June 16, 2025

Dr. Mehmet Oz, MD
Administrator
Centers for Medicare and Medicaid Services
U.S. Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

Dr. Thomas Keane, MD, MBA
Assistant Secretary for Technology Policy
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW, Floor 7
Washington, D.C. 20201

Submitted Electronically

Re: Health Technology Ecosystem RFI (RIN 0938-AV68)

Dear Dr. Oz and Dr. Keane:

Thank you for the opportunity to comment on the Centers for Medicare and Medicaid Services (CMS) and Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT (ASTP/ONC) RFI related to the Health Technology Ecosystem.

Epic envisions a robust ecosystem that prioritizes patient access to their own information, ensures physicians can base care decisions on their patients' complete and accurate medical records, and reduces abrasion through better communication between payers and providers. While the industry has made significant progress, more can be done. We support CMS and ASTP/ONC efforts to broaden the foundational infrastructure available to the ecosystem.

National Healthcare Directory

CMS' plan to build a national healthcare directory, starting with providers, is critical to achieving a thriving digital healthcare ecosystem. The United States lacks a single, reliable source of truth for the most basic information about physicians, such as their practice location, contact information, and specialty. This causes significant problems throughout the ecosystem—patients can be referred to the wrong physician location and insurers can inadvertently deny legitimate claims for payment from physicians whose information is out of date.

CMS should embrace three principles as it builds the directory. First, a unified national directory should have federated inputs with an unambiguous source of truth for each data element. Second, a national directory should have strong governance to manage data quality. Finally, access and updates to the directory should be automated. Machine-to-machine communication reduces human error and workload burden while speeding updates. It requires interoperable standards with which all insurers and providers can comply.

Digital Credentials

A common digital identity infrastructure, implemented thoughtfully and with careful governance, offers the potential to streamline access, strengthen trust, and reduce administrative costs across the healthcare system. Digital identity credentials can play an important role in establishing identity and make it easier for patients to access their health information in the custody of various providers.

As custodians of Protected Health Information (PHI), covered entity (CE) providers are responsible for managing PHI and informing patients about its use through Notice of Privacy Practices and other consents. Following identity proofing and patient matching, CEs should continue to be responsible for obtaining patient authorization before disclosing PHI to patient-facing third-party apps. This empowers patients to control their own health data through consent.

TEFCA

The Trusted Exchange Framework and Common Agreement (TEFCA) is the most critical foundational piece of the ecosystem's infrastructure. TEFCA allows a participant to plug in once and have trusted connections throughout the country. We look forward to continuing increases in net connectivity as providers who have never participated in other national frameworks join TEFCA. TEFCA has already expanded use cases beyond treatment to individual access and public health. ASTP/ONC should expand purpose-built use cases further. It is particularly important to create a new payment use case that would eventually become a required response.

TEFCA should also implement a government benefit eligibility use case. Allowing the electronic exchange of medical records for Social Security disability eligibility determination through the framework would have a profoundly positive impact on the lives of disabled Americans who today wait an average of seven months for eligibility determinations. The electronic exchange of information can cut eligibility determination time in half. More than 90% of healthcare organizations submitting records to the Social Security Administration (SSA) electronically do so through Epic, accounting for 2.5 million record exchanges last year. A TEFCA use case will help broaden adoption by the industry so that people with disabilities will not be left in poverty for months waiting for paper medical records to be shipped.

To avoid the serious governance problems other exchange frameworks have encountered, we encourage the government to ensure TEFCA has the resources it needs to properly police the framework so that patient data is not exploited for inappropriate purposes.

Certification and Standards

Many aspects of the ASTP/ONC Health IT Certification Program not related to interoperability have outlived their usefulness. The program should be streamlined to focus primarily on interoperability and standards-based data exchange. Standards-based data exchange has significantly improved discrete data access for patients, caregivers, app developers, and other tech vendors. For example, third-party apps made over 111 billion U.S. Core Data for Interoperability (USCDI) FHIR API calls across our customer community in the last year, enabling a broad range of app integration. More than 750 patient-facing apps used open Epic APIs to help patients retrieve their health data from Epic customer systems in the last year.

An example of standards-based work that ASTP/ONC could help advance is the exchange of medical images. Epic has long facilitated the exchange of reference-quality key images, enabling physicians to view images alongside radiology reports. We are now working to expand exchange to full diagnostic-quality DICOM images, removing the current patient burden of bringing their images with them on a DVD. Unfortunately, DICOM exchange today is a patchwork of proprietary solutions. We encourage ASTP/ONC to set standards so images can move across various technologies, cut waste, and accelerate patient care.

In addition, CMS should promote broader adoption of the USCDI standard among organizations that have not adopted standards-based exchange because they do not use certified health IT. This includes standalone diagnostic labs, imaging centers, pharmacies, and long-term and post-acute care facilities. Despite managing a vast, clinically relevant set of patient data, many of these organizations can't easily interoperate inside the ecosystem, creating significant abrasion for patients, providers, and payers.

