surescripts®

May 28, 2024

Office of the National Coordinator for Health Information Technology (ONC)
U.S. Department of Health and Human Services
330 C St SW
Floor 7
Washington, DC 20201

Submitted via healthit.gov

Dear Dr. Tripathi,

Thank you for the opportunity to provide comments on the *Draft 2024-2030 Federal Health IT Strategic Plan*. We appreciate the amount of effort, collaboration, and coordination across several agencies to produce this future-looking, comprehensive plan document.

The Surescripts Network Alliance® brings together healthcare professionals and organizations across the United States to collaborate, tackle shared challenges, and advance care. Our purpose is to serve the nation through simpler, trusted health intelligence sharing. Our Network Alliance® includes nearly all electronic health records vendors, pharmacy benefit managers, pharmacies and clinicians in the U.S., plus health plans, long-term and post-acute care organizations, patient access vendors, and specialty pharmacy organizations.

Our annual network statistics[1] from 2023 include:

- 2.14 million healthcare professionals and provider organizations connected
- 2.5 billion e-prescriptions processed, including 21 million for specialty prescriptions
- 2.97 billion medication histories delivered
- 28.4 million electronic case reports sent to public health agencies
- $36.74 average savings per prescription with Real-Time Prescription Benefit

In a post-Dobbs decision[2] era, we continue to see new legislation and regulations enacted that place new patient consent and health information exchange restrictions on sensitive health information, including reproductive health data. We applaud your colleagues at the Office of Civil Rights (OCR) for the release of the recent *HIPAA Privacy Rule To Support Reproductive Health Care Privacy*[3], and we are hopeful this rule will make a difference in the protection of reproductive health data privacy and confidentiality. Regardless of what future state legislation may develop regarding reproductive health data and other types of sensitive health data fields (i.e., substance abuse, gender affirming care, behavioral health), we raise concerns regarding existing

[1] Surescripts, "2023 National Progress Report," March 2024, https://surescripts.com/report
[2] 19-1392 Dobbs v. Jackson Women's Health Organization (06/24/2022) (supremecourt.gov)
[3] Federal Register :: HIPAA Privacy Rule To Support Reproductive Health Care Privacy

state regulations and the exchange of sensitive health data. In these emerging state regulations, there are restrictions of varying degree regarding:

- the definition of sensitive health data fields,
- patient consent requirements,
- electronic exchange of sensitive health data.

Our primary concern relates to the fact there is not a standardized, nationwide, electronic patient consent framework that could enable compliance with varying state requirements. In addition, different definitions of sensitive health data sets across states create headwinds for health IT developers, particularly related to the additional efforts and overall costs of product compliance.

We highlight recent state requirements in Maryland and California. These comments are not meant as political opinion on the logic behind the regulations. Rather, we point out the differences in the definitions of sensitive data sets, and the requirements for patient consent and exchange.

Maryland (COMAR 10.25.18).[4] and Health Information Exchange Guidance.[5]

- **Regarding patient consent**: “*A patient cannot provide general consent to an HIE for the release of legally protected health information. The regulations require legally protected health information only be released by an HIE to a specific treating provider at the written request of a patient, for services for which the patient can provide consent under State law, or a parent or guardian of a patient, for services which the parent or guardian can provide consent under State law. A patient could provide consent to specific multiple providers at one time, but a patient could not provide general consent to unknown future providers. Consent is not required for the release of information to a payer or its business associates for the adjudication of claims*”.

- **Sensitive health data**: generally prohibits the disclosure of mifepristone data or the diagnosis, procedure, medication, or related codes for abortion care and other “sensitive health services”.

California (AB352).[6]

- Requires “…*limiting user access privileges and segregating medical information related to gender affirming care, abortion and abortion-related services, and contraception*”.

[4] Pages - COMAR Search (maryland.gov)
[5] HIE_Guidance_012624.pdf (maryland.gov)
[6] Bill Text - AB-352 Health information. (ca.gov)

- Excludes "...*the exchange of health information related to abortion and abortion-related services from automatically being shared on the California Health and Human Services Data Exchange Framework*".
- Segregates "…*medical information related to gender affirming care, abortion and abortion-related services, and contraception from the rest of the patient's record*".
- Requires "…*the ability to automatically disable access to segregated medical information related to gender affirming care, abortion and abortion-related services, and contraception by individuals and entities in another state*".

Patient Consent Framework Groups

- **HL7 FAST Consent Management Workgroup**[7]
- ***Objective***: *Consent management is the central component in a consent ecosystem and at the core of a scalable consent architecture. There is currently some support for some basic consent management use cases in the existing specifications, including FHIR Core and the IHE.ITI Privacy Consent on FHIR (PCF), mostly at the basic operations for creating, reading, and updating consent resources. Consent management, however, needs more implementation guidance and standardized specification that is still missing. This includes the interactions between patients and the consent management system in the process of soliciting, navigating, and executing consents, which is sometimes referred to as consent ceremony, as well as a high-level API (e.g., defining custom FHIR operations) to cover use cases for consent management.*

- **Shift: The Independent Healthcare Task Force Interoperability**[8]
- *Shift is the independent health care task force for equitable interoperability with a mission to advance safe, equitable, and patient-empowered sharing of health information. To this end, the task force has gathered expert stakeholders across the industry with the purpose of maturing granular data segmentation standards and implementation guidance in order to sponsor patient-driven sharing of health information with informed consent and advance interoperability in a more equitable manner*.

We encourage the ONC team to continue involvement in these two industry groups for the purpose of future development of an industrywide, standards-based, patient consent management framework. A standardized consent framework could also enhance overall operations and state regulatory compliance of current and future QHINs participating in TEFCA.

[7] Consent Management - FAST - Confluence (hl7.org)

[8] Shift: The Independent Healthcare Task Force for Interoperability (drummondgroup.com)

Cybersecurity

We share the opinion of the Pharmacy Health Information Technology Collaborative regarding the need for a greater emphasis on cybersecurity initiatives across the government. We appreciate the current discussions between HHS's Administration of Strategic Preparedness and Response (ASPR), the White House, Cybersecurity and Infrastructure Security Agency (CISA), and other agencies and stakeholders regarding the critical need to strengthen and defend the healthcare system's IT infrastructure from attackers. The recent Change Healthcare and Ascension cyberattacks and their respective repercussions are a glaring reminder of the vulnerability of this critical infrastructure from a variety of overseas-based hackers.

We suggest adding a fifth goal to the final plan with a greater emphasis on cybersecurity. As currently drafted, the topic of cybersecurity does not come across as sufficiently strong and does not adequately address the topic; particularly with regard to how cybercriminals are using AI-powered cyberattacks[9]. As per a May 8, 2024 press release from the Federal Bureau of Investigation (FBI), "The FBI San Francisco division is warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams. Cybercriminals are leveraging publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns, exploiting the trust of individuals and organizations alike". Every healthcare entity, including government agencies, is vulnerable.

Thank you for the opportunity to comment on the final strategic plan and for all the efforts that went into the draft report creation. We look forward to the final document and for additional information, I can be contacted at Deanne.Primozic@surescripts.com.

Best regards,

Deanne Primozic

Deanne Primozic
Vice President, Policy and Federal Affairs

[9] FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence — FBI