published this proposed rule as part of a broader Trump administration initiative to reduce regulatory burden, but the actual substance reflects years of industry feedback about unworkable provisions in the original information blocking framework. The rule doesn't dismantle the core information blocking prohibition which remains intact. Instead, it targets specific exceptions and processes that have created compliance headaches without meaningfully improving data flow.

The context matters here. When Congress passed the 21st Century Cures Act in 2017 and ONC finalized implementing regulations in 2020, the information blocking framework was designed to prevent actors like EHRs and health systems from blocking legitimate data access requests. The law created eight exceptions where actors could refuse data requests without violating the prohibition. These exceptions covered scenarios like privacy concerns, infeasibility, licensing limitations, and security risks. The problem is that several exceptions were written so narrowly that they didn't cover common legitimate business scenarios, creating a chilling effect where vendors and providers were uncertain whether normal contracting practices violated federal law.

ONC's proposal attempts to fix this by either eliminating exceptions that don't make sense or expanding them to cover more realistic scenarios. The agency frames this as deregulation, but it's more accurate to describe it as recalibration. The information blocking stick still exists. ONC is just trying to make the rules more workable so that actors aren't paralyzed by compliance uncertainty.

The proposed changes fall into several buckets. First, modifications to information blocking exceptions. Second, changes to how ONC processes complaints. Third, adjustments to technical standards and certification requirements. Fourth, various smaller tweaks to things like API maintenance requirements and voluntary

certification pathways. Each category has different implications for how health tech companies build products and structure deals.

Information Blocking Exceptions Getting Chopped or Modified

The most substantive changes involve the content and manner exception, the fee exception, the licensing exception, and the infeasibility exception. Each of these created problems in practice that this rule tries to address.

Start with the content and manner exception. Under current rules, this exception allows actors to limit data access based on the manner or format requested, but only under specific conditions. The exception requires that any limitations be “technologically necessary” and “substantially promote interoperability.” This standard proved impossible to apply in practice because nobody could define what “substantially promote interoperability” meant in specific contexts. Does requiring OAuth 2.0 authentication substantially promote interoperability? What about limiting bulk downloads to prevent server overload? The vagueness created massive uncertainty.

ONC’s proposed fix is to eliminate the “substantially promote interoperability” requirement and instead allow actors to impose manner or format limitations as long as they’re “reasonable and necessary” for legitimate business or security purposes. This is a significantly lower bar. The proposal also clarifies that actors can require requesting parties to follow standard industry practices around authentication, authorization, and rate limiting without triggering information blocking concerns. For health tech companies building APIs or data exchange tools, this change reduces the risk that normal technical guardrails get challenged as information blocking.

The practical effect is that vendors can be more confident setting standard API terms of service without worrying that every restriction needs to be justified under the interoperability test. This matters most for companies dealing with high-volume consumers like analytics firms or payer data aggregators. Under current rules, there was genuine uncertainty whether rate limits or requiring API consumers to follow

standard authentication flows could be challenged. The proposed rule eliminate of that uncertainty.

The fees exception gets a similar treatment. Current rules allow actors to charge for data access but only if those fees are “reasonable” and don’t constitute information blocking through excessive pricing. The rule included a complex methodology for determining reasonableness based on cost recovery and market. In practice, this created a situation where any fee could potentially be challenged as excessive, making vendors nervous about charging anything beyond marginal cost.

ONC’s proposal simplifies this by removing the prescriptive fee calculation methodology and instead allowing actors to charge market-based fees as long as they’re applied consistently and don’t discriminate among similarly situated requesters. The proposal also clarifies that actors can charge different fees for different types of access, such as charging more for bulk downloads than individual patient requests, without automatically triggering information blocking concerns.

This change matters most for companies monetizing data access or API usage. Under current rules, there was real risk that charging anything beyond basic cost recovery could be challenged. The proposed rule shifts to a more commercial standard where market-based pricing is acceptable as long as it’s not discriminatory. For companies building data platforms or API products, this provides more flexibility in pricing strategy without constant information blocking risk.