Conclusion

Every day, organizations using Epic's software demonstrate the value of a strong health information exchange ecosystem. Last month alone providers used Epic to exchange more than 700 million patient records to inform treatment. Half of those exchanges were with healthcare organizations using other vendors' EHRs. As a more detailed example, two provider systems using Epic, Sutter Health and Stanford Health Care, exchange 38,000 records each day through our Care Everywhere interoperability platform. This open exchange of information directly improves patient outcomes. Over the past year, external data exchanged through interoperability drove more than 10 million automated point-of-care drug interaction advisories that led providers to change their medication plan, ensuring patients received the most suitable treatment.

We look forward to working with CMS, ASTP/ONC, and stakeholders throughout the industry to advance the ecosystem for the benefit of patients and the health care organizations serving them.

Attached are detailed recommendations.

Sincerely,

Ladd Wiley
Senior Vice President for Global Corporate Affairs, Public Policy, and Advocacy

I. Nationwide Healthcare Directory

This section includes Epic's comments on PC-12, PR-5, PR-10, PA-4, TD-5, TD-14, and VB-15.

The government should establish a robust, nationwide directory to ensure all members of the digital healthcare ecosystem—providers, hospitals, clinics, payers, health plans, public health systems, health data utilities (HDUs), health information exchanges (HIEs), regional health information organizations (RHIOs), and government agencies—can be reached for secure data exchange. Establishing a national healthcare directory will play a foundational role in creating a more interoperable, API-driven healthcare system. By enabling accurate, up-to-date information exchange over a trusted exchange framework, the directory can support essential patient, caregiver, and administrative use cases.

A. The unified national healthcare directory should have federated inputs with an unambiguous source of truth for each data element

The directory should be a unified database populated by the unambiguous source of truth for each data element needed by the ecosystem. CMS should own provider identity, including name and National Provider Identifier (NPI), since the National Plan and Provider Enumeration System (NPPES) is the primary source for provider identity information. Other organizations should be the source of truth for their relationship with the provider. This hybrid model—centralized identity, federated context—is the only approach that acknowledges the realities of today's healthcare operations and positions the national directory as a trusted, scalable foundation for interoperability. Without it, the government risks recreating the same disjointed, error-prone directory infrastructure that it aims to replace.

NPPES should be the ecosystem's provider identity core, and should be narrowly focused on its core competency—tracking the identity of healthcare providers and facilities and their corresponding NPI numbers. Contextual data elements that define the relationship between actors should be updated by the organization (e.g., payers, hospitals, clinics) with the clearest operational responsibility for the information. These organizations' operational workflows depend on accuracy of contextual data and they will have the knowledge and motivation to keep it correct.

Members of the ecosystem must be recognized as authoritative primary data sources and not just passive data consumers. Healthcare provider organizations maintain real-time provider practice location and specialty data because it is essential to their daily operations, for example. They should, therefore, be responsible for updating the national directory with this information. Likewise, payers should be responsible for updating the directory with the contextual elements they define, control, and monitor, such as in-network status. Licensing and credentialing bodies are best positioned to update a provider's licensing and credentialing status. Each actor should be responsible for updating the directory with its own contextual data and FHIR endpoints.

By attaching attributes to the relationship between the actors, the directory can address one of today's common challenges: physicians who practice at multiple locations. For a provider who practices at two or more facilities, entries from multiple facilities will point to that provider's single identity (maintained by CMS in NPPES). With a directory tracking the relationships between actors, multiple concurrent relationships can coexist.

B. The national directory should have strong governance to manage data quality

1. Eliminate reporting to multiple directories

CMS should ensure that every data element flows into the national healthcare directory only once, from its appropriate data steward. For example, provider organizations should be responsible for updating contextual information about individual providers (e.g., practice location, contact information, and specialties) only once to the national healthcare directory, and not to NPPES or the Provider Enrollment, Chain, and Ownership System (PECOS) separately. Existing databases such as NPPES would contribute solely the unique information they own, while shared attributes would be populated by the appropriate primary source. This would keep the national healthcare directory a single, federated source of truth.

If other government or private-sector databases need the information, the data should come from the unified national directory. For example, NPPES' function as a repository of digital endpoints should be eliminated. NPPES' failure as an accurate repository is well established and understood by CMS. A CMS taskforce determined that "NPPES was not originally designed to hold, validate, and maintain digital contact information required to 'appropriately describe the endpoints for FHIR.'" The taskforce also emphasized that "NPPES cannot sufficiently capture the data complexity necessary to fully facilitate electronic data exchange." At various points in time, government reviews determined that NPPES was missing endpoints for almost 3 million providers, and that the majority of addresses and FHIR endpoints that providers had submitted were invalid.[1]

As another example, PECOS should no longer require updates directly from providers and should instead obtain contextual provider information from the national healthcare directory. Similarly, insurers should obtain core contextual provider information from the national directory and no longer require direct provider inputs.[2]

2. Align TEFCA with the national directory

TEFCA is quickly becoming the ecosystem's foundation. Its nationwide network, backed by a common trust framework and representative governance, is where real-time data exchange is increasingly taking place. Because TEFCA is designed to support many use cases through a single on-ramp, it naturally serves as a unified transaction layer for many of the same use cases the national healthcare directory is meant to enable. The Department of Health and Human Services (HHS) should pursue alignment between TEFCA and the national healthcare directory.

