What is MDIRA?
The Medical Device Interoperability Reference Architecture (MDIRA) is a framework that provides guidance and requirements for developing interoperable, safe, and secure medical device systems that will deliver advanced and autonomous medical care. MDIRA can be used by organizations that procure and develop healthcare systems and technologies, including traditional medical devices and software as a medical device (SaMD). It incorporates and builds on internationally recognized standards (see FAQ regarding standards). A reference implementation (or engineering prototype) of a MDIRA-compliant system is currently under development.

What is the objective of MDIRA?
MDIRA’s objective is to improve care efficiency, outcomes, and patient safety by advancing the development of interoperable, secure medical devices, including, but not limited to, autonomous medical care systems.

Why is MDIRA needed?
Health care technologies and systems generally do not work well together, nor were they developed to do so. Instead of medical technologies seamlessly working together, there is a sea of individual, functionally separate components, custom vendor interfaces, and a lack of plug-and-play capability. Although many medical technology standards [e.g., Institute of Electrical and Electronics Engineers (IEEE)-11073 Service-oriented Device Connectivity (SDC)] exist, there is widespread lack of adoption, or, if adopted, there are varying forms. The lack of standards adherence not only produces high upgrade costs and
‘vendor lock’, but also poses data and cyber security risks. Interoperability often only exists within technologies manufactured by a single company. Although MDIRA is needed within current medical systems and operations, it will be even more essential for any future medical system that requires autonomous and closed-loop operations.

**How can MDIRA be effective where past efforts have not?**

Even prior to COVID-19, health care provider organizations and stakeholders, including the U.S. Defense Health Agency, have wanted better interoperability among health care equipment to enable more informed or autonomous care of patients, particularly in remote locations. To date, neither health care organizations nor key stakeholders have been able to produce a universally adopted, suitable-for-all-use-cases standard approach to information exchange among medical devices. For instance, the IEEE-11073 standards have been in development since the early 2000’s and ASTM-F2761\(^1\) was released in 2009. Rather, manufacturers tend to produce proprietary software or hardware solutions that are not widely interoperable with software or hardware from other manufacturers. In fact, in some cases, the interoperability does not even exist across one manufacturer’s own products lines. The U.S. Defense Health Agency is intent on advancing interoperability by working with the Johns Hopkins Applied Physics Laboratory (APL) to create a reference architecture and develop a reference implementation to show innovators and medical device manufacturers how interoperability can be achieved. APL is working with researchers, academicians, and industry to produce consensus and provide solutions to the challenges that have prevented interoperability.

**What are the functional elements of a MDIRA-compliant system?**

A functional element is any software or hardware component created for a specific operational purpose or task to meet a requirement in the MDIRA specification or to deliver care to or monitor care of a patient.

1. **Supervisor:** Determines and manages system health and status (i.e., whether the system is operating correctly), manages the registry of authenticated components in the system, executes system fault protocols, and manages and authorizes requests of components to control other components that are externally controllable.

2. **Data logger:** Stores detailed and comprehensive system and patient data during a care encounter for later download to an information system for analysis. It is expected to conform to the Association for the Advancement of Medical Instrumentation (AAMI) 2700-2-1 Data Logger Standard, once published.

3. **Use manager (optional):** Facilitates the setup of user accounts and privileges, controls access to the system according to those privileges, and maintains a user audit log.

4. **Medical Electrical Equipment and Medical Electrical Systems:** These technologies are involved in monitoring the patient’s medical state and administering medical interventions.

5. **Software applications:** Include SaMDs and medical applications that may not fall within the SaMD definition (i.e., non-SaMD medical apps) as well as other (non-medical) applications.

6. **Non-medical equipment:** Equipment not intended for a specific medical purpose, although it may support medical operations (e.g., sensors that monitor the environmental conditions like temperature, humidity, air pressure).

Figure 1 provides an example of a MDIRA-compliant system that includes several medical devices as well as software applications.

---

\(^1\) ASTM-F2761, Medical Devices and Medical Systems - Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE)
What are some functional elements external to a MDIRA-compliant system?

