Healthcare recommendations

Recommendation HC1: Support and promote industry and SDO efforts to address interoperability of medical and healthcare devices and systems.

Justification: Interoperability challenges are a major barrier to maximizing the value of IoT in healthcare. One of the primary challenges in achieving interoperability in healthcare IoT and IoMT is the inherent fragmentation of the ecosystem. Healthcare facilities often deploy a variety of devices and systems from different manufacturers, each operating on proprietary protocols and standards. In addition, consumer wearable health trackers have limited interoperability, depending on the device, standards and integration capabilities. This lack of uniformity creates silos of data, with disparate IoT devices and systems having limited to no ability to communicate with each other. Besides hindering the free flow of information between devices and systems, this lack of interoperability limits the ability of the systems with multiple devices to monitor patient conditions, inform and support diagnoses, and provide effective and accurate individualized treatment. The lack of interoperability among these devices poses a significant challenge to the seamless integration of IoT in healthcare.

The lack of interoperability is manifested in many forms, including:

- Diverse communication protocols
- Disparate data formats and structures. Diverse coding systems, data models, and terminology standards are prevalent across healthcare organizations, making it challenging to ensure consistency in data interpretation and exchange.
- Legacy systems that may not be inherently compatible with IoT and IoMT technologies.
- Inability to integrate and interoperate with electronic health record systems

Recommendation HC2: Facilitate cybersecurity in IoT in smart medical devices and equipment, including wearables, in-home devices, community IoMT systems, and in-clinic systems

- **Expand cybersecurity trust mark program to include IoT devices and modules used in a variety of healthcare systems and applications**
- **Facilitate workforce development programs to increase pool of IoT cybersecurity trained resources for healthcare industry on both the solution provider side and care provider (buyer) side**
- **Consider development of programs, resources and incentives to help healthcare providers migrate away from those vulnerable legacy equipment and devices that cannot be patched, or upgradeable, or were not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act)**

- **Develop a plan to audit, inspect and update healthcare and medical IoT devices, and the networks they operate in used in federally owned or funded health facilities (e.g. VA medical facilities, military medical facilities, etc.). Replace those legacy devices and equipment that cannot be patched or upgradeable or not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act). Verify devices and systems, and practices meet IoT cybersecurity guidance and best practices.**

Justification:
Healthcare and medical IoT devices and systems are susceptible to cyberattacks. These cyberattacks not only expose sensitive and personal health data and information, but they could lead to disruption to the operation of the devices and systems, leading to potential injury and loss of life. Areas of healthcare and medical device IoT cybersecurity concerns include:

- Vast attack surface due to the interconnected nature of IoT and IoMT devices. Each connected device represents a potential entry point for malicious actors seeking to exploit vulnerabilities.
- Protecting data in transit and at rest is of concern because the data generated by IoT and IoMT devices in healthcare include sensitive patient information. Encryption is critical to preventing unauthorized access.
- Unauthorized access to healthcare data can have severe consequences, ranging from identity theft to compromised patient care. Robust authentication and access control mechanisms is essential to restrict data access to authorized personnel only.
- Patching millions of IoT and IoMT devices is logistically and operationally challenging. These devices often have a longer life cycle than traditional IT devices, and some lack the capability for regular software updates. Not all device and system owners apply patches and firmware updates.
- Legacy systems and devices that cannot be patched or updated with the latest software to address known vulnerabilities
- Compliance with regulatory frameworks (e.g. HIPAA) can be challenging due to the dynamic and evolving nature of IoT and IoMT technologies.
- Securing endpoints (devices) and gateways against unauthorized access and breaches is critical as they act as crucial points in the data transmission process for IoT and IoMT devices.

Recommendation HC3: Facilitate U.S. government adoption and use of medical and healthcare IoT technologies, including:

- **By federal healthcare providers in federally owned or funded health facilities (e.g. VA medical facilities, military medical facilities, Indian Health Service, federal prisons medical centers, etc.)**
- **Consider programs by healthcare payers (HMOs, PPOs, etc.) that support federal employees to adopt these technologies in the treatment of their patients**
- **Consider programs by federal healthcare programs (Medicare, Medicaid, the Children's Health Insurance Program, Affordable Care Act) that support qualifying patients to adopt these technologies in the treatment of their patients**
- **Developing guidance that supports and integrates the use of IoT devices in existing medical services, procedures**

and supplies codes in Medicare (HCPCS, ICD-10-CM)

Justification

The federal government has a major influence in facilitating the adoption of IoT in healthcare. Directly, and indirectly, the federal government programs provide and support the health of millions of Americans. For example, a number of major healthcare insurance companies (payers) support its 2.951 million federal civilian employees (October 2023).1 Approximately 1.3 million active duty military in 2022 receive government sponsored healthcare insurance (Tricare).2 Nearly 45%, or 143.3 million persons are enrolled in, or heavily subsidized by, the big federal health programs: Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and the Affordable Care Act health insurance exchange plans.3 Because of the number of people it supports, the government can use its significant influence and scale to use innovation to help improve delivery of services, quality of services, and health outcomes in a way no private insurer can.