At the heart of TEFCA is a high-quality directory of participating organizations, including their endpoints and locations, across the network. TEFCA does not support provider data today, but it will in the future as new use cases are added. If TEFCA and the national healthcare directory are not aligned, there is significant risk of overlap that would result in two competing sources of truth, fragmenting provider data and leading to duplicative maintenance work between CMS and ASTP/ONC. With a direct connection to operational systems and live exchange, TEFCA's directory would be superior for use in real-world workflows while the

[1] Federal Register, "National Directory of Healthcare Providers & Services RFI," https://www.federalregister.gov/documents/2022/10/07/2022-21904/request-for-information-national-directory-of-healthcare-providers-and-services

[2] Council for Affordable Quality Healthcare, "The Hidden Causes of Inaccurate Provider Directories," https://www.caqh.org/sites/default/files/explorations/CAQH-hidden-causes-provider-directories-whitepaper.pdf

national healthcare directory would become an obsolete parallel directory disconnected from operational use.

To avoid this, the government should develop a roadmap that harmonizes the national healthcare directory with TEFCA. CMS and ASTP/ONC should ensure that TEFCA can reference or use the national healthcare directory, and that the national healthcare directory can leverage TEFCA participants as trusted, vetted, primary sources of real-time provider directory data. The national healthcare directory could even be built on top of the TEFCA directory, with connectivity options for non-Qualified Health Information Network (QHIN) participants. TEFCA could be a path for trusted, vetted sources to automatically exchange required data elements with the national healthcare directory. This alignment will significantly speed the creation of the national healthcare directory.

3. Improve data quality through automated validation and routine audits

To improve efficiency in the healthcare system, the national healthcare directory must remain current and reliable. Even a small amount of outdated or inaccurate data will undermine trust. To address this need, CMS should implement a robust plan for validation, attestation, and monitoring.

The first step is validation as data is entered into the directory. CMS should implement data cleanliness checks for updates, such as verifying address formats, taxonomy codes, and deactivation status. FHIR endpoints can be verified on submission and on a rolling basis by ensuring that they are online and accessible.

The second step is ongoing attestations from directory participants (individuals, facilities, payers) that information is still current. CMS should use automated reminders to prompt participants to either update their information or attest that it remains accurate. CMS could consider measures to encourage compliance, such as flagging entries and sanctioning actors who fail to meet annual attestation.

Finally, CMS should appoint a dedicated directory quality officer to lead a multi-stakeholder panel responsible for defining data quality metrics, conducting audits, offering guidance, and publicly reporting on the quality of data sources and the overall integrity of the directory.

C. Access and updates to the directory should be automated

Automated, machine-to-machine communication reduces human error and burden while speeding updates. Automated updates will enable real-time directory data, which is necessary to facilitate workflows like checking if a provider is in-network, or for reliably routing a referral. The directory should prioritize API-based, machine-readable infrastructure over static portals or self-attested files.

Portals should be eliminated from routine use and be available only as a fallback for participants lacking technology for automated submissions. NPPES currently requires individual providers to update their information and suffers from non-timely and incomplete reporting. To facilitate reliable and automated updates, submissions of provider directory data should, when possible, be provided by healthcare organizations' systems (not individuals) that have the means and infrastructure to track provider information and implement automated APIs.

Machine-to-machine communication requires common adoption of a healthcare directory specification to both contribute data to the directory and read it back. CMS and ASTP/ONC should build the national healthcare directory as an implementation of an open, interoperable, FHIR directory specification (e.g., Mobile Care Services Discovery or FAST's National Directory of Healthcare Providers and Services).

II. Patient Digital Identity

This section includes Epic's comments on PC-14, PR-9, PR-10, PR-11, PA-3, PA-4, TD-3, and VB-14.

A. Credential Service Providers

Implemented thoughtfully and with careful governance, optional use of digital identity could help streamline access, strengthen trust, and reduce administrative costs across the digital healthcare ecosystem. Provided appropriate patient matching and authorization occurs, the optional use of Credential Service Providers (CSPs), such as CLEAR and Login.gov, could give patients more choices for managing multiple portal logins without requiring a password. Identity credentialing policy for releasing patient data to third party apps must address the full identity lifecycle—verification, patient matching, and authorization.

1. Identity verification through CSPs

CSPs establish identity in conformance with Identity Assurance Level 2 (IAL2) requirements. IAL2 verifies strong identity evidence, typically a government-issued picture ID, that is compared with a person's face. Once identity is established, a CSP provides a reusable digital credential. Epic's software already includes features to support Kantara-approved CSPs. Some of our customers are using IAL2 identities for workflows such as onboarding patients to the portal from home, automating patient portal account recovery if a patient loses their password, and allowing patients to arrive at a clinic and check-in without staff involvement. When a provider is asked to disclose a patient's information to a third-party app, a digital credential could help affirm the patient's identity.

2. Patient matching after identity is established

While identity verification confirms who a person is, patient matching ensures that identity is linked to the correct medical record in the provider's database. In healthcare, mismatches can compromise patient safety, lead to duplicate records, or result in privacy breaches and improper data access. To illustrate the problem, one health system found 231 patients with the same name and the same date of birth—some may be duplicates; others are distinct individuals.[3] In addition, demographic information often changes over time as patients legally change their names, move to new addresses, or switch phone numbers.

