CHIME® DIGITAL HEALTH LEADERS

June 16, 2025

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

Dr. Mehmet Oz, Administrator
Dr. Thomas Keane, Assistant Secretary for Technology Policy and
National Coordinator for Health Information Technology
Centers for Medicare and Medicaid Services
Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

RE: Request for Information on Health Technology Ecosystem [CMS–0042–NC]

Dear Drs. Oz and Keane:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) and Assistant Secretary for Technology Policy (ASTP)/Office of the National Coordinator for Health Information Technology (ONC) (collectively, ASTP/ONC), request for information (RFI) on the Health Technology Ecosystem, as published in the *Federal Register* on May 16, 2025 (Vol. 90, No. 94).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. With more than 3,000 individual members in 58 countries and two U.S. territories and 200 CHIME Foundation healthcare IT business and professional service firm members, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate for the effective use of information management to improve the health and care in the communities they serve.

Key Recommendations and Takeaways

CHIME's feedback addresses the questions outlined in this RFI, which seeks input from the public regarding the market of digital health products for Medicare beneficiaries, as well as the state of data interoperability and broader health technology infrastructure.

CHIME members have made substantial, ongoing investments in health information technology (IT) systems aligned with the statutory objectives of the 21st Century Cures Act and its implementing regulations – including the Office of the National Coordinator for Health

Information Technology's Cures Act Final Rule,[1] the CMS Interoperability Rules[2] as well as the Health Data, Technology, and Interoperability (HTI-1 and HTI-2) Final Rules.[3,4] Additionally, we have made substantial, ongoing investments in privacy and cybersecurity infrastructure to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations. **These efforts reflect a deep commitment to promoting data privacy, secure health information exchange, and patient empowerment through greater access to and control over their health information.**

As noted in the RFI, CMS and ASTP/ONC would like to continue to build on the existing policy framework to drive large-scale adoption of health management and care navigation applications, reduce barriers to data access and exchange, realize the potential of recent innovations in healthcare that promote better health outcomes, and accelerate progress towards a patient-centric learning health system.

CHIME members appreciate the opportunity to contribute to this important dialogue; we commend CMS and ASTP/ONC for seeking stakeholder input to guide infrastructure advancements that will expand equitable access to digital health tools, empower beneficiaries in their care decisions, and enhance data-driven collaboration across the healthcare continuum. **CHIME has and continues to be a staunch champion when it comes to the need for the use of technology standards aimed at facilitating better patient care.**

Patients and Caregivers (B), Data Access and Integration (B2), Providers (C), and Technology Vendors, Data Providers, and Networks (E)

The RFI asks how the Trusted Exchange Framework and Common Agreement (TEFCA) is currently helping to advance patient access to health information in the real world (PC-10) and to provide specific examples (PC-10, a). It also asks whether TEFCA is currently helping to advance patient and provider access to health information, and if there are adequate alternatives available outside of TEFCA (PC–10 and PR–6). The RFI also asks about the policy or technical limitations of TEFCA, and whether these hinder participation in TEFCA (PA–1), and finally, what unique interoperability functions TEFCA performs. Furthermore, the RFI asks a series of questions regarding digital identity implementation (TD-3), and what new opportunities and advancements could emerge with APIs providing access to the entirety of a patient's electronic health information (EHI) (TD-13, a).

In the RFI, CMS and ASTP/ONC welcome links to screenshots or brief video demonstrations as part of submitted feedback. **We are grateful for this opportunity, and CHIME member Baptist Health has created a brief video highlighting how TEFCA is enhancing interoperability at their organization. TEFCA facilitates secure, rapid sharing of patient health information for treatment purposes across healthcare providers.**

Baptist Health actively participates in TEFCA – connecting via Epic Nexus, a Qualified Health Information Network (QHIN) developed specifically for Epic community members. Notably, Baptist Health was the third organization in Florida – and the thirty-fourth nationwide – to join the TEFCA network, underscoring its role as an early adopter of this

