



May 28, 2024

Micky Tripathi, Ph.D., M.P.P.
National Coordinator for Health Information Technology
Department of Health and Human Services
Mary E. Switzer Federal Office Building
330 C St. SW
Washington, D.C. 20201

[Submitted electronically via healthit.gov/feedback]

Dear Coordinator Tripathi:

The Joint Commission appreciates the opportunity to comment on the Office of the National Coordinator for Health IT (ONC) draft *2024-2030 Federal Health IT Strategic Plan*.

As the nation's oldest and largest health care accreditation organization, The Joint Commission helps health care organizations (HCOs) to continuously improve the quality of care. By setting rigorous standards and sharing leading practices, The Joint Commission aims to share its vision that all people always experience safe, high quality health care. Founded in 1951, The Joint Commission is an independent, not-for-profit organization that evaluates the performance of HCOs across the globe and our programs accredit or certify more than 22,000 HCOs and programs in the United States. While accreditation and certification are voluntary, more than a dozen Joint Commission programs are recognized by federal and state regulatory bodies, including the Centers for Medicare and Medicaid Services (CMS).

The Joint Commission is pleased to provide comments on the ONC's strategic goals. In general, The Joint Commission encourages ONC to include strategies that recognize and support trusted private sector activity and entities, such as The Joint Commission, to further the development and implementation of best practices and standards for HCOs, particularly in areas where gaps in federal policy exist and technology advancements are happening rapidly. The Joint Commission would further recommend that strategies include ONC and other federal agencies partnering with such trusted organizations and encouraging HCOs to participate in voluntary private sector efforts.

The Joint Commission provides specific comments regarding certain strategies in the draft Strategic Plan as follows:

I. Privacy

- *Protect the privacy and security of EHI in circumstances beyond those addressed by all applicable federal and local regulations and statutes*
- *Support efforts to address patient identity and record linking solutions*

- *Foster data governance that reinforces privacy protections for large datasets*
- *Protect de-identified health information from re-identification*

The Joint Commission's Comments:

The Joint Commission strongly supports ONC's identification of privacy and security as a primary principle of federal health IT strategies. The confidentiality of patient information is a fundamental expectation within health care and should be considered when developing any policy regarding electronic health information (EHI) in order to maintain trust. Specifically, The Joint Commission supports ONC's plan to protect the privacy and security of EHI in circumstances beyond those addressed by federal protections. Many stakeholders, including federal agencies such as ONC, have identified the risk to privacy presented by the amount of health information that is created, collected, shared, and used outside of the scope of the Health Insurance Portability and Accountability Act (HIPAA) and other federal protections. The Joint Commission has also seen increased concern about the privacy of large data sets and the risks to de-identified data that is not subject to HIPAA, given that there is no law prohibiting re-identification.

In January of this year, The Joint Commission launched a Responsible Use of Health Data (RUHD) voluntary certification for hospitals and health systems. The certification is intended to provide direction to hospitals on how to navigate the appropriate sensitivities needed to safely use de-identified data collected by hospitals and health systems for secondary uses, such as for the creation of disease registries or operations and clinical quality improvement.¹ The Joint Commission developed this certification based on principles from the Health Evolution Forum's "Trust Framework for Accelerating Responsible Use of De-Identified Data in Algorithm and Product Development."² This certification provides standards and an objective verification that hospitals and health systems have policies and procedures in place regarding the de-identification process, data controls, limitations on use, algorithm validation, patient transparency, and oversight structure.

The Joint Commission believes that the new RUHD certification provides hospitals and health systems with important guidance on how to protect the privacy of data that currently falls outside of HIPAA, one of the strategies in the draft Strategic Plan. Since there are no federal standards for using de-identified data or validating best use practices, the RUHD certification helps to fill the gap in regulations by providing a framework for hospitals and health systems to implement policies on the appropriate de-identification process, including having qualified personnel to validate the proper de-identification of datasets and impose limitations on recipients that may not be subject to HIPAA.

The RUHD certification takes steps to mitigate risks. Through data use agreements, certified hospitals must institute controls to prevent against the unauthorized re-identification of data. The

¹ J. Perlin & J. Merlino, *Protecting Patient Privacy*, 39 HEALTHCARE EXECUTIVE (2024), <https://healthcareexecutive.org/archives/march-april-2024/protecting-patient-privacy>.

² Health Evolution Forum, *Trust Framework: Accelerating Responsible Use of De-Identified Data in Algorithm Development* (Apr. 1, 2022), <https://www.healthevolution.com/innovation-and-discovery/trust-framework-deidentified-data/>.

Joint Commission believes the RUHD certification is a significant marker that hospitals and health systems are implementing practices to protect patient privacy in an area where little, if any, protection exists currently. As such, The Joint Commission encourages ONC, OCR, and other federal agencies to advance policies to protect secondary use of health data, including de-identified health data and to build on or support private sector efforts, such as the RUHD certification. To further these efforts, The Joint Commission welcomes input from federal agencies on ways to build on RUHD certification to address other gaps in privacy protections.

