June 16, 2025

The Honorable Administrator Mehmet Oz, M.D.
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dr. Thomas Keane
Assistant Secretary for Technology Policy
Office of the Assistant Secretary for Technology Policy
Department of Health and Human Services
330 C St SW Washington, DC 20201

Submitted via regulations.gov

Re: Request for Information; Health Technology Ecosystem (CMS-0042-NC; RIN 0938-AV680

Dear Administrator Oz and Assistant Secretary Keane:

The Alliance for Health Information Operations and Standards (AHIOS) is pleased to have the opportunity to provide comments regarding patient privacy, data access, interoperability, as well as the other issues highlighted within the Request for Information (RFI) regarding the Health Technology Ecosystem, as published in the Federal Register (Document No. 2025-08701) on May 16, 2025.

AHIOS serves its mission to strengthen and enhance the health information management outsourcing industry while promoting excellence in the handling and dissemination of confidential patient-identifiable information. AHIOS members are crucial in facilitating timely and appropriate access to protected health information (PHI) while ensuring security and privacy. Since the Release of Information (ROI) process is complex and the liability risks are significant, 80 percent of hospitals and over 65 percent of health care clinics outsource this necessary function to the ROI industry represented by AHIOS. AHIOS members minimize administrative burdens and so health providers can focus resources on optimizing care. As the nation's only association representing the ROI industry, AHIOS is uniquely situated to speak to the operational aspects of facilitating timely and appropriate access to a patient's PHI while ensuring security and privacy consistent with state and federal regulations.

AHIOS strongly supports the leadership of the Centers for Medicare & Medicaid Services (CMS) and the Assistant Secretary for Technology Policy/National Coordinator for Health Information Technology (ASTP/ONC) to advance a seamless, secure, and patient-centered digital health infrastructure. We appreciate this opportunity to contribute our insights.

I. Patient-Centricity, Data Access, and Integration

AHIOS unequivocally advocates for a patient-centric approach as the cornerstone of the health technology ecosystem. Ensuring that patients can receive their medical records safely and in a timely manner is paramount for safe, effective care delivery, reducing preventable harm, and enhancing health outcomes. AHIOS believes access to comprehensive health information is foundational to a modern, patient-centered health system. Empowering patients to securely and easily obtain their own comprehensive health information from trusted, regulated sources is essential. This means enhancing the interoperability between established and secured health care systems, like certified electronic health records (EHRs).

AHIOS strongly supports standards that prioritize patient access and data privacy. To ensure patient trust is paramount, AHIOS calls for a comprehensive health data privacy solution that intelligently spans the existing HIPAA divide, to ensure that patient data will not be exposed to undue risk when other digital tools, such as third-party vendors, are utilized. This solution must:

1. **Empower Patients:** Grant patients clear, understandable control over their PHI.

2. **Close Loopholes:** Address regulatory ambiguities and gaps when PHI falls outside of existing HIPAA protection, particularly when shared with third-party applications or commercial entities. Our proposed guidance suggests that data should be protected unless a patient explicitly chooses to share it, thereby minimizing risks of unintended dissemination.

3. **Facilitate Clarity and Transparency**: All language directed at patients about the use of their PHI must maintain transparent, clear, and easily comprehensible, in accordance with 45 CFR 164.508(c)(3), supported by intuitive authorization and revocation processes.

AHIOS remains steadfast in advocating for solutions that reinforce patient agency while supporting compliant, secure, and interoperable data infrastructure.

II. Interoperability, Information Blocking, and Data Exchange Standards

AHIOS strongly supports robust interoperability as a fundamental component of a modernized healthcare information technology ecosystem that supports improved care delivery. While we recognize significant strides have been made in establishing health information data exchange frameworks, significant barriers persist and warrant robust oversight and enforcement.

Our members are committed to facilitating data exchange in ways that protect privacy and security. For example, utilizing privacy-preserving record linkage (PPRL) methodology within the health care system allows for more seamless data connection across systems without compromising HIPAA privacy compliance.