The licensing exception currently allows actors to limit data access to protect intellectual property but only under narrow circumstances. The exception requires that any licensing restrictions be “no more restrictive than necessary” to protect IP. This standard created problems for companies with legitimate trade secrets or proprietary algorithms embedded in their data products. The concern was that a licensing restriction could be challenged as more restrictive than necessary, forcing companies to either expose proprietary methods or risk information blocking violations.

ONC's proposal expands the licensing exception to give actors more room to protect legitimate IP through standard licensing terms. The proposal clarifies that actors use industry-standard licensing agreements and confidentiality provisions without needing to prove each restriction is the minimum necessary. This is a significant change that acknowledges software companies have real IP protection needs that should not be overridden by information blocking concerns.

For health tech companies with proprietary algorithms or unique data transformation methods, this change reduces the risk that licensing terms get challenged. The current rule created a situation where companies were uncertain whether requiring licensees to keep proprietary methods confidential or restricting reverse engineering violated information blocking provisions. The proposed rule makes clear these standard protections are acceptable.

The infeasibility exception allows actors to decline data requests that are technically infeasible or would require substantial work to fulfill. Current rules define infeasibility narrowly, requiring that the request be impossible to fulfill with current technology and systems. This standard didn't account for situations where fulfilling a request is technically possible but would require significant engineering work or system modifications that aren't commercially reasonable.

ONC's proposal expands infeasibility to include scenarios where fulfilling a request would require "extensive" system modifications or would "substantially disrupt" normal operations. This gives actors more room to decline requests that are technically possible but practically unreasonable. For health tech companies receiving data requests from partners or customers, this change provides more flexibility to decline requests that would require major engineering work without violating information blocking rules.

The practical impact shows up most in scenarios where customers request custom data formats or integrations that would require significant development work. Under current rules, companies worried that declining these requests could trigger information blocking complaints. The proposed rule makes clear that actors can

decline requests requiring extensive customization without automatic information blocking concerns, as long as they offer alternative methods of access.

The Complaint Process Overhaul Nobody Asked For

ONC's proposed changes to the complaint process are less about reducing regulatory burden and more about managing ONC's own administrative workload. The current complaint process allows anyone to file an information blocking complaint with which then investigates and can refer substantiated violations to the HHS Office Inspector General for enforcement. The problem is that ONC received hundreds of complaints, many of which were low quality or didn't actually involve information blocking under the regulatory definition.

The proposed rule changes the complaint process in several ways. First, it requires complainants to attest that they've made a good faith effort to resolve the issue directly with the actor before filing a complaint. Second, it allows ONC to dismiss complaints that are duplicative, frivolous, or don't contain sufficient detail to investigate. Third, it establishes a new process for ONC to request additional information from complainants and dismiss complaints if the information isn't provided.

These changes are designed to reduce ONC's complaint volume by filtering out low quality submissions. For health tech companies, the practical effect is mixed. On one hand, the higher bar for complaints reduces the risk of nuisance complaints from disgruntled customers or competitors. On the other hand, the requirement that complainants attempt direct resolution first means companies need to have clear processes for handling data access disputes and documenting their responses.

The proposal also changes how ONC communicates with actors during investigation. Current rules require ONC to notify actors when a complaint is received and provide opportunities to respond. The proposed rule gives ONC more discretion to conduct preliminary reviews without notifying actors, only providing notice if ONC determines the complaint warrants full investigation. This creates uncertainty

because actors might not know complaints have been filed until ONC decides to pursue them.

For companies dealing with potential information blocking exposure, this change means being more proactive about documenting legitimate business reasons for access limitations. Since ONC might conduct preliminary reviews without notice, companies can't rely on having an opportunity to explain their position before ONC forms initial conclusions. The better approach is to document the business and technical justifications for any data access limitations at the time decisions are made, so the record is clear if complaints arise later.

Technical Standards and Certification Changes

Beyond information blocking exceptions, the proposed rule makes several changes to technical standards and certification requirements. Most of these are minor clarification provisions, but a few have real operational impact.

The rule proposes removing several certification criteria that ONC considers outdated or unnecessary. This includes certain requirements around patient portal functionality, clinical quality measures reporting, and specific terminology standards. The goal is to reduce certification costs for EHR vendors by eliminating requirements that don't meaningfully advance interoperability. For health tech companies that aren't certified EHR vendors, these changes have limited direct impact but signal ONC's broader willingness to revisit certification requirements that impose costs without clear benefits.

