ECRI | The Most Trusted Voice in Healthcare

2024-2030 Federal Health IT Strategic Plan Draft

Feedback and Commentary from ECRI

May 28, 2024

Micky Tripathi, Ph.D., M.P.P.
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

Re: 2024-2030 Federal Health IT Strategic Plan Draft for Public Comment

Dear Dr. Tripathi,

ECRI is grateful for the opportunity to share insights for the draft 2024-2030 Federal Health IT Strategic Plan. As an Agency for Healthcare Research and Quality (AHRQ) listed Patient Safety Organization (PSO) and Evidence-based Practice Center (EPC), we applaud the U.S. Department of Health and Human Services (HHS), the Office of the National Coordinator for Health IT (ONC), and the more than 25 federal organizations who collaborated to develop the draft.

The draft strategic plan is a critical step forward in modernizing the nation's public health infrastructure. It offers an ambitious vision of the healthcare landscape of the future. The health IT infrastructure is the cornerstone of our nation's healthcare system, where we face significant threats and opportunities to improve its resiliency, effectiveness, interoperability, adaptability, and standardization.

ECRI's Health IT Expertise

ECRI is a non-profit global patient safety organization and the world's only independent evaluator of medical devices. ECRI has been evaluating the safety and effectiveness of healthcare technology for over 50 years. We harness the nation's largest datasets, a team of over 500 experts, and more than five decades of industry expertise, to deliver transformative insights into patient safety and savings opportunities that enable better care. Our research and clinical data have played a significant role in leading the global effort to dramatically reduce preventable harm and make healthcare more transparent and accessible. As one of the foremost independent healthcare patient safety experts, we leverage our expertise to respond to the request for public comment on the 2024-2023 Federal Health IT Strategic Plan.

Strengths and Alignment in the Plan

The Federal Health IT Strategic Plan is a necessary advancement in healthcare data strategy that could improve health equity and accessibility, decrease healthcare costs, improve quality, and reduce incidents of preventable harm. These are core components of ECRI's mission and vision, and we fully support this effort.

We are aligned and supportive of the goals in the strategy, including: Promote Health and Wellness; Enhance the Delivery and Experience of Care; Accelerate Research and Innovation; Connect the Health System with the Data. We wholeheartedly agree with the need for accelerated use of healthcare data to enhance all these areas and ensure care is delivered equitably to all patients.

We applaud that the plan is designed to enhance the basic infrastructure that connects the data upon which our healthcare system operates – so we can then realize the benefits of applying innovative, emerging technologies that show great promise. Before we can safely and responsibly scale up innovative applications of health IT and data nationally, we must first connect our data and health IT systems in a strong infrastructure that prioritizes access, standardization, functional interoperability, security and privacy safeguards, and most importantly patient safety.

We are especially supportive of prioritizing health equity in the strategic plan. The well-documented and pervasive health inequities that exist in America today are abhorrent and unacceptable. Due to your race, ethnicity, gender, degree of disability, socioeconomic status, veteran status, religion, and sexual orientation, you could receive considerably worse healthcare and suffer higher rates of preventable harm. The plan's goal to "advance the use of data to represent social needs and the conditions in which people live, learn, work, and play," taking into account the societal factors and explicit and implicit bias that influence care, is of the utmost importance. Effective use of health IT and data is critical in bringing quality, affordable, safe healthcare within reach for all Americans.

Cybersecurity Threats

The draft plan states that cybersecurity guidance and resources will be provided to execute the plan's strategies. ECRI advises that these resources be meaningful, tangible, and accessible to all healthcare delivery organizations (HDOs).

Healthcare is considered critical infrastructure, yet there is great disparity in available funding for cybersecurity amongst healthcare organizations. Currently, security compliance is compelled by potential fines and penalties levied on organizations that are typically operating on narrow margins including not for profit organizations. Government funding and investment is required to see significant improvement in the health IT security landscape.

ECRI has long recognized cybersecurity threats as detrimental to patient care in our annual Top Ten Technology Health Hazards reports – including ransomware attacks, third-party web

analytics software, cloud-based clinical systems, connected home health environments, and the risk of hackers exploiting remote access systems.

Most recently, we identified the critical threat of ransomware targeting the healthcare sector as one of the top health tech concerns for 2024. Ransomware will continue to pose a serious threat and the current approach is not working to mitigate risk and protect patients.