[1] 85 FR 25642

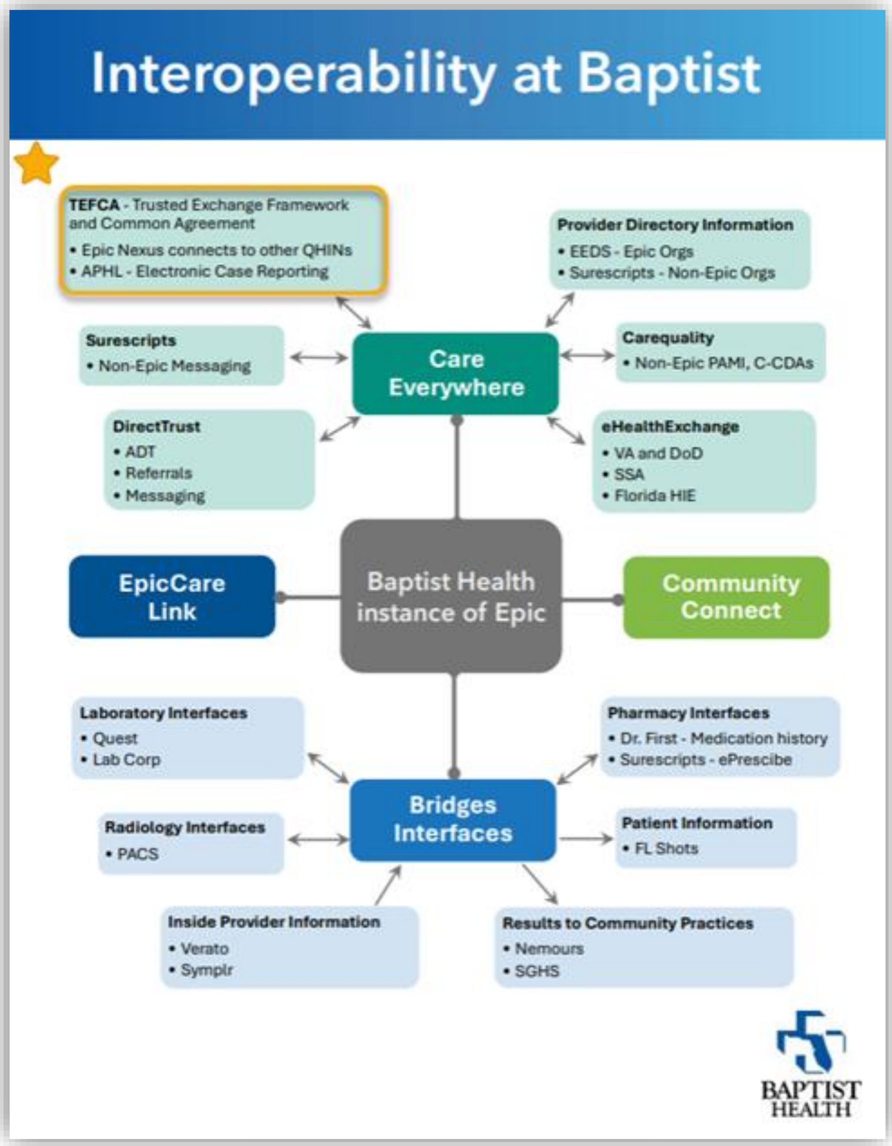
[2] "CMS Interoperability and Patient Access" final rule (85 FR 25510), and "Interoperability and Prior Authorization'' final rule (89 FR 8758)

[3] ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing" final rule (89 FR 1192)

[4] Health Data, Technology, and Interoperability: Trusted Exchange Framework and Common Agreement'' final rule (89 FR 101772)

important national framework. Through Epic Nexus, Baptist Health interacts with multiple other QHINs, significantly broadening interoperability across the entire healthcare continuum. This engagement allows Baptist Health to securely and seamlessly exchange health information across diverse healthcare settings and use cases (PR-8, PC-10, PC-11, PC-12, PR-1, PR-2, PR-3, PR-6, PR-7, PR-8, PR-11, TD-6, TD-17).

Since joining TEFCA in May 2024, Baptist Health has exchanged nearly 81,000 health records – 34,879 sent and 45,869 received – with 546 trading partners as of June 2025. Baptist Health adheres to the TEFCA Treatment Exchange Purpose Code guidelines established by TEFCA's [Recognized Coordinating Entity® (RCE).]()



Interoperability at Baptist

TEFCA - Trusted Exchange Framework and Common Agreement
- Epic Nexus connects to other QHINs
- APHL - Electronic Case Reporting