II. Data Security

- *Implement appropriate mechanisms for privacy and security to protect EHI*
- *Mitigate individual health information security and privacy risks*
- *Ensure data collection involves consent for and understanding of secure sharing and use, as appropriate*

The Joint Commission's Comments:

The Joint Commission strongly supports ONC's strategic goals concerning data security. As recent headlines have demonstrated, threats to data security have become both more frequent and more severe. The continuing digitization and interconnection within health care will only serve to escalate these risks. The Joint Commission's CMS recognized accreditation programs include emergency management standards that direct hospitals and other health care provider types to consider cybersecurity during hazards vulnerability assessments to strengthen the ability of health care providers to respond to cyberattacks. This was done to frame the expectation of cyberthreats as an essential part of emergency preparedness.

Additionally, The Joint Commission believes the RUHD certification provides hospitals with data security measures in a space that falls outside HIPAA authority. To complement the data privacy controls mentioned above, RUHD certified hospitals are required to maintain a security infrastructure to protect against unauthorized access, use, and disclosure of data.

The Joint Commission also recognizes that many hospitals and health systems may export and potentially share de-identified data with third parties, who may use that data for purposes such as quality and operations improvement, discovery, or algorithm and artificial intelligence development. Data recipients are also a lucrative target for cyberattack, and de-identification should not be the only layer of security for patient data. Both the hospital and the data recipient have data security responsibilities. This is built into the RUHD certification, which requires a certified hospital or health system to obtain evidence that the data recipient holds a security certification or has undergone an external audit against security best practices and has policies to monitor ongoing compliance with security standards, before the hospital discloses any data.

III. Artificial Intelligence/Machine Learning

- *Promote education, outreach, and transparency about the use of artificial intelligence (AI) technologies*
- *Promote increased transparency into the development and use of AI algorithms in health care settings*
- *Increase transparency and understanding of health data that goes into algorithm-based decision support tools*

- *Promote the safe and responsible use of AI tools*

The Joint Commission's Comments:

The Joint Commission supports ONC's proposed strategies to facilitate the safe, transparent use of artificial intelligence and machine learning (AI/ML) tools. Increased transparency and understanding of algorithm-based tools will support ONC's objective to allow the health care workforce (and their patients) to use health IT with confidence. ONC has already taken significant steps to integrate transparency as part of the development process for algorithm-based decision support tools. The Joint Commission believes that support and guidance from ONC and other federal health agencies will be critical in setting expectations for how AI/ML tools are deployed within health care settings. Importantly, The Joint Commission believes that we need the right balance – guardrails to protect appropriate use while also ensuring any limitations placed still allow the use of these tools to help improve care.

As part of the RUHD certification, certified hospitals and health systems are required to have an initial and recurring process to validate and test internally developed algorithms, including a process to document appropriate use cases and algorithm accuracy thresholds. Hospitals and health systems must also validate that any algorithm (whether internally developed or from a third party) is tested for the specific population it serves and evaluate algorithms for nondiscrimination to mitigate risks of algorithmic bias. Furthermore, certified hospitals and health systems must also ensure transparency for patients by implementing a process that educates patients on the potential uses of de-identified data and that establishes a public process to address patient concerns and/or questions regarding de-identified data, which would include uses and disclosures for AI/ML training and use.

The Joint Commission supports the aligned strategic goals of ONC in safe handling of patient data and looks forward to examining ways Joint Commission's RUHD certification process may help to advance these federal priorities.

IV. Measuring Progress

- *ONC intends to prioritize the following areas for measuring progress:*
 - *U.S. Core Data for Interoperability (USCDI)*
 - *USCDI+*
 - *Certified Health IT*
 - *TEFCA*
 - *Information Sharing Consistent with the Information Blocking Regulations*
 - *HHS Health IT Alignment*

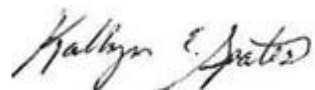
The Joint Commission's Comments

The Joint Commission supports ONC's work to encourage the adoption and use of data standards to promote the interoperability of health information. ONC intends to prioritize the use of standardized data sets such as USCDI and USCDI+ and exchange capabilities supported by ONC's Health IT Certification Program and TEFCA serve as areas for measuring progress. The Joint Commission believes that monitoring adoption and use in these areas will serve as a useful benchmark for the maturity of the U.S. health data ecosystem. Progress towards widespread use of these standards would provide significant benefit to health care systems and organizations

working to improve quality in health care by instituting clear, consistent, and comparable sources of measurement and serve to improve patient access to their own health data.

The Joint Commission is pleased to answer any questions you may have regarding our comments. If you have any questions, please do not hesitate to contact me at kspates@jointcommission.org or Patrick Ross, Associate Director, Federal Relations at pross@jointcommission.org. Both can be reached at 202-783-6655.

Sincerely,

A handwritten signature in cursive script that reads "Kathryn E. Spates".

Kathryn E. Spates
Executive Vice President, Public Policy & Government Relations