Once IAL2 identity is established, the best way to support no-password-required portal access begins with assessing whether a disclosing party has previously associated the IAL2 digital identity to a patient's chart. The association might exist because a digital credential was established at the creation of the portal account—meaning there is a consistent CSP identity connecting the portal to the person seeking access. In some cases, the CE may seek independent verification from the patient, such as in cases of chart

[3] PRLog, "Harris County Hospital District Puts Patient Safety in the Palm of Your Hand," https://www.prlog.org/11430165-harris-county-hospital-district-puts-patient-safety-in-the-palm-of-your-hand.html

merges and suspected identity theft. After an associated chart is confirmed, the disclosing party would grant access to the app that electronically presented the IAL2 digital identity (through an associated ID token or Security Assertion Markup Language (SAML) assertion).

However, digital identity is often not already associated with a patient's chart in advance of app requests because it is impractical for all portal account creations to use the IAL2 process. Some providers may choose to use other processes such as enrolling patients during offices visits. Some patients, such as children without government-issued identification, may not be able to undergo IAL2 verification. It would be inappropriate to deny these patients portal access to their health information.

In these scenarios, if the associated demographics are sufficient to identify the individual in the discloser's database, the discloser would send a multifactor authentication (MFA) message to a known phone number (or other contact) in the patient's record to confirm the correct person before allowing access to the portal. Provided MFA matches the person, no password is required for portal access.

Where there is no existing identity association or demographic match, a manual workflow such as a login and password would be required. Policy frameworks should recognize that patient matching is a requirement distinct from identity verification, and that it merits its own implementation safeguards.

3. Consent and authorization

Once identity is confirmed and there is a matched patient, authorization—the patient's consent to release specific health data—is a critical step before a custodian releases the patient's health data. While identity verification and patient matching respectively ensure that the patient is who they claim to be and that the right chart is found, authorization ensures lawful and appropriate use and disclosure.

CEs are directly responsible for managing authorization and for the legal and clinical implications of inappropriate disclosures. Federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA), require that CEs maintain control over disclosure decisions. CEs are also bound by state regulations, which often go further than HIPAA by outlining consent requirements for highly sensitive data or complex privacy restrictions, such as HIV status, intimate partner violence, known data breaches, or provider safety concerns.

To facilitate no-password-required portal access, after identity is established and there is a matched patient, the patient would use Open Authorization (OAuth) to authorize release of the information to the app. OAuth is a modern technology standard used to grant apps access to information without giving a password. It has been adopted by major Internet leaders, including Facebook, Google, and Microsoft. As a result, patients are already familiar with this workflow from their experiences in other industries, such as linking food delivery apps to their Google account.

Within healthcare, OAuth has already reached widespread adoption and is included in ASTP/ONC certification criteria.[4] It is widely successful with both SMART and patient access FHIR APIs and has been formalized within TEFCA.

[4] 45 CFR § 170.315 (g)(10)(v)(B) requires support of SMART Backend Services: Authorization Guide, which in turn requires OAuth 2.0.

Using the OAuth workflow, the patient confirms which clinical data they wish to release and the length of time the app is authorized to request updates. This creates transparency regarding precisely what data will be released, for how long, and to whom. It also ensures the CE captures appropriate patient authorization. The fact that an app has an identity token is not sufficient to assume patient authorization. For instance, people using a CLEAR identity linked to an airline app would not want the airline to be able to access their health data simply because it has a verified identity token. Consent must be managed and processed by the entity disclosing the data. For the discloser to manage consent in an automated system, they must know the content of the consent, a requirement not satisfied by simple attestations from the app requesting the data.

Authorization between the patient and the CE puts the patient in control of when, where, and to whom data is released because it provides the opportunity for a patient to thoughtfully select whether to unlock health data to particular apps, along with choosing which data and for how long the app can request updates.

4. Access on behalf of other patients

People often use portals or other health apps as an authorized representative (proxy) to manage care for their children, aging parents, or others for whom they are acting as a caregiver. In this case, verifying a caregiver's identity alone would not confirm that a proxy relationship has been granted by the people whose care they are managing.

The relationship between legally authorized proxies and patients is explicitly defined and captured in the patient record when one or both parties (patient and proxy) make their choice known to the provider involved in the patient's care. This is something that is known and then verified by the provider/organization with the consents they have on file. Once these mappings and authorizations are on file at the CE, the proxy requesting access with their digital identity credentials can be given access to data from other patients as defined by those mappings and authorizations.

B. Other forms of digital identities should be supported

The government should not mandate an approach to digital identities that results in proprietary identity tokens. Other forms of digital identity, such as mobile driver's licenses stored on smartphones or platform-managed passkeys, are alternatives that can meet user needs while expanding access. Passkeys have already gained traction with users in other industries, such as finance and airline travel. Some of Epic's customers support passkeys for MyChart access, and are now seeing over 1,400 patients enroll per day, signaling strong consumer interest in alternatives to passwords.

Similarly, state-issued mobile driver's licenses (ISO 18013-5[5], ISO 18013-7[6]) are live in 14 states and supported by Apple and Google Wallet. Mobile passports are live for Android users today and coming to iOS in the fall of 2025. These technologies signal an industry shift toward patient-mediated identity that is free for all patients, apps, and health systems to leverage with no financial burden.