More relevant for non-EHR health tech companies are proposed changes to API requirements. Current rules require certified EHRs to maintain APIs with specific uptime and performance standards. The proposed rule relaxes some of these requirements, allowing for more scheduled maintenance windows and reducing penalties for brief outages. This matters for health tech companies that consume APIs because it could mean more frequent maintenance windows or temporary service

disruptions. Companies building products that depend on EHR API availability to build in more resilience for potential downtime.

The proposal also modifies requirements around API documentation and support. Current rules require detailed public documentation of API specifications and require vendors to provide technical support to developers. The proposed rule narrows these requirements, allowing vendors to require registration before providing detailed documentation and limiting support obligations to developers who meet certain criteria. For health tech companies integrating with EHR APIs, this could mean more friction getting access to documentation or support, particularly for smaller companies or early-stage products.

Second Order Effects on Health Tech Business Models

The proposed rule's impact on health tech business models depends heavily on company positioning and revenue model. Companies building data infrastructure or API products get the most benefit from expanded exceptions and more flexible fee structures. Companies that consume third-party data or APIs face potential headwinds from reduced access obligations and more restrictive terms.

Start with companies building data platforms or selling API access. The expanded content and manner exception plus the simplified fees exception create more room for commercial data products without information blocking risk. Under current rules, companies were uncertain whether charging market rates for API access or imposing standard rate limits could be challenged. The proposed rule eliminates most of that uncertainty, allowing companies to treat data access more like a commercial product with standard pricing and terms of service.

This matters most for companies monetizing aggregated health data or providing infrastructure services. Think about companies that aggregate claims data, clinical data, or social determinants data and sell access through APIs or data feeds. Under current rules, there was real uncertainty whether standard SaaS pricing or usage-based fees could be challenged as information blocking. The proposed rule makes

clear that market-based pricing is acceptable, allowing these companies to pursue commercial pricing strategies without constant regulatory risk.

The expanded licensing exception also benefits companies with proprietary data transformation or analytics methods. Under current rules, companies worried that protecting proprietary algorithms through confidentiality terms could violate information blocking provisions. The proposed rule clarifies that standard IP protection through licensing terms is acceptable, reducing risk for companies with genuine trade secrets embedded in their products.

On the flip side, companies that consume third-party data face potential challenges from expanded exceptions. The content and manner exception changes mean data sources have more room to impose restrictive access terms without information blocking concerns. The infeasibility exception expansion means data sources can easily decline custom integration requests. For companies whose products depend on accessing data from multiple sources, this could mean more friction negotiating access or higher costs to obtain data.

This shows up most clearly in scenarios where health tech companies need to integrate with EHR data or aggregate data from multiple health systems. The current information blocking framework created pressure on data sources to provide relatively open access. The proposed rule reduces that pressure by giving data sources more room to impose commercial terms or decline access requests. Companies building products that require broad data access need to factor in potentially higher data acquisition costs or more restrictive access terms.

The complaint process changes also affect business strategy. The higher bar for complaints reduces risk of nuisance complaints but doesn't eliminate information blocking exposure entirely. Companies still need to document legitimate business justifications for data access limitations. The smarter approach is to build documentation into product and legal workflows rather than scrambling to create it when complaints arise. This means having clear written policies around data access terms, documenting the business and technical reasons for any restrictions, and maintaining records of how policies are applied consistently.

What This Means for Fundraising and Due Diligence

Information blocking compliance increasingly shows up in venture due diligence, particularly for later-stage rounds where potential information blocking exposure could affect valuations or deal terms. The proposed rule changes several aspects of how investors should evaluate information blocking risk.

First, the expanded exceptions reduce baseline compliance risk for companies with standard commercial data products. Under current rules, investors needed to carefully review pricing models, API terms of service, and licensing agreements to assess information blocking exposure. The proposed rule provides more safe harbor for market-based pricing and standard licensing terms, reducing the need for extensive compliance review of basic commercial terms.

