

Internet of Things Advisory Board Healthcare Subgroup

Draft Recommendations

May 2023

Subgroup Members:

Ann Mehra

Mike Bergman

Maria Rerecich

Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Teams

Justification

- IoMTs monitor, detect, inform, and deliver therapies to patients, therefore, they deserve just as much attention and call out as cloud services, for example.
- IoMTs are ignored by healthcare IT organizations, as the responsibility to make decisions and/or purchase the devices is owned by the biomedical engineering department.
- IoMTs may not undergo strict infrastructure, privacy, and security guidelines as to large capital equipment investments such as MRI scanners.

Make **IoMT** equivalent in **priority** for all healthcare stakeholders as is IT infrastructure, cybersecurity posture, or applications.

Recommend the notion of a **Chief IOT Officer** and a **Federal program office** to manage IOTs.

Barriers

Implementation

Federal Considerations

Agencies

Promote Data Exchange Interoperability for IoMT

Justification

- Data exchange standards for IoMT would result in data interoperability, which would result in efficiencies and provide safety benefits that would encourage the adoption of IoT.

Promote and, if necessary, develop a protocol for **data exchange standards** for IoMT for interoperability, and promote the adoption of these standards.

Barriers

- Resistance from healthcare organizations that have already invested in an IoT solution
- Resistance from industry manufacturers because of concerns about their proprietary solutions and captive user base.

Implementation

- Coordinate with relevant stakeholders, including product manufacturers and healthcare organizations, to ensure widespread adoption.

Federal Considerations

- Procurement: Prioritize solutions which adhere to the IoMT data exchange standard in government contracts
- Tax Incentives: Provide tax benefits to companies that implement the IoMT data exchange standard
- Promotion: Promote the IoMT data exchange standard and educate healthcare organizations about the benefits.

Agencies

- NIST
- CISA
- HHS

HIPAA-like Protection for Medical Data in Mobile Apps and IoT Devices

Justification

- Many consumer-grade IoT devices and mobile apps collect users' sensitive medical data.
- Consumers tend to believe that this data is protected similarly to medical data in a healthcare facility, but it is not.

Enact **HIPAA-like protection** for users' medical data in **mobile applications** and **IoT devices**. Consider medical data as a category for defined data protections.

Barriers

- Possible resistance from industry manufacturers to restricting the sharing of user data.

Implementation

- Extend HIPAA protections to these classes of devices and mobile apps, or enact a similar type of protection

Federal Considerations

- Regulation: Enact HIPAA-like regulations to protect user PHI in consumer IoT devices and mobile apps

Agencies

- HHS