Finally, some individuals may not want to provide sensitive documents or biometrics to CSPs, and CMS should not mandate that they share personal information with third parties just to access their own health information. A login-and-password solution should be maintained as an option for these individuals. While

[5] ISO, "ISO/IEC 18013-5:2021," https://www.iso.org/standard/69084.html
[6] ISO, "ISO/IEC TS 19013-7:2025," https://www.iso.org/standard/91154.html

CSP-managed digital identities clearly have an important role to play, CMS should avoid mandating a single approach that could stifle innovation, enable regulatory capture, or fail to accommodate the spectrum of identity options that patients prefer.

C. Governance of digital identities

1. CSPs should be interoperable

To contain the spread of "portalitis," the government should not inadvertently spread "credentialopathy," a related, but distinct, identity-verification condition. The five Kantara-approved CSPs (1Kosmos, CLEAR, Exostar, ID.me, and Login.gov) do not interoperate with each other, which forces patients and providers to repeat proprietary identity verification when apps use different CSPs. This fragmentation increases cost and complexity without improving patient experience.

Establishing standards for cross-walking identities between CSPs would reduce proprietary identity verification burdens on patients and reduce onboarding and integration costs for app developers. It would also simplify workflows for providers by allowing cached tokens from one CSP to be used across systems, promoting a competitive and dynamic marketplace that supports consumer choice.

2. Patients should be able to revoke and audit digital identity use

Individuals should have meaningful control over how their identity is used and shared. CSPs must give patients the ability to revoke identity tokens entirely or on a per-application basis, including offering both universal and app-specific revocation tools, and enabling patients to pause or permanently disable digital identities. CSPs should also provide APIs allowing a CE to check identity revocation before disclosing patient data.

In addition, patients should be able to view when and where their digital identity has been used, including which apps accessed it, and from which CEs they requested data. This capability is essential in situations involving fraud, identity theft, suspected misuse, or changes in personal circumstances. For example, a patient concerned about overuse or misuse of their identity should be able to suspend its use without needing to contact each individual app or provider. CSPs should be required to provide real-time, patient-accessible audit trails showing where and how identity tokens have been used.

3. CSP standards

Kantara currently certifies CSPs that meet National Institute of Standards and Technology (NIST) 800-63A IAL2 standards. As the market evolves, the list of certified providers will grow and change, and the industry will need a real-time, digital source of truth to identify certified CSPs. With potentially millions of automated identity checks and disclosures every hour, this should be a real-time API to define the list of certified CSPs. This API and digital directory could be maintained by Kantara, CMS, or another designated body.

Governance policy should also require monitoring of CSP success rates, with results being made public. Specifically, CSPs should benchmark their patient matching success rates annually against a CMS-curated population and file a report of their test results, including rates of true/false positives and true/false negatives. The test population should be curated to include populations that are likely to be disadvantaged

in digital identity verification, such as those with name changes after marriage, twins (both pediatric and adult), newborns, the homeless, and people who frequently change addresses, such as military personnel. Epic can contribute to creation of the test population.

4. Liability

In addition to establishing standards for identity verification and authentication of users, CMS should require CSPs to meet standards for secure transmission of transactions. TEFCA has already adopted NIST IAL2 and AAL2 standards to ensure that CSPs follow the same standards for identity verification and ongoing authentication of users. NIST also defines Federation Assurance Levels (FAL) to define the standards CSPs use to securely transmit an identity to another app. CMS should require FAL2 or FAL3 and work with Kantara so that CSPs meet those standards. This will ensure that the identity transmission process is trustworthy across the healthcare ecosystem.

As digital identity solutions mature, HIPAA regulations should evolve to reflect the shared responsibilities between CEs and third-party CSPs. Under current rules, CEs bear liability for inappropriate disclosures, even when a disclosure results from an error in a third-party identity service they do not control. CSP errors have already caused inappropriate disclosures. In one case we're familiar with, a health system using a Kantara-approved CSP in a production environment linked an identity to the wrong patient chart within the first weeks of use, resulting in a consumer accessing a different person's medical information through a patient portal. HIPAA does not currently hold the CSP accountable for their error.

This misalignment of responsibility creates a disincentive for adoption. In order for policy to encourage CEs to support automated disclosures via third-party CSPs, it must allocate liability in a way that reflects operational control. To that end, HIPAA should be updated to extend liability to CSPs and app developers when unauthorized disclosures result from their errors and provide a safe harbor for CEs when they rely on verified digital identity assertions from CSPs.

III. TEFCA

This section includes Epic's comments on PC-10, PC-11, PC-12, PR-6, PR-7, PR-8, PR-11, PA-1, PA-2, TD-2, TD-6, TD-7, TD-11, TD-12, TD-13, TD-14, TD-15, TD-16, and TD-17.

TEFCA, as a federally endorsed trust framework, is in the best position to establish a true foundation for nationwide interoperability. At a year and a half in operation, TEFCA has achieved much faster adoption than other exchange networks at similar points of maturity. Healthcare organizations using Epic's software have already connected more than 1,150 hospitals and 25,500 clinics, and another 1,050 hospitals and 23,750 clinics are actively implementing. As more provider organizations go live over the next six to twelve months, TEFCA will see exchange numbers increase rapidly and will become the nation's primary exchange framework, with legacy frameworks, such as Carequality, becoming obsolete.