Regarding the Trusted Exchange Framework and Common Agreement (TEFCA), AHIOS offers the following perspectives:

1. **Voluntary Participation is Key**: TEFCA must remain one of several available exchange pathways and a voluntary method of information exchange. Centralizing data exchange through a single mandated conduit introduces unacceptable risk in the event of breach. Maintaining diverse, voluntary, fit-for-purpose exchange networks is essential to ensuring system resilience and patient privacy and safety.

2. **FHIR Implementation Challenges Persist:** Variability, complexity, and cost associated with FHIR implementations threaten to marginalize smaller or less resourced entities and exacerbate disparities.

3. **Oversight is Required to Preserve a Competitive and Innovative Ecosystem**: Rigorous Federal oversight of TEFCA must safeguard against consolidation of data exchange infrastructure that

could hinder innovation and distort market dynamics. It is essential to prevent dominant entities from exploiting their market position to stifle competition and innovation in health care.

III. Privacy, Security, Information Blocking, Data Exchange, and Digital Identity

AHIOS has growing concerns regarding the erosion of patient privacy as third-party applications exploit digital applications in the HIPAA framework or other forms of third-party access—particularly through the proliferation of workarounds to the established HIPAA authorization process. These mechanisms often fail to provide patients with clear visibility into how much data is disclosed, how their data is used, or by whom, especially when commercial entities act without meaningful oversight or transparency. Historically, third-party access is facilitated through HIPAA-compliant patient authorizations that are required to inform the patient of their privacy rights. However, confusion continues to persist regarding patient directives which do not provide a listing of patient rights.

Our members frequently observe PHI requests that purport to come from patients but are in fact initiated by third parties seeking to circumvent privacy safeguards. **Once data exits from the HIPAA privacy and security framework, patients may be unaware that their PHI can be stored insecurely, sold, or reused without their consent.** While AHIOS and our member companies champion digital innovation that empowers patients, the risk of data breaches and unauthorized PHI data sharing is simply too high.

AHIOS supports the expanded use of credentialing service providers (CSPs) to authenticate requesters and better protect patient data in digital exchange. CSPs can help reduce fraud and reinforce trust through identity verification identities, issue electronic credentials, and manage those credentials for users accessing online services and systems, could improve access to health information more securely. In our experience, most patients are unaware that a third-party has attempted to use a patient directive to request their PHI or the range of potential implications for their PHI. They are often unfamiliar with the actual commercial entity requesting their health record on their behalf. The use of CSPs will verify and ensure the credibility of commercial third-party applications, allowing patients easier and safe access to their health information.

In the context of data exchange, our members strongly support health information interoperability and access, and we believe it can and should be achieved without sacrificing patient privacy. With new opportunities emerging with application programming interfaces (APIs) providing access to patient PHI, AHIOS believes patients should have modern tools and mechanisms to access their health information. APIs and other digital access tools must be accompanied by rigorous standards that ensure data is accessed only by authorized parties, for authorized purposes, and in ways that respect both HIPAA standards and patient expectations. AHIOS members are committed to ensuring that access to PHI is available where appropriate yet strictly limited to authorized use cases to prevent inappropriate access and maintain data security and compliance.

The reality is that PHI is, and can be, shared with recipients who are not required to safeguard a patient's PHI. While we understand that many data requesters are authorized to receive PHI for legitimate purposes, our member organizations have seen an increase in fraudulent record requests made to obtain a patient's sensitive medical information. We are concerned that an increasingly data-rich digital environment has become an even more attractive target to bad actors. Data breaches have been on the rise for the past nine years, with an upward trend in the number of compromised medical records. In 2023 alone, 725 data breaches involving 500 or more records were reported to the U.S. Department of Health and Human

Services' Office for Civil Rights[1], impacting over 133 million records. As access to health records continues to evolve, in the absence of a modernized patient privacy and security regime, we are concerned that the frequency of data breaches will also increase, leading to a rise in fraud across the health care industry, including programs like Medicare and Medicaid.

IV. Operational Realities and Professional Standards

AHIOS brings unique operational expertise through its deep experience managing the ROI process across diverse settings in the health ecosystem. We recognize that the ROI process is exceptionally complex due to the interplay of numerous regulations, diverse EHR systems, and various document management platforms. Our commitment to continually updating our *"Release of Information (ROI) Process"* report – now 45+ steps reflecting the complexity of navigating legal, regulatory, and technical requirements.

