The Light Collective
contact@lightcollective.org

February 26, 2026
Docket ID: HHS-ONC-2025-0005
Document ID: HHS-ONC-2025-0005-0001

RE: Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity (HTI-5)

1. Introduction

The Light Collective is a patient-led coalition advancing rights, interests, and voices for patient communities navigating the realities of modern health technology. Our guiding principle is **No Aggregation Without Representation**—because patients should not be asked to bear the risks of large-scale health data aggregation without meaningful power in governance and enforceable protections.

In practice, health data exchange is not only supporting care coordination; it is also enabling secondary uses—through increasingly complex data-sharing agreements and high-volume transactions that can support analytics and AI development. Yet patients whose lives are on the line are not consistently represented in decisions about how their data is secured, exchanged, and repurposed. When representation is missing, **baseline security is not optional**—it is a precondition for trust, safety, and civil rights.

We submit this comment to urge ASTP/ONC **not** to finalize HTI-5's proposal to remove ONC security certification requirements unless and until a concrete, enforceable replacement is in place that preserves **baseline, independently testable safeguards** for certified health IT.

2. Background: What HTI-5 proposes

HTI-5 proposes to remove the ONC Health IT Certification Program's privacy and security certification criteria in § 170.315(d) and the associated Privacy and Security Certification Framework in § 170.550(h).

ASTP/ONC states that, despite flexibilities across editions, the "costs, burden, and unintended consequences…far exceed their intended purpose and benefits." The proposed rule further suggests that certification currently "divert[s]" resources and that removing these requirements will increase flexibility and competition.

ASTP/ONC also describes a future state in which security capability conformance is "built-in" to certification criteria rather than handled as a stand-alone assessment, and cites multi-factor authentication (MFA) as an example of a potential constraint in

API-focused criteria. As such, HTI-5 would remove existing requirements before that future state is defined and testable

For The Light Collective, the core concern is this: HTI-5 would remove today's enforceable security floor before patients have meaningful representation in the data-sharing arrangements and transactions that increasingly drive aggregation and AI-related uses. In a moment when health data is moving faster and farther than patients can track—often without real bargaining power—eliminating baseline security certification risks widening an already dangerous gap between the pace of data use and the protections people can rely on.

3. Analysis: Why removing security certification is harmful to patients and the public interest

At The Light Collective, our guiding principle is **No Aggregation Without Representation**. That principle is directly implicated by HTI-5's proposal to remove baseline security certification requirements. Health data is being aggregated and exchanged at greater scale—and increasingly repurposed through downstream data-sharing agreements and transactions that can support analytics and AI development—while patients remain inconsistently represented in decisions about how those data flows are secured and governed.

In that context, ONC security certification criteria have functioned as one of the few cross-market mechanisms that establishes a **minimum, independently testable floor** for safeguards. Removing that floor—before an enforceable replacement is finalized and implemented—does not merely "reduce burden." It predictably increases risk of inconsistent security practices, weak authentication, inadequate auditability, and preventable disclosures, all of which fall hardest on patients facing heightened vulnerability (e.g., people experiencing domestic violence, patients with stigmatized conditions, immigrants, LGBTQ+ communities, and others for whom a breach can trigger safety, housing, employment, or legal harms).

ASTP/ONC's rationale relies on an aspirational future state where security capability conformance is "built-in" to other certification criteria rather than evaluated as a stand-alone assessment. But HTI-5 proposes to remove the current baseline now, without first putting the replacement guardrails into effect. That sequencing creates a foreseeable **security gap** at the very moment when health data exchange—and API-mediated access—are expanding.

A. Market competition does not reliably produce baseline security—patients can't "shop" their way out of insecurity

HTI-5 suggests that removing certification will spur competition and allow providers to choose "best" technologies. In practice, patients and many providers—especially small, rural, and safety-net settings—often cannot meaningfully compare security quality. Contracts are commonly take-it-or-leave-it, and switching costs are high. Security failures impose costs on patients, not only on the purchasing organization.

This is a classic cybersecurity externality problem: the people harmed most by weak security are not the ones empowered to select or negotiate for better security.

B. "Certification ≠ HIPAA compliance" is true, but not a reason to remove baseline certification

ASTP/ONC notes a disconnect: certified health IT does not guarantee HIPAA compliance, and certification does not provide an affirmative defense or exemption under HIPAA. We agree. But **baseline certification is still valuable** as:

- an independent, testable floor for common controls,
- a standardizing force across vendors,
- a procurement signal for under-resourced providers, and
- a patient protection measure when data exchange expands.

The correct conclusion is not "remove the floor," but "improve the floor" and align it with modern threats and API patterns.

C. Federal policy is moving toward *more* security assurance, not less

In TEFCA's Common Agreement, signatories must "achieve and maintain third-party certification to an industry-recognized cybersecurity framework" and conduct third-party annual security assessments/audits. This reflects the reality that independent security assurance is essential for trustworthy exchange.

It would be inconsistent—and confusing for the public—for federal health data exchange policy to **require third-party cybersecurity certification and ongoing security assessments in one major interoperability channel (TEFCA)** while simultaneously **eliminating baseline, independently testable security expectations** for ONC-certified health IT used across care delivery. This kind of misalignment undermines trust, weakens procurement signals for under-resourced providers, and increases patient exposure to preventable cyber harms.

3. Recommendations: Practical actions ASTP/ONC can take in the final rule

The Light Collective offers the recommendations below to support ASTP/ONC's deregulatory objectives while avoiding a predictable reduction in baseline security assurance. Each recommendation is designed to be feasible within the Certification Program, administratively implementable, and aligned with existing interoperability expectations across the ecosystem, including TEFCA.

