HITRD RFI Responses, March 15, 2019

ACTION ON INTEROPERABILITY OF MEDICAL DEVICES, DATA, AND PLATFORMS TO ENHANCE PATIENT CARE

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

Action on Interoperability of Medical Devices, Data, and Platforms to Enhance Patient Care

Organization: NeuroWave Systems Inc.

Description of organization: NeuroWave Systems is an ISO-13485 medical device company, dedicated to developing innovative, state-of-the-art signal processing and control technologies for the next generation of brain monitors and anesthesia drug delivery systems, for improved and safer patient outcome and safety.

One of our current effort involves the development of a closed-loop anesthesia and sedation drug delivery platform that combines our brain monitoring technology with an infusion pump mechanism and a robust controller. The goal of this innovative platform is to automatically drive and maintain patients at a depth of anesthesia or sedation prescribed by the care provider. This program is currently supported by the Office of Naval Research, and was supported by the US Army under various SBIR programs.

(1) What is your vision for addressing interoperability issues between medical devices, data, and platforms? How would this plan to create interoperable systems address your key use cases and pain points?

When it comes to interoperability, we believe we should consider separately an (1) open-data-access scenario, and (2) an open-control scenario.

Open-data-access: we believe that manufacturers of medical devices should provide at the very least:

- an access port on the medical device for data upload, and

- a communication protocol (publicly available) to allow third-party to read data from the device, and

- a test protocol (also publicly available) to allow third party developing drivers to verify and document that the implementation of the driver is successful and follows the medical device manufacturer's intent.

Within this type of data sharing concept, the medical device manufacturer should not be liable for how the data is being used by the third-party application.

Our experience with open-data-access: when we started our business (20 years ago), communication protocols were difficult to get from manufacturers. We would typically need to enter into some sort of agreement with the medical device manufacturer to keep the protocol confidential and share the

results/conclusion of any studies done with their equipment. This was definitely an impediment to research and development. As a result, when we commercialized our first brain monitor back in 2010, we included the communication protocol in the user manual to help researchers collect real-time data with our device. Now that we have an installed base of monitors, we get requests from third party integrators to get a copy of our communication protocol. They are surprised that the protocol is disclosed in the user manual, and that we do not require any specific use agreement for them to use our data. So even today, device manufacturers do not make it easy to fully leverage their device technologies and integrate their information into a large database. We very much believe that regulations and standards should make open-data-access mandatory.

Open-control: another type of interoperability is the ability of the device to respond to commands from a third-party application (2-way communication). A typical example is infusion pumps. As of today, there is no single infusion pump available commercially for human use that can be controlled remotely via a third-party software. One fundamental reason is related to risk control. Risk controls involve the identification of sequence of events leading to hazardous situations resulting in harm to the patient (or the operator). Risk mitigations are designed to reduce the likelihood of such sequence of events to occur, or the severity of harm. When doing such analysis, the presence of a qualified operator next to the medical device (and therefore next to the patient) is assumed. Infusion pump manufacturer do not include situations in their risk analysis where a third-party device takes control, and where the operator of the third-party device may be located remotely, away from the infusion pump and the patient. There is therefore an important risk that therapy may be inadequate if the operator changes the infusion rate, without being at the bed side:

- is the change in therapy really needed based on the patient's state? …
- is the infusion pump connected to the right drug/concentration?…
- is it connected to the right patient?
- etc.).

When considering automation, other concerns arise, e.g., is there someone nearby ready to intervene in case the therapy is inadequate? Another question is how can the infusion pump manufacturer enforce basic safety protocols if the pump is being operated by a third-party software/device that is out of the manufacturer's control?

Another important design aspect (also controlled through risk analysis) is Usability. Considering again the infusion pump example, pump manufacturers develop their technology to fit certain usability scenarios. If a third-party device substitutes the original user interface with a new one, risk mitigations addressing risks related to

use errors may no longer be valid. New usability testing would need to be performed, this time by the third-party integrator.

Our recommendation would be that medical device manufacturers should be *encouraged* to consider and 'open-control' interoperability scenario by identifying risk items in their risk management file that a third-party would need to address in order to take control of the device. It should be made very clear whether the open-control allows for an operator to be remotely away from the medical device (e.g., in a different room), and what is the minimum information signals that the third-party interface must display to the operator. Another consideration is related to the alarm system, and whether the device's built-in alarm system is sufficient or needs to be integrated to the third-party alarm system (e.g.: if the third-party platform is in a different room, visual alarms triggered on the user interface of the medical device should be echoed back on the screen of the third-party platform.)

Our experience with open-control: back in 2011, we have been looking for infusion pumps to interface with our brain monitor in order to develop a closed-loop drug delivery system. None were found on the market, and this situation has not changed since then. This has prompted us to develop our own infusion technology, which has significantly slowed down our product development and delayed the market introduction of our closed-loop anesthesia platform.

We recently decided to open our infusion pump system to third party developers by offering an OEM infusion module. This is essentially to support DoD vendors developing critical care medical devices for our Armed Forces that would not be able to develop their own infusion technology. We are currently working on integrating as many safety features as possible within the OEM device to minimize the amount of risk control specifications that a third-party application would be required to implement. We are also working on a safety assurance case where risk mitigations implemented through the third-party application can be easily identified. Work on the OEM module is a first step towards an open-control infusion pump device.

(2) Who are the relevant parties and their contributions to your interoperability solution?

Regulatory agencies are key. Implementing the open-data-access solution will require policy makers (e.g., FDA) and decision makers at the level of the IEC to issue guidance documents and standards mandating medical device manufacturers to share their communication protocols.

As far as ‘open-control’ is concerned, this would be more of a case-by-case consideration. Governmental organization like the DoD would be very helpful in guiding this effort. Open-control would allow for telemedicine and automation provided that (1) the end-stage integrator implement all the risk controls identified by the original device manufacturer, and (2) is ultimately responsible for the operation and safety of the platform.

(3) What are the challenges and impediments to making interoperability happen? How might these issues be addressed and by whom?

The medical device product cycle is long. Adding mandated interoperability features like open-data-access may take a long time for medical device manufacturers to issue in their new generation of products. A communication protocol standard can go a long way to facilitate this implementation and the adoption of this concept (e.g., the HL7 standard for electronic data exchange can be a good starting point, but can be overly complicated for simple devices and simple peer-to-peer interfaces).

(4) Is the federal vision for a medical device, data, and platform interoperability end state outlined in this RFI viable? Please explain why you have reached the conclusion that you have.

Yes, it is viable and (very) desirable. Closed-loop operation can be a factor of added safety and improved outcome as it would lead to more consistent health care delivery and would help project expertise at the bed side. Governmental organizations like the DoD have an essential role to play to nurture interoperable technologies as they can insist on having interoperability as part of the requirements for future devices. This would help medical device manufacturers develop such technologies, which would invariably spill over in the civilian market.