To ensure that privacy and compliance are preserved amidst increasing demand and record digitalization, AHIOS maintains rigorous training standards including the CRIS designation for ROI staff (Certified Release of Information Specialist). This operational knowledge base is critical to supporting federal efforts to modernize the health data ecosystem and reflects our dedication to best practices.

V. Data Access and Integration

While TEFCA aims to provide a unified framework for national health information exchange, its implementation must proceed with caution. As stated above, AHIOS strongly opposes any movement toward mandatory participation. TEFCA must unequivocally remain a **voluntary** mechanism for data exchange.

- **Cybersecurity Concerns**. Mandating such a singular network poses an existential risk; a significant cybersecurity breach within a centralized system could precipitate a catastrophic compromise of the entire healthcare data infrastructure, endangering both patient privacy and, more critically, patient safety on a national scale.
- **Lack of Patient Transparency**. AHIOS is deeply concerned by the lack of explicit patient consent and comprehensive transparency regarding how their sensitive health data is utilized and reused once it enters the TEFCA network, potentially undermining patient trust and control.
- **Implementation Costs.** This apprehension is compounded by the inherent complexities and substantial financial costs associated with implementation, which, if not meticulously managed, threaten to create disparate access and exacerbate existing market imbalances, inadvertently stifling innovation and fostering anti-competitive environments to the detriment of equitable and widespread health data exchange.

AHIOS recommends maintaining multiple, secure exchange options to ensure patients can access their data efficiently through trusted channels that meet regulatory standards. Fit-for-purpose solutions can help streamline and accelerate access to patient-requested records while maintaining compliance. AHIOS member organizations also collaborate with third-party applications that abide by security rules under HIPAA and are approved under the trusted exchange framework, allowing members to provide patients with access through personal health record apps or mobile health platforms patients already utilize.

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/

VI. Recommendations

To support a resilient and patient-centered data ecosystem, AHIOS provides the following key recommendations to CMS:

1. **Build Trusted Exchange on Clear and Specific Use Cases Centered on Patient Care:** Clear and consistent definitions of appropriate exchange purposes focused on treatment and improving patient outcomes are critical to the success of a trusted exchange framework to avoid confusion, misuse, abuse, and erosion of trust.

2. **Preserve TEFCA as Voluntary and Provide Oversight to Prevent Anti-competitive Behavior**: TEFCA participation should remain strictly voluntary to avoid impeding innovation, advantaging incumbents, creating unnecessary duplication of efforts, and ensuring responsible allocation of taxpayer resources. CMS/ASTP/ONC oversight must exist to prevent dominant entities from stifling competition and innovation in healthcare data exchange.

3. **Enhance Emphasis on TEFCA Privacy & Security:** CMS/ASTP/ONC should apply oversight of TEFCA to ensure that all participating network entities consistently protect patient privacy and comply with evolving privacy and security regulations. Robust security and identity management protocols will be critical to building trust and growing participation. Federal regulators should implement privacy and security standards that strike an optimal balance, actively encouraging beneficial uses of health data (e.g., for treatment or research) while simultaneously preventing and mitigating misuse.

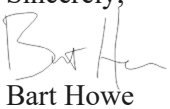
4. **Develop Clear and Accessible Patient Consent Mechanisms:** Implement clear, understandable language and user-friendly processes for patient authorization of data use, including a simple and accessible mechanism for revoking consent.

5. **Foster Collaborative Cybersecurity Solutions:** Promote collaborative efforts among stakeholders to develop effective cybersecurity solutions enhancing protections without imposing unintended or financially burdensome consequences on health care providers and businesses.

6. **Educate Patients on Data Sharing Risks:** Implement initiatives to educate patients on the implications and potential risks of sharing their PHI with third-party applications and entities outside of HIPAA's direct oversight.

AHIOS appreciates the opportunity to provide these comments and stand ready to partner with federal agencies to protect patient date, promote access, and foster a robust, competitive, and trustworthy health technology ecosystem for the benefit of all Americans.

Sincerely,



Bart Howe
President
Alliance for Health Information Operations and Standards (AHIOS)