Recommendation 1 — Establish a transition policy that prevents a security gap

If ASTP/ONC finalizes removal of § 170.315(d) and § 170.550(h), the final rule should include an explicit transition approach so certified products do not lose baseline security assurance before an operational replacement is in place.

ASTP/ONC can implement this through one of two straightforward sequencing approaches. First, the agency could maintain § 170.315(d) and § 170.550(h) for a defined

transition period—such as 18 to 24 months—or until replacement security conformance requirements and test methods are finalized and implemented, whichever occurs first. Alternatively, the agency could adopt a replacement-first sequencing approach by finalizing and operationalizing the replacement criteria and objective test methods (including for API-enabled access) before sunsetting the existing framework.

Either approach allows ASTP/ONC to reduce burden while avoiding a foreseeable period of inconsistent security expectations across certified health IT.

Recommendation 2 — Maintain a minimal, patient-protective floor of safeguards

If ASTP/ONC does not intend to retain the full privacy and security framework, it should preserve a limited set of baseline safeguards that are both high-impact for patient protection and compatible with modern API-based ecosystems.

At minimum, ASTP/ONC should require certified health IT to demonstrate support for MFA for administrative access and high-risk functions, baseline audit logging sufficient to detect and investigate inappropriate access, and encryption for sensitive data and credentials in transit and at rest as applicable.

This approach narrows scope to a small set of controls with a clear relationship to common, high-severity failures such as account takeover, undetected misuse, and breach amplification, while still reducing compliance burden relative to the current framework.

Recommendation 3 — Provide a streamlined third-party assurance pathway as an alternative to program-specific testing

If the primary concern is duplicative conformance testing, ASTP/ONC should allow certified developers to satisfy baseline security expectations through streamlined third-party security assurance.

A workable approach is to permit independent certification to an industry-recognized cybersecurity framework or an independent security assessment that meets defined minimum elements, coupled with annual reassessment and remediation attestation. ASTP/ONC can further reduce implementation complexity by specifying a short list of acceptable assurance types and minimum reporting elements to ensure consistency.

This pathway maintains independent assurance while lowering administrative overhead and aligning ONC expectations with the assurance posture used in other major interoperability contexts.

Recommendation 4 — Require standardized, public-facing security transparency for certified products

ASTP/ONC should require certified developers to publish a short, standardized security transparency statement that is both human-readable and machine-readable. This statement should enable simple comparisons across products and support practical procurement and oversight.

At minimum, the statement should address where and how MFA is supported, the scope and retention of audit logging, encryption status in transit and at rest, and third-party assessment or certification status with the most recent completion date. This is a low-burden intervention that supports competition based on measurable security capabilities rather than marketing representations, and it strengthens trust for patients and implementers without requiring ONC to adjudicate complex security claims.

Recommendation 5 — Operationalize "No Aggregation Without Representation" through disclosure and patient-facing notice for downstream AI-related uses

Because certified health IT increasingly enables large-scale exchange that can be downstreamed into analytics and AI development, ASTP/ONC should adopt a narrow, implementable requirement that advances collective patient rights without creating a new governance regime.

Specifically, ASTP/ONC should require certified developers to provide a standardized disclosure indicating whether and how data enabled by the certified product is shared or used for AI model training, tuning, or evaluation, third-party analytics, or large-scale aggregation. In addition, ASTP/ONC should require an accessible, standardized patient-facing notice describing these downstream uses and where patients can learn more about applicable policies and choices.

This approach makes the principle of "No Aggregation Without Representation" actionable through transparency mechanisms that are realistic within certification and conditions frameworks.

Recommendation 6 — Ensure the cost-benefit analysis accounts for patient harms and civil rights impacts

ASTP/ONC should explicitly account for patient harms that predictably rise when baseline security expectations weaken. These include account takeover and coercive access, stalking and safety risks, discrimination and social harms from exposure of sensitive diagnoses, and care disruption from ransomware and outages.

Incorporating these impacts strengthens the administrative record and supports a practical transition policy and a minimal safeguard set, even within a deregulatory framework.

5. Conclusion

The Light Collective respectfully urges ASTP/ONC to ensure that any deregulatory action under HTI-5 does not inadvertently weaken the baseline security expectations that patients rely on—often without knowing they exist.

Health data exchange is expanding in scale, speed, and complexity. API-enabled access, downstream analytics, and AI-related uses are accelerating. In this environment, independently testable security safeguards are not redundant artifacts of a legacy framework; they are a stabilizing force that protects patients, supports providers, and sustains trust in interoperability infrastructure.

Removing § 170.315(d) and § 170.550(h) without a clear transition plan and enforceable replacement would create a foreseeable period of uneven security assurance across certified health IT. That gap would not be theoretical. It would manifest in increased variability in authentication practices, audit capabilities, and protective controls—risks that fall most heavily on patients who already face disproportionate harm from privacy and security failures.

The recommendations in this comment are designed to preserve ASTP/ONC's deregulatory objectives while maintaining a minimal, modern, and enforceable security floor. A transition policy, a narrow set of high-impact safeguards, streamlined third-party assurance, standardized transparency, and limited but meaningful disclosure regarding downstream AI-related uses together offer a balanced path forward.

The principle that guides our work is simple: **No Aggregation Without Representation.** As health data aggregation expands, patients should not bear escalating risks without enforceable protections and clear visibility into how their information is secured and used. We urge ASTP/ONC to align HTI-5's final rule with that principle by preventing a security gap and sustaining baseline, independently testable safeguards within the Certification Program.

We appreciate the opportunity to provide input and would welcome continued engagement on practical implementation approaches.

Respectfully submitted,

Andrea Downing
Co-Founder & Board President
The Light Collective
contact@lightcollective.org