Provider Directory Information
- EEDS - Epic Orgs
- Surescripts - Non-Epic Orgs

Surescripts
- Non-Epic Messaging

Care Everywhere

Carequality
- Non-Epic PAMI, C-CDAs

DirectTrust
- ADT
- Referrals
- Messaging

eHealthExchange
- VA and DoD
- SSA
- Florida HIE

EpicCare Link

Baptist Health instance of Epic

Community Connect

Laboratory Interfaces
- Quest
- Lab Corp

Pharmacy Interfaces
- Dr. First - Medication history
- Surescripts - ePrescibe

Bridges Interfaces

Radiology Interfaces
- PACS

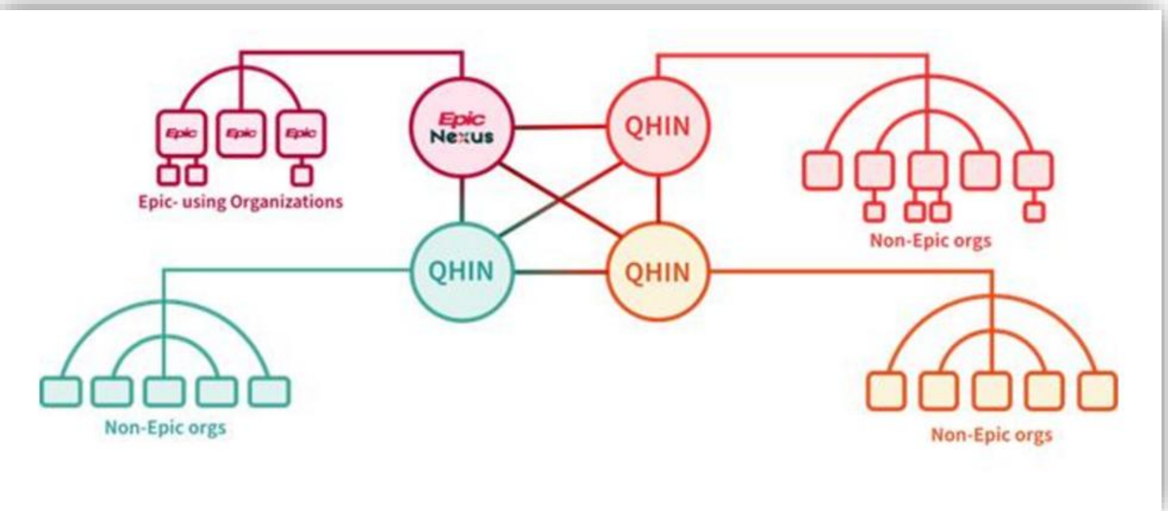
Patient Information
- FL Shots

Inside Provider Information
- Verato
- Symplr

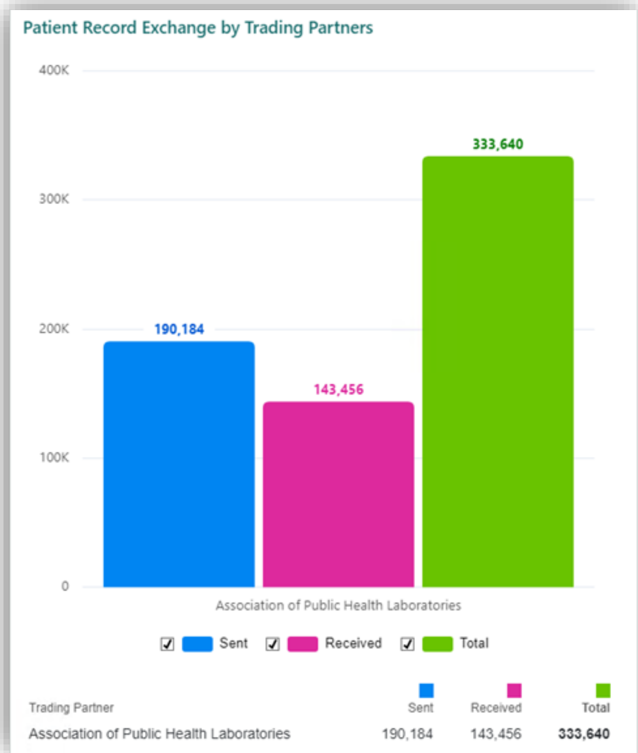
Results to Community Practices
- Nemours
- SGHS

BAPTIST HEALTH

Baptist Health primarily engages with TEFCA through three key use cases:1) Treatment; 2) Individual Access Services (IAS); and 3) Electronic Case Reporting to Public Health Agencies. TEFCA enables patients to securely access their health information using third-party apps of their choosing, enhancing patient engagement, care coordination, and individual health management. At Baptist Health, Individual Access Services (IAS) capabilities are active, although no exchanges have been observed to date. Baptist Health adheres to the TEFCA Treatment Exchange Purpose Code guidelines established by TEFCA's RCE.