Recommendation HC4: Facilitate the resolution of privacy concerns in healthcare and medical IoT

- **Support research in privacy enhancing technologies specific to the needs of the healthcare industry**
- **Consider the incorporation of PETs on IoT technologies used in the treatment of patients in federal government owned medical facilities, and federal supported healthcare programs (Medicare, etc.)**
- **Incorporate considerations for healthcare in the development of a national privacy framework and regulations**

Justification

Privacy matters are a cause of concern and can potentially hinder the adoption and use of IoT technologies in healthcare. Concerns about the information collected and how it is used, as well as the accuracy of the data collected and the ability of the technology to create the correct outcomes. These concerns are wide-ranging and include:

- Securing data from unauthorized access. Personal health data can come from a variety of sources, including clinical medical devices, as well as consumer wearable devices.
- Ownership and consent to use of patient data. The interconnected nature of healthcare IoT devices raises questions about data ownership and the extent to which patients have control over their health information. Obtaining informed consent from patients for the collection, use, and sharing of their data (outside of patient treatment) is a complex process, especially when considering the numerous devices involved in IoMT and the number of people who could have access to the data (e.g. insurance companies, researchers, etc.).

---

[1] "All Employees, Federal (CES9091000001)", Federal Reserve Economic Data (FRED), St. Lous Fed, Link.

[2] "What is the state of the military, and how are US veterans faring?" USA Facts, Link.

[3] "The truth about government controlled healthcare," R. Moffitt, The Heritage Foundation, Link

- Ethical use of data. The extensive data collected by IoT and IoMT devices provide valuable insights into patient health and behavior. However, the ethical use of this data is a concern. Ensuring that data is used responsibly, without enabling discrimination or exploitation, requires robust ethical frameworks and regulations.

Recommendation HC5: Facilitate and support the use and adoption of healthcare IoT in rural communities.

- **Facilitate grants to drive healthcare IoT adoption among heathcare providers in those communities that have received broadband grants to build on new connectivity infrastructure**
- **Coordination with federal agencies to drive physician and patient awareness of IoT in healthcare for treatment**

Justification

Rural communities lack many of the same resources, services and amenities that residents in urban areas benefit from. Many rural areas are considered medical deserts with limited number of healthcare providers and facilities. In addition, residents in rural areas tend to be sicker than their urban counterparts, as well as older and more likely to suffer from chronic conditions. In addition, many have limited transit options to go see a doctor on a regular basis.

As a result, healthcare access inequities exist. Telehealth, home healthcare monitoring and consumer health tracking are IoT enabled services that can alleviate some of these inequities by providing access to healthcare and improving their health outcomes.

Implementation considerations

- Code IoT enabled services in Medicare to support senior population in rural areas
- Facilitate support from private payers (insurance companies)
- Focus on chronic disease management

Barriers

- Cost of connectivity services (rural residents may have affordability issues)
- Limited connectivity (wireless and fixed broadband service)

Recommendation HC6- Facilitate adoption of IoT among small physician practices (< 50 physicians)

- **Consider programs by healthcare payers (HMOs, PPOs, etc.) that support federal employees to adopt these technologies in the treatment of their non-federal employee patients**
- **Consider programs by federal healthcare programs (Medicare, Medicaid, the Children's Health Insurance Program,**

Affordable Care Act) that support qualifying patients to adopt these technologies in the treatment of their patients
- **Coordination with federal agencies to drive physician and patient awareness of IoT in healthcare for treatment**

Justification - Small physician practices make up the majority of physician practices in the United States. However, these practices tend to be less likely to use electronic information than those physician offices with 50 people or more.[4]

Recommendation HC7: Facilitate policies and programs that support the key education and digital skills development for the current and future healthcare workforce, including

- **Data analytics and management**
- **Artificial intelligence**
- **IoT technologies**
- **Networking and systems integration**
- **Cybersecurity**
- **Installation, maintenance and servicing of IoT systems**

IoTAB Themes: Healthcare, Workforce

Justification

The healthcare industry is undergoing a major digital and technology transformation towards revolutionizing healthcare, including the potential for data led individualized care and treatment. The integration of IoT and digital technologies in healthcare will provide more effective treatment, reduce the impact of a shortage of healthcare labor, and reduce healthcare expenditures. However, a lack of the relevant digital skills and workforce is hindering this transformation of healthcare across all levels, from device development and use, integration into hospital and healthcare systems, to analysis of patient data and development of AI algorithms for treatment and diagnosis.

Implementation Considerations

- Integrate the needs for the development of digital skills and workforce in the National Cyber Workforce and Education Strategy

[4] "Interoperability among office-based physicians in 2019", ONC Data Brief No. 59, Office of the National Coordinator for Health Information Technology, July 2022. Link

Recommendation HC8: Facilitate the adoption of AI in IoT in healthcare through

- **Support research in the development of trustworthy AI algorithms and tools, including AI explainability**
- **Facilitate the development of IoT data usage and privacy policies that support the development of AI algorithms [linkage with Debbie recommendation]**
- **Support workforce development efforts to increase the pool of workers trained in data analytics and AI**

IoTAB Themes: Healthcare, Workforce

Justification

While AI can help automate the analysis of massive amounts of IoMT data, and other data collected from health records, its ability to create explainable, beneficial and personalized outcomes specific to the patient that are clinically appropriate, reliable and accurate is a major challenge.

AI algorithms review and analyze data, and make recommendations and in cases requiring autonomous operations, take action. Diagnosing people and identifying treatments for people is complex. Diseases such as cancer are complex, and there is still much to be learned. Furthermore, each person has a different reaction to treatments and what works for one person may not work for another. AI generated recommendations may yield treatment recommendations that lead to adverse outcomes, including injury and death. There are a variety of reasons AI may lead to negative or unintended outcomes, including data that may be outdated, contains bias, or incomplete. The source of the data may be unknown for privacy reasons. While the AI algorithms have been trained on this data, the reasons it led to a specific recommendation may not be explainable and transparent. This leads to a loss of confidence in the AI's ability to analyze the data accurately and reliably.

Implementation barriers

- Data privacy regulations and policies limit what data can be collected, and how it is used
- Lack of workforce trained to develop, test and refine data and AI algorithms