A. Expand TEFCA's use cases

The best way to promote interoperability adoption is through purpose-built uses case that benefit both parties exchanging EHI. CMS and ASTP/ONC should:

1. Create mandatory support for payment and operations use cases

ASTP/ONC should create a roadmap for required responses for payment use cases that aligns with CMS' 0057 Final Rule, which includes support for provider access, prior authorization, patient access, and payer-to-payer. TEFCA could scale adoption of these required APIs that otherwise would be point-to-point connections.

As TEFCA expands to mandatory payment response, CMS will have an opportunity to exchange with an existing broad set of providers in its role as the country's most influential payer. Alongside CMS participation, all payers offering Medicare Advantage (MA) plans could be required to participate, with the possibility of conditioning reimbursement on a provider's participation in TEFCA in the future.

2. Expand use cases for treatment-based interoperability

Epic is making image exchange work better for patients, so that they will no longer have to use DVDs to bring images to appointments. We have long exchanged reference quality images and are now working to exchange diagnostic-quality images. By publishing clear implementation guidance using existing standards (FHIR ImagingStudy and DICOMWeb WADO-RS), TEFCA would scale adoption throughout the ecosystem.

Another opportunity is to include push-based use cases, such as closed loop referral coordination, post-discharge care coordination, and event notifications. Today, these use cases require intermediaries, such as Health Information Service Providers (HISPs). TEFCA adoption of 360X can significantly streamline referral workflows and enhance patient outcomes. For example, Sutter Health used electronic referrals to shorten referral scheduling by 20 days, largely because 97% of electronic referrals contain all needed information (previously only 30%).

3. Expand public health use cases

Electronic Case Reporting (eCR) is live on TEFCA and has the potential to save millions of dollars spent on administrative tasks. In March 2025, more than 3.3 million case reports were submitted electronically through TEFCA. HHS through Centers for Disease Control and Prevention (CDC) grant conditions or Medicaid program requirements) should incentivize public health authorities to adopt TEFCA and encourage states to waive manual submission requirements for healthcare organizations that use TEFCA for case reporting. Our customers estimate eCR saves three to five minutes per case. Other public health use cases could be supported using FHIR transactions for electronic case investigation, cancer reporting, adverse event reporting (such as Vaccine Adverse Event Reporting System (VAERS)), and syndromic surveillance.

4. Support government benefits determination

TEFCA should implement government benefits eligibility determination to allow the SSA to receive electronic health records for disability benefits determinations. Epic has partnered with the SSA for years. As a result, more than 90% of healthcare organizations submitting records electronically do so through Epic. Claim determination is 50% faster when electronic health records are available.[7] Supporting record sharing for benefits determination through TEFCA could broaden this capability.

[7] SSA, "Healthcare Providers Can Help Social Security Improve the Disability Process," https://blog.ssa.gov/healthcare-providers-can-help-social-security-improve-the-disability-process/

B. Governance

Today, the majority of interoperable healthcare organizations exchange information through data-sharing networks such as Carequality. While these networks have advanced interoperability for treatment, they have minimal use case expansion, and their lack of effective oversight and enforcement mechanisms have led to privacy concerns.

By institutionalizing a robust compliance infrastructure, ASTP/ONC can ensure TEFCA will continue to reduce information silos and foster innovation across the healthcare ecosystem. To avoid the flaws encountered in private-sector national networks, HHS should:

- Prohibit data brokers and intermediaries from siphoning patient records to monetize through secondary markets.
- Empower CEs that are required to disclose sensitive patient data in response to network requests with the final say on governance, rather than vendors.
- Act as a neutral party to keep patient data safe by providing oversight and "policing" TEFCA participants.
- Establish transparent governance structures and hold all parties involved in governing TEFCA accountable to the public through periodic performance evaluations.
- Use the A-19 process to request Congress pass legislation that holds all TEFCA participants accountable for protecting patient privacy under HIPAA, and places liability on the appropriate actor if violations occur.

IV. Health IT Certification Program and Standards

This section includes Epic's comments on TD-8 and TD-9.

Epic supports narrowing the ASTP/ONC certification criteria to focus on interoperability. Many non-interoperability certification requirements have outlasted their usefulness. Specifically, we recommend ASTP/ONC remove the Insights Condition and the Real-World Testing requirements of the certification process. These components add significant certification burden and present minimal benefit.

In addition, ASTP/ONC should structure an effective certification process that ensures each party to a data exchange can adhere to the same standards. To accomplish this, ASTP/ONC should define EHI Export as USCDI and continue incrementally expanding USCDI. This provides a pathway to advance interoperability that can be both generated and consumed without special effort. Transitioning to USCDI would ensure all parties can exchange the right information which would increase interoperability more than would be possible by revising EHI Export separately.

Removing workflow and reporting requirements from the certification process while ensuring data can flow freely between participants will empower market participants to focus on true innovation and may encourage participation by groups that found the workflow and functionality-based certification process prohibitive.

V. Strengthening LLM Adoption

This section includes Epic's comments on PC-8, TD-7, TD-9, and TD-13.

Large Language Models (LLMs) offer substantial value in healthcare, especially when working with unstructured data in patient records such as clinical notes and textual diagnostic results. For example, The Christ Hospital, based in Cincinnati, Ohio, used LLMs with Epic software to track incidental findings and follow-up recommendations in diagnostic imaging reports. This initiative contributed to earlier lung cancer detection, with 70% of cases identified at stage 1 or 2, well above the national average of 27%.[8] LLMs will have the greatest utility when using USCDI datasets of both structured (e.g., laboratory results, vital signs, medications, allergies, diagnoses, and procedures) and unstructured (e.g., notes, pathology reports, and radiology reports) data.