Through TEFCA, healthcare organizations can electronically and efficiently submit mandatory case reports to public health agencies, supporting timely public health interventions and improved data quality. In February 2025, Baptist Health transitioned from the eHealth Exchange to TEFCA for electronic case reporting, resulting in improved data submission success, reduced maintenance, and lower operational costs. As of June 2025, Baptist Health has successfully exchanged 333,640 electronic reportable case records – 190,184 sent and 143,156 received.



Trading Partner	🟦 Sent	🟪 Received	🟩 Total
Association of Public Health Laboratories	190,184	143,456	**333,640**

CHIME encourages ASTP and CMS to expand the range of incentives available to promote participation in TEFCA, as such incentives are essential to accelerating nationwide adoption. For instance, ASTP could formally recognize TEFCA participation as an affirmative safe harbor under the *Manner Exception* to the Information Blocking regulations, thereby providing greater regulatory certainty to participating actors. Additionally, CMS should consider implementing enhanced reimbursement mechanisms or bonus payments for healthcare providers who engage in TEFCA-based exchange, recognizing the operational costs and public benefits associated with secure, interoperable data sharing at scale.

CHIME has and continues to be a staunch champion when it comes to the need for the use of technology standards aimed at facilitating better patient care. However, for TEFCA to realize its full potential as a nationwide framework for trusted health information exchange, it is imperative that providers across the full continuum of care – including acute, ambulatory, post-acute, behavioral health, individual providers, and safety-net settings – are deliberately and equitably included in its design, implementation, and operational support strategies. Failure to meaningfully incorporate these diverse care settings risks perpetuating existing disparities in interoperability and undermining the effectiveness of TEFCA as a truly inclusive, nationwide exchange infrastructure. Targeted policy levers, financial incentives, and technical assistance will be essential to ensure these provider communities are not left behind as the health system transitions toward a more connected and patient-centered data environment.

CHIME respectfully underscores that future health IT policymaking has the potential to impose disproportionate burdens on certain segments of the provider community – particularly safety-net providers and long-term and post-acute care (LTPAC) providers who were excluded from prior federal incentive programs, such as those established under the Health Information Technology for Economic and Clinical Health (HITECH) Act.[5] These providers often operate with constrained financial and technical resources, and without targeted support or policy flexibility, may face significant challenges in meeting new regulatory requirements, thereby exacerbating existing disparities in health IT adoption and interoperability.

According to the Medicare Payment Advisory Commission (MedPAC), since 2020, more than 40 percent of Medicare fee-for-service (FFS) beneficiaries discharged from an inpatient prospective payment system (IPPS) hospital stay transitioned to a post-acute care (PAC) setting. These settings include skilled nursing facilities, home health agencies, inpatient rehabilitation facilities, and long-term acute care hospitals.[6] This statistic underscores the critical role that PAC providers play in the care continuum – especially for Medicare beneficiaries. To ensure the success of TEFCA as a nationwide health information exchange framework, it is essential that PAC providers are not only included but also meaningfully supported in their participation. Without targeted assistance and tailored implementation strategies, these providers – many of whom face persistent resource constraints and were excluded from previous federal health IT incentive programs – may struggle to join TEFCA, undermining both care coordination and the broader goal of seamless interoperability across the healthcare system.[7]

While the HITECH Act made significant investments in certain areas of our sector, more robust support and funding is needed to improve interoperability across the entire care continuum. Many providers are still – after nearly twenty years – playing catch up with those who received

[5] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

[6] MedPAC March 2025 report to the Congress

[7] MedPAC March 2025 report to the Congress

EHR funding under HITECH. Therefore, we are concerned that a “one size fits all” approach could be especially detrimental to long-term and post-acute care providers that have made significant investments in EHRs, including certified EHRs (CEHRT). Furthermore, future policies could constitute a significant burden on small, rural, and under-resourced providers. **CHIME respectfully requests that CMS and ASTP/ONC ensure that any future policymaking does not inadvertently hinder the success of advancing interoperability across the healthcare continuum – which the agencies acknowledge has been an ongoing challenge.**

As an industry accepted and government-endorsed framework for nationwide health information exchange, TEFCA holds the potential to serve as a unified, scalable on-ramp for a wide array of healthcare providers and other stakeholders seeking to participate in interoperable data sharing. More than 1,000 hospitals and 22,000 clinics are now connected to the network through Epic alone.[8] However, to establish and maintain the trust of all participants – including patients and caregivers – it is imperative that TEFCA be underpinned by robust governance structures. This includes rigorous pre-participation vetting processes and continuous oversight to ensure ongoing compliance with applicable privacy, security, and interoperability standards. Such safeguards are critical to preserving the confidentiality, integrity, and availability of health data exchanged through the network.