An external element is any software or hardware component contributing to the care of a patient that operates outside of the specification requirements of a MDIRA-compliant system (Figure 2). Examples include:

1. Electronic medical record/Health information systems
2. Evacuation vehicles
3. Communication support systems
How is MDIRA being developed?

MDIRA is being developed through a multi-agency, multi-partner collaborative research project to develop a sustainable framework supported by autonomous/closed-loop MDIRA implementations and demonstrations for military health care, which are dual use for the civilian health care system.

The initial MDIRA specification was built through analysis of existing standards (see FAQ: What standards are considered in MDIRA?), operational scenarios, and clinical workflows to identify operational objectives and requirements to support those objectives.

Based on the initial MDIRA specification, candidate medical scenarios relevant to the battlefield environment have been identified for development of reference implementations to provide demonstrations of MDIRA-compliant systems. The insights gained from the reference implementations will be used to evolve and mature MDIRA through the incorporation of use cases and the related technologies within them.

Who can use MDIRA?

- Organizations that procure and use medical devices, including civilian and military medical treatment organizations and disaster relief organizations. These organizations can use MDIRA to identify requirements to support procurement decisions.
- Developers of medical devices, including patient care related software applications, autonomous healthcare and trauma systems, and medical robots. Developers can apply the MDIRA requirements and guidance to ensure interoperability with other systems.

Figure 2. A graphical representation showing some components external to a MDIRA-compliant system
What does MDIRA provide?
MDIRA provides requirements and implementation guidance to help ensure the development and deployment of interoperable, safe, and secure medical device systems. The MDIRA specification document:

- Defines an environment into which combinations of medical devices, some under closed-loop control, can be quickly integrated to meet healthcare needs
- Provides a common terminology and taxonomy for physical and functional elements
- Identifies the pertinent interoperability standards as well as requirements (e.g., for medical devices) not yet addressed in the standards (stimulates enhancements to standards)
- Supports development of MDIRA-compliant medical device systems, including core components
- Enables an open-systems business model where devices from multiple manufacturers/software developers can be integrated to work together without translation between the components
- Specifies requirements that must be met to have a MDIRA-compliant system

What is NOT provided by MDIRA?
MDIRA does not define the requirements for a specific operational system. MDIRA is intended to be an input to the systems engineering process for development of a system. It does not replace the need to derive system requirements based on operational needs but rather complements that process by providing the requirements to ensure interoperability and security. There is no MDIRA system, but a system with a given operational capability may be MDIRA-compliant if it satisfies MDIRA requirements.

MDIRA does not provide requirements for clinical care protocols. The MDIRA requirements are focused on the technology enablers that ensure secure and interoperable systems. Requirements for specific clinical care protocols are outside the scope of MDIRA and will vary depending on the operational need.

What is the scope for MDIRA?
The U.S. Defense Health Agency in collaboration with the U.S. Army Medical Research and Development Command asked APL to initially focus on care in austere combat situations, but MDIRA is useful for medical device interoperability enabling advanced care in a multitude of care settings, including hospital, home and ambulatory environments, disaster relief, and military combat casualty care. Given that future combat operations may require prolonged patient field care for multiple days without medical evacuation, or future pandemics may present high patient care requirements with limited medical personnel, MDIRA currently focuses on autonomous medical care technologies.

The MDIRA specification document establishes requirements and implementation guidance for the functional and information architectures, as well as non-functional characteristics (e.g., data integrity, security), of MDIRA-compliant medical care systems and their components. Key MDIRA topics include:

- System health and status monitoring
- Technical enablers for system reliability and patient safety
- Data integrity, confidentiality, and validity
- Discovery and authentication of components that connect to the system as well as operators that use the system
- Trusted authorization for a component to change the settings of another component (i.e., trusted control)
- Time synchronization of data streams
• Data logging
• Use of standard information models, controlled vocabularies, and semantics.