Healthcare is a primary target for such attacks because 1) the systems that are held hostage can be critical to urgent care delivery, which means hospitals are more likely to pay to neutralize a threat; and 2) many hospitals operate on thin margins and generally do not adequately fund their cybersecurity programs. When it comes to cybersecurity, healthcare is an easy target.

Cyberattacks can be extremely disruptive to patient care, to the point of risking serious adverse patient outcomes and even fatalities. After such an attack (which can also be financially devastating to a healthcare institution already under financial pressure), hospitals are then subject to regulatory fines and lawsuits. ECRI's hazard report on ransomware provides guidance for security controls to put in place to mitigate this risk; and calls for government investment to build up healthcare security.

Privacy and Data Protection

ECRI recommends applying considerable thought to the privacy and security implications of the plan. Throughout the plan, patient data is referred to as EHI (electronic health information) instead of PHI (protected health information) in acknowledgement that as the data migrates out to the consumer and out of the hands of covered entities, HIPAA no longer protects it. While the FTC has occasionally stepped in on some cases, there is a lack of federal protection of individuals' personal data and information.

The plan posits the benefits of ensuring patients have easy access to their health data, which could certainly enhance the patient's role in the delivery of their care. However, as we improve the interoperability of and access to that data, we must prevent systems from leaking sensitive information to third parties with authorization.

While the accessibility of one's own health data is appealing, data providers and manufacturers are likely to be large tech corporations, data brokers, or credit bureaus. We must consider the implications of these entities potentially serving as clearinghouses of critical data. There must be strong federal privacy legislation in place before this sensitive data is made available to entities that have proven repeatedly that they often use it without the consumers' knowledge and against their best interests.

With the emergence of newer technologies, such as AGI (artificial general intelligence, the next evolution of AI systems), it becomes even more critical that we connect systems in a seamless, safe manner. Additional privacy legislation would put guardrails in place to protect patients and the sensitive health IT data foundational to the plan.

Artificial Intelligence

We are supportive of the plan's goal to **"**promote the safe and responsible use of AI tools." AI shows great promise to revolutionize healthcare – but we must proceed with both optimism and caution. ECRI has been increasingly vocal about this, as AI applications in healthcare have proliferated and opened new doors for exciting breakthrough interventions – and new safety risks and equity concerns.

AI has been present in healthcare for decades, but now we are seeing AI touch nearly every clinical specialty (with radiology being the dominant category). About 90% of AI-enabled devices are cleared via the 510(k) pathway, which is not sufficient to determine if these applications are safe and effective. AI tools are often marketed as decision-support tools, but as clinicians are inundated with more variables in patient care and workflows, these tools can quickly become decision-making tools, and pose a threat to patient safety.

There are many factors to consider, including – the ethical implications of AI tools that may restrict patients' access to care to increase profitability; the health equity risks of AI trained on biased or incomplete data; and alarm fatigue for clinicians using AI tools to monitor patients. Certain AI models have been reported to demonstrate bias regarding demographics such as race, socioeconomic status, or geographic location. Biased data will result in biased models.

Regulatory bodies are developing processes to assess the safety of AI applications, but we are not moving quickly enough to prevent AI from causing harm and introducing biases in the delivery of care. ECRI has released hazard reports and action strategies for our healthcare partners to safely leverage the power of this promising technology without introducing new risks.

Supply Chain and Pricing Data

The draft plan does not mention the impact of the global medical supply chain on health IT. ECRI believes the global medical supply chain is one of the greatest opportunities for cost reduction in healthcare. In addition to actionable individual patient and population health data, the strategic plan should address initiatives to improve supply chain data and reporting for utilization, spend management, and efficiency. We encourage improved price transparency, strategic sourcing, as well as improved practices in supply chain management to ultimately reduce the costs for patient treatment.

The strategic plan is centered on a vision in which "a health system uses information to engage individuals, lower costs, deliver high-quality care, and improve individual and population health." Ensuring cost-effectiveness is mission-critical in improving health IT systems and health outcomes for Americans overall. However, the impact of this is difficult to measure. Promoting health and wellness should include focus on internal and external data sets. There is no

reference in the draft plan to bring in external data such as safety, quality, and cost to enable informed decision making by both the providers and the patients.

The draft plan includes the goal to "educate healthcare consumers on the availability of quality and price information." The strategy should call for the education of providers and consumers on the availability of quality and price information to ensure the most appropriate form of care is provided at the right price.