To preserve the integrity of TEFCA and foster trust among participants, ASTP/ONC must ensure that timely and decisive action is taken against entities that violate its terms and conditions. In particular, we urge ASTP/ONC to implement safeguards that protect TEFCA participants from bad actors who misrepresent their legal basis or intended purpose for requesting EHI. This issue has become increasingly pronounced under TEFCA, especially in light of the HITECH Act’s mandate requiring that patient information be shared with third parties at the patient’s direction and at minimal cost. Unfortunately, this provision has inadvertently created opportunities for certain entities to exploit the system by falsely claiming to act on behalf of patients in order to gain access to EHI under false pretenses. Such conduct undermines the trust, security, and legal clarity that TEFCA is intended to promote, and must be addressed through both policy and enforcement mechanisms (PR-8, PC-10, PC-11, PC-12, PR-1, PR-2, PR-3, PR-6, PR-7, PR-8, PR-11, TD-6, TD-17).[9]

Our members also believe that in order for TEFCA to truly succeed, and for a seamless and secure flow of health information between patients, providers, and payers – they need to be able to correctly identify – and “match” their patients with their correct patient record. For example, the globally interoperable framework for the Financial Sector demonstrates how the combination of identification, technical standards, governance, and incentives can achieve secure, real-time transactions across thousands of independent institutions (PR-9, PC-10, PR-6, PA-1, TD-3, TD-13, a).

CHIME is a founding member of Patient ID Now, a coalition of more than 50 healthcare organizations representing a wide range of healthcare stakeholders, including patients, physicians, health information professionals, health IT companies, and public health, committed to advancing a nationwide strategy to address patient identification and matching.

Without the ability of clinicians to correctly connect a patient with their medical record, lives have been lost, and medical errors have needlessly occurred. These are situations that could have been avoided had patients been accurately identified and matched with their records. This

[8] Epic connects 1,000+ hospitals to national data exchange - Becker's Hospital Review | Healthcare News & Analysis
[9] How To Stop Abuses In Patient Health Data Exchange | Health Affairs

problem is so dire that one of the nation’s leading patient safety organizations, the ECRI Institute, has named patient misidentification as a recurring top ten threats to patient safety.

Patient misidentification happens in the healthcare ecosystem in two main ways: duplicate records and overlaid records. Duplicate records occur when a patient visits multiple healthcare settings, and each of those settings has a separate medical record for the patient that are not combined into one record, resulting in clinicians working from incomplete patient information. Overlaid records occur when two or more patients’ information is combined into one health record because of similar demographic information, potentially leading to privacy violations if a patient can access another patient’s health information, or leading to safety risks, where one patient may be treated based on another patient’s information. Such errors not only compromise the confidentiality and integrity of sensitive health data but may also result in the delivery of clinical care based on another patient’s medical history, posing serious risks to patient safety (i.e., a patient receiving treatment based on another patient’s diagnosis).

The lack of a national strategy on patient identification and matching creates financial burdens for patients, clinicians, and institutions. The expense of repeated medical care due to duplicate records costs an average of $1,950 per patient inpatient stay, and over $1,700 per emergency department visit. Thirty five percent of all denied claims result from inaccurate patient identification, costing the average hospital $2.5 million and the US healthcare system over $6.7 billion annually.[10] In a survey conducted by the Patient ID Now coalition, 72 percent of respondents agreed that there are delays in billing and reimbursement due to inaccurate patient information, and 70 percent indicated that patients undergo or receive duplicative or unnecessary testing or services due to difficulties in managing patient identities.[11]
The continued absence of a national strategy for patient identification and matching significantly exacerbates patient privacy and safety risks. **These are all challenges that, if addressed through a comprehensive national strategy on patient identification and matching, could bring real benefits to patient safety and privacy, while lowering healthcare costs, and fostering the desire end state of an interoperable healthcare system.**

For over 25 years, innovation and industry progress on patient matching have been stifled due to appropriations language included in Section 510 of the Departments of Labor, Health and Human Services, Education and Related Agencies (Labor-HHS) Appropriations bills that prohibit the HHS from spending federal dollars to promulgate or adopt a unique patient identifier (UPI) standard for individuals. Interpretation of this language has led to the failure to institute a nationwide patient identification strategy, preventing patients from having longitudinal access to their complete and accurate health information as they seek treatment across the care continuum.