However, adoption of LLMs should not be viewed as a replacement for existing tools that consume standards-based data exchange. Many data elements already enable risk scoring, trend analysis, and decision support. These structured formats are best transmitted and interpreted through FHIR APIs, which are both more reliable and more cost-effective than using LLMs to deduce them from unstructured notes.

EHI Export has not achieved widespread adoption as a data exchange mechanism and therefore may have limited utility as it relates to LLM adoption. Across our customer community, EHI Export accounted for only ~0.0000055% of requested medical record releases from December 2024-May 2025. Our customers have told us that EHI Export releases, which by definition include all data in the designated record set, fail to meet the needs of requestors. As a result, additional follow-up is required, often concluding with a traditional release of medical information in another format.

VI. Quality Measures

This section includes Epic's comments on PR-8, PA-5, TD-9, VB-1, VB-2, VB-3, VB-4, VB-6, VB-8, VB-9, VB-10, VB-11, VB-12, and VB-13.

A. Short-term: keep small provider groups in Medicare Shared Savings Program Accountable Care Organizations

Since 2013, CMS has required Medicare Shared Savings Program (MSSP) Accountable Care Organizations (ACOs) to report quality measures through the Web Interface Portal. The process is time-consuming and expensive, driving up costs for ACOs and patients, as it requires manual abstraction, or the cutting-and-pasting of data.

Now, CMS is transitioning from manual to digital reporting methods. This is intended to reduce provider burden and increase the total number of patients on whom ACOs report quality measures. The CY 2025 Physician Fee Schedule (PFS) Final Rule sunset the Web Interface Portal and requires digital quality measures reporting. This transition creates significant challenges, as the policy does not consider the technical capabilities of smaller practices. The reporting of eCQMs requires all practices in an ACO to

[8] American Lung Association, "American Lung Association, "New Report: Lung Cancer Survival Rate Improves, But Gaps in Biomarker Testing and Lack of Screening Hinder Progress," https://www.lung.org/media/press-releases/state-of-lung-cancer-2024

generate QRDA files, through their EHR software. While Epic has the capability to generate these files, smaller practices whose EHR vendors cannot generate the requisite files will be forced to leave MSSP ACOs.

While the transition to eCQMs is well-intended, in the short-term, CMS should provide flexibility for ACOs to exclude reporting on patients whose records are not stored in QRDA-capable EHRs, so long as CMS' overall reporting requirements are met (i.e., reporting data on 75% of an ACO's patients). This will allow ACOs to provide quality measures for most of their patients while exempting smaller practices within the ACO that do not have the capacity to report.

B. Long-Term: Bulk FHIR for data submission

In the long term, Bulk FHIR Submit is the best path toward FHIR submission for quality data using a quality-specific standard. Broad implementation across payment models would reduce administrative burden for healthcare organizations by standardizing quality measurement. This would eliminate the need for providers to collect and report different metrics across multiple programs.

CMS should allow ACOs to submit calculated data. Quality data plays a dual role for healthcare organizations: it supports regulatory reporting requirements and also drives clinical decision-making at the point of care. By embedding quality logic into workflows, dashboards, and care management programs, healthcare organizations can improve patient safety, outcomes, and operational efficiency at the point of care. Today, quality directors and physicians routinely calculate both individual and aggregate measure performance to identify care gaps and guide targeted interventions.

If CMS plans to calculate quality measures on behalf of providers, real-time feedback, per patient, from CMS will be essential to support timely action at the point of care. Without timely insight, providers risk losing visibility into their performance and may miss opportunities to intervene and improve the quality or efficiency of their care for their patients.

To support a successful transition to FHIR reporting, CMS should offer an "on-ramp" for early adopters—including clear implementation timelines, technical documentation, and sandbox environments—for both healthcare organizations and health IT vendors to test and deploy efficiently. Targeted use cases are achievable for early adopters within current capabilities if appropriately scoped and phased.

VII. Better Guidance on Information Blocking

This section includes Epic's comments on PR-12, PR-13, PR-14, and PA-7.

ASTP/ONC should focus on expanding information sharing by developing clear pathways and practices for data exchange and defining a set of actions that are not considered information blocking. This would be consistent with ASTP's mandate from Congress under the 21st Century Cures Act, would provide much-needed clarity to regulated actors, and would increase data exchange to a greater extent than increased enforcement as contemplated in the RFI.

A. ASTP/ONC should act on its obligation to define activities that are not information blocking

With the 21st Century Cures Act, Congress delegated to HHS the authority to specify "reasonable and necessary" activities that are not information blocking. ASTP/ONC has not acted on this mandate. Instead, ASTP/ONC has:

- Used its rulemaking authority to issue complex exceptions that regulated actors have found difficult to understand and operationalize.
- Taken actions outside of its mandate from Congress, including proposing vague examples of practices that are "interferences" and therefore constitute information blocking.
- Failed to provide meaningful guidance to help actors understand and navigate compliance with the complex regulatory regime.