To provide industry as much design flexibility as possible, an objective for MDIRA was to not be overly prescriptive. For example, requirements for component authentication and system health and status monitoring do not prescribe the details of how those functions will be implemented. Furthermore, regarding safe use of the system for advanced patient care, the emphasis is on technical enablers rather than the clinical applications themselves.

The scope of MDIRA does not include requirements that would derive from a system’s unique operational requirements or from industry-specific standards (e.g., Military Specifications) that dictate design particulars and qualification requirements for particular applications, customers, and deployment settings. For example, MDIRA does not consider:

• Specifics on user interface implementations (i.e., data entry and displays)
• Physical characteristics such as form factor and mechanical and electrical interfaces
• Operating and non-operating environments
• External power supply and battery requirements
• Particulars of how a MDIRA-compliant system is deployed to a specific operational domain (e.g., hospital, austere military setting)
• Methods of supply and preservation (e.g., refrigeration) of medical consumables (e.g., fluids, blood, medication) used in the patient’s medical care, although a MDIRA-compliant system may have an application that tracks the usage of these medical consumables, thus supporting the re-supply process.

Practical deployment of MDIRA-compliant systems will require rigorous assessment of these types of operational considerations.

What are the primary research deliverables for MDIRA?
1. A reference architecture that guides development of interoperable and autonomous medical device systems and that addresses technical and clinical interoperability challenges, but leaves policy issues to the U. S. Food and Drug Administration for future guidance
2. An engineering prototype system that provides a proof-of-concept for a MDIRA-compliant system, including demonstration of autonomous, closed-loop applications that are common for multiple medical devices or algorithm-controlled healthcare

What are example clinical conditions where a MDIRA-compliant system can be considered?
• Pulmonary insufficiency
• Hemorrhagic shock and coagulopathy
• Burn
• Cranio-cerebral trauma
• Septic shock
• Multi-system organ failure
• Acute renal failure
What standards are considered in MDIRA?
IEEE-11073 Health informatics – Point-of-care medical device communication
  IEEE-11073-10101:2004(E): Nomenclature
  IEEE-11073-10101a:2015(E): Nomenclature Amendment 1: Additional Definitions
  IEEE-11073-10201:2004(E): Domain information model
  IEEE-11073-10207:2017: Domain Information and Service Model for Service-Oriented Point-of-Care Medical Device Communication
  IEEE-11073-20101:2004(E): Application profiles – Base standard

ANSI/AAMI 2700-1:2019 (formerly ASTM F2761 09(2013)), Medical Devices and Medical Systems – Essential safety and performance requirements for equipment comprising the patient-centric integrated clinical environment (ICE) – Part 1: General requirements and conceptual model

IEC 60601-1-8:2006, Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems +Amendment 1:2012

AAMI TIR 71:2017 – Guidance for logging of alarm system data

ANSI/AAMI/IEC 62304:2006/ AMD 1:2015, Medical device software – Software life cycle processes – Amendment 1

ISO 14155:2011, Clinical investigation of medical devices for human subjects -- Good clinical practice

IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices


Who is working on MDIRA?
In collaboration with the U.S. Defense Health Agency and U.S. Army Medical Research and Development Command, APL is leading MDIRA with multiple partners, including the Medical Device Plug-n-Play (MD PnP) Interoperability & Cybersecurity Program at the Massachusetts General Hospital, DocBox, Trusted Solutions Foundry, Philips, Dräger, ARCOS, ICU Medical, Capsule Technologies, Zoll Medical Corporation, Integrating the Healthcare Enterprise (IHE), and IEEE. As part of the National Emergency Tele-Critical Care Network, the Army’s Telemedicine and Technology Research Center (TATRC) is asking its performers to use specifications in MDIRA to establish secure data transfer within the network.

Who is funding MDIRA?
The U.S. Defense Health Agency is funding MDIRA through the U.S. Army Medical Research and Development Command.

Are there additional MDIRA resources?
Project development video: https://youtu.be/EdWZgn8EoQI
Project Website (specification document and participation information): https://secwww.jhuapl.edu/mdira/