The repeal of Section 510 would remove the barriers currently in place preventing CMS and ASTP/ONC from exploring all potential solutions that could improve patient identification and matching, including but not limited to a UPI, and foster the implementation of a nationwide patient identification strategy. The Patient ID Now coalition urges the Administration to support the repeal of Section 510 from the Labor-HHS appropriations bill within the fiscal year (FY) 2026 federal budget.

[10] Available at: https://www.blackbookmarketresearch.com/blog/improving-the-patient-identification-process-and-interoperability-to-decrease-patient-record-error-rates.
[11] Available at: https://patientidnow.org/wp-content/uploads/2022/11/PIDN-Research-Findings-Final.pdf.

We strongly urge CMS and ASTP/ONC to prioritize the establishment and national adoption of a standards-based UPI as a foundational element to modernize and secure the U.S. health technology infrastructure. The absence of such an identifier continues to undermine interoperability, patient safety, care coordination, public health responsiveness, and administrative efficiency.

The United States Core Data for Interoperability (USCDI) has been integral to the standardization of available data elements within certified health IT products, leading to improved interoperability and exchange. However, many elements within the current version of USCDI (e.g., first name, last name, and date of birth) do not have standards that dictate how these data should be entered, causing variation across systems and challenges in data usability and care coordination. Additionally, while the number of data elements included in the Draft USCDI V6 has more than doubled the number of data elements from what was included in USCDI V1, it is not known if the current number of data elements is enough to allow each patient to be uniquely identified, which in turn could avoid circumstances where two patients have the exact same demographic information within their health records leading to an overlaid record (TD-7).

As a result, additional standards and research are needed to improve and evaluate USCDI. These challenges led to the introduction of H.R. 2002, the *Patient Matching and Transparency in Certified Health IT Act of 2025* or the MATCH IT Act of 2025. CHIME, as a founding member of the Patient ID Now coalition has endorsed this critical legislation alongside more than 20 organizations.

The MATCH IT Act has four tenets aimed at improving patient identification and matching through improved standardization of demographic elements within health records. The legislation would: 1) define a patient match rate; 2) establish an industry standard data set to improve patient matching; 3) update health IT certification requirements; and 4) promote interoperability requirements. **CHIME encourages the Administration to consider the MATCH IT Act of 2025 to address patient identification and matching through improving definitions and standardization, including standardization within USCDI**.

Under TEFCA, when a healthcare provider initiates a query to retrieve a patient's health information, QHINs and their participants must adhere to a standardized, policy-governed process for patient identity resolution and record location. This process, known as patient discovery, is executed using demographic-based identity matching protocols. These protocols are governed by the Common Agreement Version 2.0 (CA v2), the Standard Operating Procedures (SOPs), and the QHIN Technical Framework (QTF) v2.0, which collectively define the technical and procedural requirements for secure and accurate health information exchange.[12,13]

While this supports broad interoperability, it remains limited by the absence of a UPI — contributing to inefficiencies, variability in match rates, and potential risks to patient safety. Standardized adoption of robust matching criteria and consideration of new and existing identity frameworks (e.g., digital credentials) could enhance the accuracy and reliability of national health data exchange under TEFCA.

[12] Common Agreement for Nationwide Health Information Interoperability

[13] TEFCA | HealthIT.gov

The RFI asks several questions regarding how health information exchanges (HIEs) are currently helping to advance patient access to health information in the real world (PC-11). CHIME members broadly believe that at this time, CMS and ONC/ASTP play a pivotal role in ensuring the long-term viability and sustainability of existing and future health information networks (HINs), including HIEs. CMS could develop policies and financial incentives that directly address the operational costs of these networks and stimulate robust participation (both data sharing and data consumption).

The RFI also asks additional questions about HIEs (PC-11); many of our members see the value of HIEs and TEFCA, especially in improving data access and care coordination; however, implementation, cost, and trust remain barriers for some providers and states (e.g., some states require participation in their HIE, however, this places cost, responsibility, and liability for their patients' data on our members). Some of our members experience frustration with the current complexity and fragmentation of the ecosystem – with redundancies in participation with Carequality, CommonWell, TEFCA, and their state HIEs – which may have inconsistent standards.

While each state HIE operates under its own structure, policies, and capabilities, they all bring unique strengths – and weaknesses – for our members. These differences reflect the diverse needs of their communities, and many have developed innovative approaches to data sharing, care coordination, and public health reporting that offer valuable lessons for broader interoperability efforts. For example, in New York, HealtheConnections and Hixny provide critical services such as notifications and alerts, which TEFCA and QHINs currently do not handle. However, New York's state law is stricter than HIPAA, and requires "opt-in" (patient consent to access) rather than an "opt-out" consent, so even a clinician providing treatment needs a signed form before checking patient records.[14] This has been noted by our members in New York as a major barrier to participating in national exchanges like CommonWell and TEFCA. Other states use opt-out models, making cross-state data sharing difficult without explicit consent. ASTP/ONC offers resources on "opt-in" vs "opt-out" models, but they haven't been updated since 2019.