Establishing an infrastructure to provide improved, actionable population health data is important and will identify and drive care to key areas that are currently underserved. However, improving the minimum level of care and directly reducing costs to patients is one of the most impactful drivers of equity. The strategy does not include direct actionable drivers, such as access to medication assistance programs. Sharing key data may improve the costs and effectiveness of these programs, as well as simplify access for patients.

HIT Technology/EHR Documentation

While electronic health record (EHR) systems have made access to patient data easier for multiple clinicians using the same system, electronic sharing of a patient's information between different EHR systems remains difficult or impossible. The current means used by EHRs to facilitate communication of encounter-specific information with other EHRs—which could involve electronic transfer of documents summarizing the patient's care —has been problematic. In particular, the EHR system may be unable to verify that the documentation was sent, much less sent to the correct outpatient physician. This is especially important as patient care is shifting away from inpatient acute care settings to different outpatient settings.

Regarding a subgoal of the health information technology (HIT) guidance draft – "the healthcare workforce uses health IT with confidence," and "leverages health IT expertise from different health care settings" – ECRI recommends the plan consider the different ways an HIT technology and EHR can be used. That includes how they are commonly used today, often in stark contrast to how they were originally designed. The ideal and imagined workflow is often different than the reality of clinical workflows in how providers engage with health IT tools and documentation.

For example, outpatient providers should receive discharge summaries from acute care hospitals, but in reality, that doesn't always happen. Hence, outpatient providers need to rely on a different document, such as patient facing discharge summaries, to make care coordination decisions. ECRI has led several studies regarding this type of data-sharing and interoperability issue, including assessing usability of EHR-generated discharge documents. Our recommendations for our healthcare partners are based on usability issues identified by our human factors and clinical experts, and should be used to inform EHR design, policies, and procedures for generating documents that effectively support care coordination.

Patient Safety and Total Systems Safety Approach

The significance of the patient safety implications of the plan cannot be overstated. Healthcare providers cannot prevent adverse events in the delivery of care, provide equitable care, or treat patients in need without a strong health IT infrastructure.

It's a notable strength of the plan that it identifies principles that are aligned with a Total Systems Safety approach including person-centered inclusive design, increase health equity across all populations, and improved safety and quality. Total Systems Safety focuses on creating greater efficiency and resilience in clinical and safety operations. It incorporates principles of human factors, systems design engineering, health equity and advanced safety solutions to redesign how individual components of a system can be more transparent and aligned, facilitating healthcare teams to deliver safer and more effective care.

One of the plan principles includes "safety," but there is an opportunity in the plan to expound on safety's connection to health IT. We recommend making more explicit connections between patient safety and health IT in areas such as medication management, infectious disease, and sepsis, for example.

In "enhancing the delivery and experience of care," there is an absence of any reference to corresponding measures that will ensure the delivery of safer patient care. We recommend including proactive mechanisms to ensure the most appropriate technologies and pharmaceuticals are being utilized in patient care with the corresponding evidence to support those interventions. These additional elements will help to improve the delivery, experience and quality assurance of care provided.

Prerequisites for Plan Execution

To execute the plan, it will require a national coordinated effort that brings multidisciplinary expertise and credible insights to bear on our greatest health IT challenges. A coordinated public-private partnership is required to regulate, purchase, develop, and use health IT to deliver care, improve patient health, align standards, and share best practices to enable a national learning system for improvement. ECRI identified several strategies in the plan that will require government funding and investment to shore up resources in areas of the healthcare landscape that are already under immense financial strain. We have also identified the need for rigorous national privacy laws related to sensitive health data, of which the plan strives to provide patients easier access to. Several standout elements in the plan align closely with our vision for the future: standardizing critical healthcare practices; integrating with third party systems; and bringing data accessible to end-users in a safe and secure manner.

Conclusion

Today, one in every four patients will suffer an adverse event during care, a quarter of which are avoidable. We can and must do better. Together, focusing on impactful improvements, we can build a safer, equitable healthcare system for all.

These comments were generated by an interdisciplinary team of experts from ECRI led by:

Marcus Schabacker, CEO and President, ECRI

Dheerendra Kommala, Chief Medical Officer, ECRI

Darryl Goss, Chief Technology Officer, ECRI

Tim Browne, Vice President of Supply Chain Solutions, ECRI

Scott Lucas, Vice President of Device Safety, ECRI

Shannon Davila, Executive Director of Total Systems Safety, ECRI