May 28, 2024

The Office of the National Coordinator for
Health Information Technology, Office of
the Secretary, United States Department
of Health and Human Services

Submitted electronically via: ONC Health IT Feedback and Inquiry Portal

Subject: 2024-2030 Federal Health IT Strategic Plan

DirectTrust commends the Office of the National Coordinator (ONC) for the coordinated multi-agency collaboration to create a comprehensive 2024-2030 Federal Health IT Strategic Plan. We appreciate the transparency and the opportunity to comment.

Relevant Background

DirectTrust® is a non-profit, vendor-neutral, 501(c)(6) alliance dedicated to instilling trust in the exchange of health data. We began as an initiative of the ONC in 2009 and spun off as a private organization to continue the work in 2012. Since that time, more than 5 billion Direct Secure Messages have been exchanged, and the number continues to grow.

DirectTrust serves multiple roles to promote interoperability and interconnectivity for health and related services. We develop consensus-driven community-focused standards for health care communication. We are an American National Standards Institute (ANSI) standards development organization and accreditation and certification body governed by the Electronic Healthcare Network Accreditation Commission (EHNAC). We steward trust frameworks and supportive services, including our national provider Directory, for secure information exchange like Direct Secure Messaging and trusted, compliant document submission.

We are committed to fostering widespread public confidence in the interoperable exchange of health information while promoting quality service, innovation, cooperation, and open competition in healthcare.

We're a prime example of a free-standing, successful, self-sustaining, and *growing* organization without additional financial support of the ONC.

Comments

DirectTrust supports and applauds the ONC for the creation of this Strategic Plan. Concerted effort has been made by many organizations, including ours, to advance the goals laid out in this Plan. **Overall, we strongly believe that information flows at the speed of trust. Additional support to risk reduction efforts through independent assessment of adherence to security best practices, as well as consideration and emphasis of scalability, and identity assurance and**

patient matching, will help move the ONC and nation towards the goals laid out in this Plan. We highlight several areas important to us, our membership of more than 120 organizations, and our more than 100 accredited or certified organizations.

We offer the following specific comments for consideration:

- Regarding Goal 1 – Promote Health and Wellness
  - *Objective A: Individuals are empowered to manage their health*, we recommend:
    - Add an endorsement for consumer protection standards and third-party (independent) accreditations that support consumer application privacy and security (Examples of such standards and programs include the CARIN Code of Conduct[1] for Consumer-Facing Applications and DirectTrust Health App[2] Accreditations)
    - Include planned coordination and collaboration with other federal agencies for oversight, including Office of Civil Rights (OCR) and Federal Trade Commission (FTC), especially related to the proliferation of health apps and protecting health data outside of HIPAA
    - Build the cryptographic infrastructure required to support secure, scalable use of FHIR in the ecosystem. Point to point connections with FHIR will not scale; the ONC should invest in scalable trust that's secure by design
    - Adding the following to Strategy 3, *"Individuals can readily access, exchange, be and use their EHI across various technology platforms"*, as well as be entitled to identity-assurance and record accuracy
- Regarding Goal 2 - Enhance the Delivery and Experience of Care
  - *Objective A: Providers deliver safe, equitable, high-quality, and improved care // Strategy: Promote interoperable and secure health information sharing through nationally adopted standards:*
    - We recommend adding language that supports and gives examples of nationally adopted standards, including the Direct Standard®, which is the foundation of Direct Secure Messaging and a primary means of supporting push interoperability, including referrals, public health, and event notifications.
  - *Objective A: Providers deliver safe, equitable, high-quality, and improved care // Strategy: Support efforts to address patient identity and record linking solutions.*
    - We noted that this is the only reference to identity or patient/record matching in the entire document. Though critical in this context, we would like to see the ONC emphasize this critical item throughout and/or as an overarching statement of the Plan. For example, this is also essential to public health, payers, research, and patient facing applications.

[1] https://accreditation.directtrust.org/programs/carin-code-of-conduct

[2] https://accreditation.directtrust.org/programs/health-app

        - We are unclear as to what "support efforts" means. That phrase suggests that there is an effort occurring elsewhere to participate in but we are not aware of a designated entity owning this effort and would like to see ONC assuming or designating ownership of this strategy. As an example, DirectTrust convenes the Privacy-Enhancing Health Record Locator Systems (PEHRLS) Consensus Body that is exploring creating a standard to address these and similar issues.
    - *Objective B: Patients experience expanded access to quality care and reduced or eliminated health disparities // Strategy: Expand health IT use beyond hospitals and physician offices so that health care providers in behavioral health, long-term and post-acute care, and home health settings use technology to access, exchange, and use EHI*
        - We support this strategy but question whether naming these settings of care specifically is too limiting. We recommend either indicating they are examples of care settings, or adding additional areas such as correctional (justice-involved) health, schools, SUD treatment & residential centers, dental, employer/occupational/work comp, optometry, surgery centers, dialysis, child welfare, ambulance/EMS, etc. Direct Secure Messaging is growing across all care settings, and frequently becomes a means to support interoperability in under-resourced organizations and settings because of its ease of deployment and access.
- Regarding Goal 4 – Connect the Health System with Health Data:
    - *Objective D: Individuals' EHI is protected, private, and secure // Strategy: Provide guidance and resources to help health care organizations integrate high-impact cybersecurity practices, such as the Health Care Cybersecurity Performance Goals and the NIST Cybersecurity Framework, in the design and use of health IT while also prioritizing the improvement of the confidentiality, integrity, and availability of connected systems containing health data*
        - We recommend specifically providing cybersecurity practices guidance regarding vetting and oversight of vendors and partners. This should include recognition of third-party (independent) accreditation, such as DirectTrust (EHNAC) and HITRUST. By accepting these (as referenced in P.L. 116-321 as "recognized security practices …"), it reduces provider burden to individually understand and review vendor policies and practices granularly.
    - *Objective E: Communities are supported by modern and integrated U.S. public health data systems and infrastructure*. We recommend:
        - In Strategy 3 including language specific for encouraging standardized privacy, security, identity and person-matching for public health data systems. Such as, *"Develop, align, test, and implement data, **identity, and security standards** to increase interoperability across the public health data systems"*
        - We recommend including a definition or reference link to outline what systems are "public health data systems". For instance, does this include

Prescription Drug Monitoring Programs, All Payer Claims Databases, National Emergency Medical Services Information System (NEMSIS), etc.?

Overall, we appreciate the opportunity to comment on the ONC's Draft Strategic Plan. We hope the ONC considers additional emphasis on the areas we outlined, but in particular advancing trusted exchange by encouraging independent evaluation of security practices, developing a scalable model for FHIR, further championing identity assurance and verification, and supporting *all* data exchange standards across settings. We welcome any opportunity to support its implementation.

Respectfully submitted,

Scott Stuewe
President and CEO, DirectTrust