The majority of our members express optimism about TEFCA's potential to significantly advance nationwide interoperability, viewing it as a critical step toward seamless, secure, and standardized health data exchange across diverse systems and regions. However, high costs for participation, integration, and maintenance remain a barrier – especially for rural and smaller providers. Our members are concerned that due to a lack of federal incentives or support for implementation – requirements and costs are outpacing their funding cycles. Further, some members have expressed concerns that their EHR vendors charge extra for features that should be standard (i.e., fall under the definition of "Base EHR"[15] under the Certification Program).

The RFI presents several questions regarding the utilization of digital identity credentials, including their advantages and disadvantages, challenges related to adoption, and the potential role of Credential Service Providers (CSPs) in improving access to health information, reducing patient and provider burden, and enhancing identity management and security (PC-13 and 14, PR-9 to 11, PA-3 and 4, and TD-3).

[14] Privacy-Consent-WG-SHIN-NY-Consent-Presentation_final.pdf
[15] 45 CFR § 170.102

It is critical that CMS and ASTP/ONC understand that when our members – which are Covered Entities (CEs) under HIPAA – release a patient's protected health information (PHI) to a third party, three steps must occur: 1) identity verification; 2) patient matching; and 3) patient authorization. Although Credentialing Service Providers (CSPs) can verify patient identity, they cannot effectively perform patient matching or authorization.

CSPs have the potential to enhance access to electronic health information by facilitating secure identity verification. However, within the healthcare context, identity proofing is only one element of a broader, highly nuanced process that must also ensure accurate patient record matching—i.e., verifying that the health information being accessed corresponds to the correct individual (patient matching). Providers are often left to manage the operational consequences when identity verification fails to align with accurate patient record matching – an inherently complex and context-dependent process.

As a general matter, the legal and operational responsibility for ensuring the privacy, security, and appropriate access to EHI rests with the HIPAA CE or its business associate (BA). In other words, the burden of safeguarding PHI, ensuring compliance with HIPAA, and correcting errors resulting from mismatched or misdirected access frequently falls on providers, even when the underlying fault lies with third-party systems. Furthermore, any access by CSPs or their affiliates must be explicitly authorized by the patient or their legally recognized caregiver. This dynamic raises critical questions regarding the role, reliability, and accountability of CSPs – particularly in cases where CSPs are selected by patients and subsequently relied upon to facilitate access to sensitive health records.

CHIME members (as CEs) may be held liable – both under federal and state laws – for the downstream consequences of inaccurate identity proofing, misrouted access, or unauthorized disclosures, despite having little or no control over the CSP's standards, governance, or technical integrity. Without clear lines of accountability and patient-centered safeguards, healthcare providers are at increased risk of exposure to unauthorized disclosures, operational disruptions, legal liability, and harm to patient trust – despite having limited control over the identity-proofing tools being deployed.

As such, if CEs are required to support automated disclosures of PHI via CSPs, liability should be equitably apportioned in a manner that reflects each party's technical authority and operational control. Assigning full liability to CEs – despite limited oversight or governance of the CSP's infrastructure or decision-making – creates an imbalanced and legally unsustainable framework. A more appropriate allocation of responsibility would better align with core principles of risk management, data stewardship, and shared accountability under modern health data exchange models, such as TEFCA.

CMS and ASTP/ONC should carefully evaluate what statutory or regulatory changes may be necessary to ensure that CSPs are appropriately accountable for their role in accessing PHI on behalf of patients. HHS could exercise its regulatory authority to deem CSPs as BAs of the CEs whose records they access, thereby subjecting them to HIPAA's privacy and security requirements. Under either approach, CSPs would bear explicit legal responsibility for accurately verifying patient identities and ensuring that access to PHI is lawful and secure. Such reforms would establish essential protections for patients while safeguarding covered entities from undue liability resulting from third-party identity proofing or access errors outside their control. Further, HHS should explore including this in TEFCA. Ongoing HHS oversight is needed to ensure that HIPAA BAs are adhering to their contractual obligations.