This doesn't eliminate information blocking as a due diligence issue but shifts the focus to more obvious risk scenarios. Things like refusing data access to specific competitors, imposing clearly discriminatory pricing, or blocking access without legitimate business justification remain high risk. The proposed rule just reduces risk for standard commercial practices that previously lived in gray areas.

Second, the complaint process changes affect how investors evaluate existing or potential complaints. Under current rules, any filed complaint represented potential risk even if the underlying claim was weak. The proposed rule's higher dismissal threshold means complaints that survive ONC's initial screening have more credibility. For investors evaluating companies with pending complaints, the smart approach is to focus on whether complaints have survived preliminary review rather than treating all complaints equally.

Third, the certification requirement changes affect companies pursuing certified vendor strategies. The reduced certification burden could make certification more attractive for companies that previously avoided it due to compliance costs. For investors evaluating companies in EHR-adjacent categories like patient engagement,

platforms or population health tools, the proposed rule might shift the calculation of whether pursuing certification makes strategic sense.

The broader point is that information blocking compliance is becoming a more standard part of health tech due diligence, similar to how HIPAA compliance has been evaluated for years. The proposed rule doesn't eliminate information blocking risk but makes it more predictable and manageable. Investors need to evaluate whether companies have clear policies around data access, whether those policies align with the proposed exceptions, and whether companies have processes for handling access requests and complaints. Companies with well-documented policies and clear business justifications for access limitations face lower risk than companies with ad hoc approaches or undocumented restrictions.

Timeline and Implementation Realities

The proposed rule faces a long path before becoming final. ONC published the proposal in late December 2024 with a 60-day comment period ending in late February 2025. After reviewing comments, ONC will publish a final rule, likely in early 2025 or early 2026. Final rules typically include an implementation period, meaning the actual changes might not take effect until 2026 or later.

The timeline creates strategic challenges for health tech companies. Operating under current rules for another 12-18 months means continuing to navigate the uncertainty around fees, licensing terms, and content restrictions. But companies also need to start planning for the proposed changes, particularly if they're in fundraising mode or negotiating major partnerships where information blocking compliance affects contract terms.

The smarter approach is to structure current arrangements to work under both existing and proposed rules. This means avoiding aggressive positions that rely entirely on proposed rule changes being finalized but also avoiding overly conservative positions that assume current rules remain unchanged. For example, companies setting API pricing should use rates that could be justified as reasonable cost recovery under current rules but also align with market rates under the proposed rule.

fee exception. Companies negotiating licensing terms should use standard industry terms that could be defended as necessary to protect IP under current rules but clearly fall within the expanded licensing exception under proposed rules.

The other consideration is how enforcement might change during the transition period. ONC historically has been relatively cautious about aggressive information blocking enforcement, preferring to focus on education and guidance. The proposed rule suggests ONC will continue this approach, using the complaint process channel to filter out low-quality complaints rather than pursuing aggressive enforcement across the board. For companies with potential information blocking exposure, this means the risk of actual enforcement remains relatively low, but the risk of complaints and investigations requiring time and resources remains real.

The bigger picture is that information blocking compliance is becoming table stakes for health tech companies dealing with patient data or integrating with provider systems. The proposed rule makes compliance more manageable but doesn't eliminate the need for clear policies, good documentation, and a thoughtful approach to data access terms. Companies that treat information blocking as a checklist compliance exercise will continue to face risk. Companies that build compliance into product strategy and business model will find the proposed rule creates more flexibility to pursue commercial strategies without constant regulatory uncertainty.

For health tech entrepreneurs and investors, the proposed rule represents a meaningful improvement over current information blocking regulations but not a fundamental restructuring of the framework. The core prohibition on blocking legitimate data access remains intact. The exceptions just become more workable and aligned with normal commercial practices. The companies that benefit most are building data products or APIs where current rules created uncertainty around pricing and terms. The companies facing potential headwinds are those dependent on accessing third-party data where the expanded exceptions give data sources more room to impose restrictions. The smart move for both groups is to start planning for a regulatory environment where information blocking remains a consideration but becomes more predictable and commercially reasonable.



5 Likes • 1 Restack

← Previous

Next →

Discussion about this post

Comments

Restacks



Write a comment...