While regulated actors have asked for a set of scenarios that do not constitute information blocking, ASTP/ONC has stated it does not have statutory authority[9] to offer guidance. This is incorrect. What the regulated community is seeking is different from binding advisory opinions such as those issued by HHS Office of Inspector General (OIG) on the Anti-Kickback Statute. Agencies like ASTP/ONC do not need additional statutory authority to provide guidance to regulated parties.[10]

B. Regulated actors need a "Safe Harbor" for actions taken to meet regulatory obligations

Rather than help regulated actors understand their responsibilities under the information blocking regulations, ASTP/ONC has created complexity and confusion that will ultimately undermine progress toward universal interoperability. ASTP/ONC has issued a series of rulemakings that have yielded a set of complicated information blocking exceptions that are over-engineered, technical, and require close review of hundreds of pages of byzantine regulatory text with numerous internal cross-references.

ASTP's recent proposals have only sowed further confusion. Regulated actors could now face penalties for taking actions they believe are necessary to protect patient privacy as required under federal law, based merely on the premise that such actions might "interfere" with data exchange. ASTP's focus on identifying *practices* that interfere as opposed to reasonable and necessary activities that are not information blocking (as the 21st Century Cures Act mandates) converts what is meant to be a facts-and-circumstances, intent-based analysis into something more like strict liability.

C. Increasing enforcement of today's vague guidelines will not increase interoperability and may discourage new market entrants

Questions in the RFI on increasing enforcement rely on two flawed premises; the first is that individuals experiencing information blocking don't know how to report it. Based on publicly available data, more than 1,300 information blocking claims have been submitted thus far. ASTP/ONC and OIG could potentially raise awareness by announcing any public enforcement activity, but it is clear from the volume of active claims that people do know how to report cases of suspected information blocking.

---

[9] ASTP/ONC, "Information Blocking and the President's FY23 Budget for ONC," https://www.healthit.gov/buzz-blog/information-blocking/information-blocking-and-the-presidents-fy23-budget-for-onc

[10] In fact, compliance guidance is required under the Small Business Regulatory Enforcement Fairness Act of 1996.

The second and more serious flawed assumption is that lack of disincentives for information blocking has caused regulated actors to resist sharing data. That isn't true. Regulated entities such as healthcare organizations and EHR developers already face substantial disincentives for information blocking. CMS programs have also required attestations related to information blocking for years.

Healthcare organizations found to be information blocking stand to lose significant CMS revenue. Developers of Certified EHR Technology (CEHRT) found to be information blocking can face civil monetary penalties and lose certifications, which would have a devastating effect on their financial health and the customers they serve. For provider organizations that do not participate in CMS programs (e.g., dentists, private pay providers), increased enforcement will have no effect because CMS has no legal mechanism to assess penalties or other disincentives.

Instead of encouraging interoperability, CMS efforts to increase enforcement as contemplated in the RFI are likely to slow innovation and impede adoption of standards-based interoperability technology. Healthcare organizations and developers of CEHRT will shift resources from research and development activities that advance standards-based interoperability to staffing the compliance officers and lawyers necessary to navigate an increasingly complex regulatory framework. Startups and other new market entrants may determine that the barriers to offering CEHRT are too high, reducing overall competition.

D. Invest in expanding interoperability

ASTP/ONC should define a clear set of activities that do not constitute information blocking so that HIPAA-covered entities understand what "reasonable and necessary" steps they can take to meet HIPAA compliance obligations if they suspect that a request for patient data is inappropriate. In addition, ASTP/ONC should:

1. Designate TEFCA as a "Safe Harbor" pathway to share information

ASTP/ONC should establish a safe harbor from information blocking enforcement for actors who are fully compliant with TEFCA's required use cases by expanding the TEFCA Manner exception. The exception should apply when a regulated actor responds to a request by making information available through the framework, regardless of whether the requestor participates in TEFCA. This would incentivize future adoption of TEFCA, reward good-faith participation in national data sharing efforts, and provide regulatory clarity to those who align with TEFCA's vision.

Additionally, regulated entities that respond to information requests through TEFCA should not be liable if the request is later found to be inappropriate.

2. Simplify the current set of exceptions

Current guidance on exceptions is lengthy, complex, and full of vague and confusing terminology requiring actors to carefully review and understand hundreds of pages of regulatory preamble text. Exceptions are too often based on hypothetical fact patterns not representative of real-world scenarios.

3. Acknowledge regulated actors that demonstrate a commitment to information sharing

Through Open.Epic we have made hundreds of FHIR and other standards-based APIs available to app developers and new market entrants at no cost, far more than the USCDI set of APIs required for ASTP/ONC certification. This is undeniably a success, with more than 750 apps exchanging data with Epic customer organizations using solely public technology.

HHS should incentivize regulated actors to make similar investments beyond what the rules require by directing OIG to consider an actor's commitment to information sharing as a mitigating factor when evaluating information blocking claims. Evidence of a commitment to information sharing could include the extent of public API availability, adoption of the FHIR standard, voluntary TEFCA membership, and other objective facts that show an actor has positive intent.

Taking these steps would remove much of the current uncertainty around information blocking rules and may have the added benefit of encouraging more healthcare organizations not subject to CMS programs (e.g., nursing homes, dentists, and self-pay providers) to begin sharing data.