Non-HIPAA entities often handle healthcare data. CHIME has long expressed concerns about the treatment of health data that is held and stored by entities that are not governed by HIPAA. The regulatory oversight framework governing those covered by HIPAA and those who are not has created a separate and parallel but unequal universe which is at the heart of the privacy debate in healthcare. **Most patients-turned-consumers are completely unaware of how an app or a website intends to use their data, and many are under the false assumption that their data will continue to be safeguarded under HIPAA.** CEs must "comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information."[16] A CE may enter into a contract with a BA to assist in performing healthcare functions, with the BA being subject to certain provisions under HIPAA. A BA could be a medical device service provider or a cloud-based software provider, for example. **If an entity does not meet the definition of a CE or a BA, it does not have to comply with HIPAA, creating a significant gap in privacy protections**. A prime example is the vast majority of consumer health apps, which fall outside of HIPAA's scope. According to the IQVIA Institute for Human Data Science's Digital Health Trends 2024 Report, there are approximately 337,000 health-related apps in use today.[17] Examples of these are apps and technologies that track disease, fitness, fertility, mental health, and weight loss, to name a few.

Another issue is when a third-party refuses to sign what is known as a business associate agreement (BAA), despite handling health data. A BAA is a contract between a CE and a BA that outlines each party's responsibilities when it comes to safeguarding PHI. For years, our members have reported to us that they experience challenges with some vendors like medical device manufacturers refusing to sign BAAs, a situation that is only going to grow as providers begin relying more heavily on artificial intelligence (AI) tools. Our members, as HIPAA-covered entities, are required to enter into BAAs with any third-party that handles PHI. Some of these medical devices contain PHI, and/or provide the manufacturers with access to PHI. Providers come to the "bargaining table" as the underdog and often find their requests to have business associates sign BAAs flatly turned down or met with resistance resulting in less than favorable terms for their providers.

CHIME broadly supports technologies that enhance the verification process by increasing security and reducing complexity. Entities mentioned in the RFI that meet specific federal standards for identity and authentication assurance, as defined by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800-63-3[18] (i.e., NIST 800-63-3 IAL2/AAL2) CSPs can significantly contribute to these efforts, providing greater assurance that individuals are accurately identified, and facilitating a simpler identity verification process for patients and caregivers.

Additionally, alternative technologies and mechanisms for identity verification, such as platform-managed passkeys, mobile Driver's Licenses (mDLs) and other government-issued digital credentials that provide a digital counterpart to the paper and plastic IDs that Federal, state and local governments issue today, and biometric requirements should also be considered. To ensure continuous improvement in identity verification technologies, CHIME recommends that CMS and ASTP/ONC avoid mandating one approach to digital identity – and to consider all secure and reliable options rather than limiting consideration to a single technology.

[16] Covered Entities and Business Associates | HHS.gov
[17] Digital Health Trends 2024 - IQVIA
[18] https://doi.org/10.6028/NIST.SP.800-63-3

The development of these technologies and solutions fosters market innovation and expands choices for patients. We recommend that these technologies and others be considered for verification – **provided they meet appropriate standards for security, reliability, and performance** – rather than prescribing a single, static solution. This will ensure ongoing improvement and development in identify verification technologies. To support this approach, it is essential to establish clear, enforceable 'rules of the road' that provide regulatory certainty and guardrails for all stakeholders, ensuring both accountability and continued advancement in these technologies.

Conclusion

In closing, we would like to thank you for providing the opportunity to respond to this RFI and contribute to the important work being done by CMS and ASTP/ONC. As stated in the RFI, the policy framework established by CMS and ASTP/ONC rulemakings are intended to promote the seamless and secure flow of health information between patients, providers, and payers, enabling digital workflows supported by smartphone applications and other modern tools. CHIME and our members deeply appreciate the agencies' continued efforts to foster a secure, interoperable health information ecosystem that empowers patients and providers alike through patient-centered digital tools and technologies.

CHIME members are executives and senior healthcare IT leaders; thus, we are offering to continue to serve as a resource to CMS and ASTP/ONC as they continue towards their goals, which CHIME members broadly support. They remain steadfast in their commitment to using technology to deliver high-quality care and facilitating interoperability and appropriate and secure access to records across the care continuum. However, CHIME urges the agencies to ensure that future rulemaking and/or proposals do not inadvertently create and impose additional regulatory burden onto hospitals and healthcare systems.

We look forward to continuing to be a trusted stakeholder and resource to CMS and ASTP/ONC and continuing to deepen the long-standing relationship we have shared. Working together through the policymaking and RFI response process is crucial to accomplishing our shared goals and make meaningful changes in healthcare.

Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME