

# Medical Device Data Systems and FDA Regulation

## Should Medical Device Data Systems Require FDA Clearance?

Peter Kelley

### KEYWORDS

Medical Device Data Systems, MDDS, FDA, vendors, patient care, nursing.

### ABSTRACT

It is widely understood why medical devices need to be regulated by the FDA and other governing bodies. However medical software does not typically require the same level of regulation. Currently the FDA is investigating whether one type of medical software, Medical Device Data Systems (MDDS), should require FDA clearance because of the potential risk they impose when interconnected with medical devices. Hospitals are looking to implement MDDS because the technology allows nursing staff to spend more time on direct patient care and reduces charting errors. This article will explore the FDA's proposal and will review the possible risks and provide a rationale for why MDDS should be regulated by the FDA and why MDDS vendors should have the right level of quality and risk management procedures in place to ensure that they are developing and bringing to market the safest products possible.

The FDA has proposed to reclassify Medical Device Data Systems (MDDS) from a default class III to class I, with an exemption from Premarket Notification. In a sense this is not a reclassification so much as it is a definition and a classification. Until now, MDDS has not been a term that was widely used in the medical device or healthcare information industries. The FDA has proposed a definition that can be summarized as “a device that provides one or more of the following uses: electronic transfer, exchange, storage, retrieval, display or conversion of medical device data without altering the function or parameters of any connected device.”

### MEDICAL DEVICE CLASSIFICATION

The FDA uses a classification system to broadly segregate medical devices into different categories, according to the risk posed to patients and users. Each class has control requirements that manufacturers must implement to provide reasonable assurance of the safety and effectiveness of the device; the more risk associated with a device, the more controls required to mitigate it.

Classification is applied to defined types of products, such as cardiac monitors, ventilators, carbon dioxide gas analyzers and so

on. If a device does not have a defined type, like MDDS', then the default classification is class III.

The three categories of medical devices and their associated controls are:

**Class I.** Class I devices are subject to the least regulatory control. They present minimal potential for harm to the user and are often simpler in design than class II or class III devices. Class I devices are subject to General Controls as are class II and class III devices.

**Class II.** Class II devices are those for which General Controls alone are insufficient to assure safety and effectiveness and existing methods are available to provide such assurances. In addition to complying with General Controls, class II devices are also subject to Special Controls.

**Class III.** Class III devices fall in the most stringent regulatory category for devices. Class III devices are those for which insufficient information exists to assure safety and effectiveness solely through General or Special Controls. Class III devices are usually those that support or sustain human life, or, are of substantial importance in preventing impairment of human health. In addition to complying with General Controls and Special Controls, class III devices also require Premarket Approval (PMA).

General Controls include the following:

- Establishment registration.
- Medical device listing.
- Compliance with the Quality System Regulation—21 CFR 820.
- Labeling.
- Premarket notification—510(k), unless exempt.

Special Controls may include the following:

- Special labeling.
- Mandatory performance standards.
- Post-market surveillance.

Premarket Notification, or 510(k), is the means by which the FDA clears medical devices for market. Manufacturers are required to submit product specifications, performance data and final product labeling in order to receive clearance. The FDA reviews all this data to establish that a device is substantially equivalent to already marketed devices.

The 510(k) submission represents a minimal burden to the manufacturer as all of the data required for submission is produced through the Quality Management System. However, depending on the type of 510(k) in use, the process can be time consuming, taking up to 90 days per submission. The 510(k) essentially provides assurances that the manufacturer's Quality Management System is compliant and effective prior to clearing a product for shipment.

The manufacturer must also document the "intended use" for the medical device within that 510(k) submission. The intended use for a medical device is determined by the manufacturer. It is the prism through which all aspects of the device must be viewed and it is the guiding principle for understanding the capabilities of a device. Manufacturers may only make claims about their products that are

in alignment with their intended use. Physicians are free to use the devices in any way they deem necessary. If such use is inconsistent with the intended use, this is called "off label use". In this case, the Practice of Medicine Doctrine grants medical doctors wide latitude in adapting therapies for their patients-including off-label uses.

If the device manufacturer has a device that doesn't have a substantial equivalent already on the market, then the manufacturer has to apply for Premarket Approval. Premarket Approval is a lengthy and expensive process for establishing the safety and effectiveness of a medical device through scientific review, usually involving regulated clinical trials.

## **QUALITY SYSTEM REGULATION AND RISK MANAGEMENT**

Regardless of the class of a device, the most time consuming and expensive aspect of General Controls is complying with the Quality System Regulation (QSR). The FDA requires all medical

**The FDA uses a classification system to broadly segregate medical devices into different categories, according to the risk posed to patients and users. Each class has control requirements that manufacturers must implement to provide reasonable assurance of the safety and effectiveness of the device.**

device manufacturers to comply with the Quality System Regulation. The QSR is embodied in the Code of Federal Regulations, 21 CFR 820. It requires manufacturers to implement documented processes in the areas of: Management Controls, Design Controls, Production and Process Controls, and Corrective and Preventive Actions. Compliance with the QSR is confirmed through routine inspections by the FDA. Failures can lead to any number of remedies including untitled letters, warning letters, seizure, injunction, civil penalties and criminal prosecution.

The QSR is the foundation upon which the FDA expects manufacturers to build a reliable Quality Management System (QMS). Proper implementation of the QMS is critical to ensuring the safety and effectiveness of products and it represents a significant burden in terms of resources and expense for the manufacturer.

One of the means the FDA uses for ensuring that medical devices are safe and effective is to require manufacturers to implement a risk management program. As part of the Quality System Regulation each manufacturer is required to determine the risk profile associated with each of their products, and to implement mitigations to control unacceptable risks. The implementation of the mitigations must be verified and a residual risk assessment performed to determine if the risk has been reduced to an acceptable level, and to confirm that the mitigation did not introduce any additional risks. The level of rigor involved should be appropriate to the level of risk presented to the patient and user.

## **THE CHALLENGE WITH 'SYSTEMS OF SYSTEMS'**

For medical device vendors, integrators or hospitals the challenge of applying the traditional approach that the FDA uses to regulate

medical devices to regulating MDDS' quickly brings you to the issue of dealing with systems of systems. In the hospital any number of separately classified and regulated devices may be interconnected through a MDDS to create multiple solutions for managing clinical data, often in conjunction with electronic medical records (EMR). These are usually configured into individual systems to perform specific tasks, e.g. collect and chart patient status and healthcare delivery for a single department or specialty area: 1.) combined vitals for mother & infant in L&D; 2.) combined anesthesia and vitals for surgery. Taken as a whole the result is a complex system composed of multiple systems, all communicating through the MDDS.

### **REGULATING SYSTEMS OF SYSTEMS**

There are significant challenges regulating these systems of systems. The current regulatory approach treats each device individually, according to its intended use. When devices are assembled into systems of systems the intended use of the whole may not be consistent with the intended use of each component in the system. Each individual implementation will be unique with different devices, different off-the-shelf or custom components, different network configurations and different EMRs and other applications running on the network. This raises many questions. How will the FDA classify them? Will the hospitals be required to file Premarket Notifications? Who is the manufacturer of the whole system? Who establishes and validates the intended use?

In January of this year, the FDA, along with the Center for Integration of Medicine and Innovative Technology (CIMIT) and the Continua Health Alliance, sponsored the Workshop on Medical Device Interoperability. This workshop brought together over 200 individuals from the medical device and health care information industries, along with clinicians, academics and regulators to discuss this very issue. John Murray, the software expert for the FDA's Center for Devices and Radiological Health (CDRH) made a very forward thinking proposal. He suggested that a group of people from the workshop should create a 510(k) submission for a "simulated" system of systems and submit it to the Office of Device Evaluation at the FDA as a means of working through the regulatory issues. He further proposed that the un-redacted results be posted as an open source for anyone to use. Much work remains to be done to bring this proposal to reality, but it is encouraging to see the FDA working closely with manufacturers and clinicians to solve these issues.

### **APPLICATION OF RISK MANAGEMENT**

When it comes to risk management, the standards used for medical devices are also not the same for MDDS' and systems of systems. The ISO-14971 standard, "Application of risk management to medical devices," is the most commonly used process for assessing and mitigating risk in individual medical devices. It is however, limited in its ability to assess the risk for systems of systems because it is applied to individual devices. It has some utility if the manufacturer considers interactions with other equipment during the assessment process, but it is unlikely that the manu-

facturer would be able to foresee the many ways a device could be used in such an environment.

This limitation was recognized by the FDA and others and, as a result of an earlier workshop in 2005, an effort was launched to create a new risk management standard, the IEC-80001 standard, "Application of risk management for IT Networks incorporating medical devices." This standard is due to go into effect this year. This is a great step forward in managing the risks inherent with systems of systems, but it still must be implemented. This will prove to

**For a hospital, the safest thing they can do while all of this is being sorted out is to choose a manufacturer of MDDS' that has already implemented their Quality and Risk Management Systems and received all available clearances and certifications.**

be daunting as hospital staffs cope with a multitude of devices with different intended uses being assembled to accomplish vital clinical tasks. The mechanics alone of validating the interoperability of many devices can quickly lead to a combinatorial explosion.

The challenge then is in applying risk management techniques for individual devices and for IT networks to a system of systems of medical devices of varying classes and intended uses that are assembled largely by the hospital biomedical and IT staffs. What is needed is a new approach.

### **A POSSIBLE ANSWER**

At the January Workshop on Medical Device Interoperability I proposed to take a page from the IHE book and apply it to managing risks in systems of systems. Risk profiles would be identified that include actors and transactions just as the IHE profiles do. But these transactions would be modeled on hazardous situations and are called risk case scenarios.

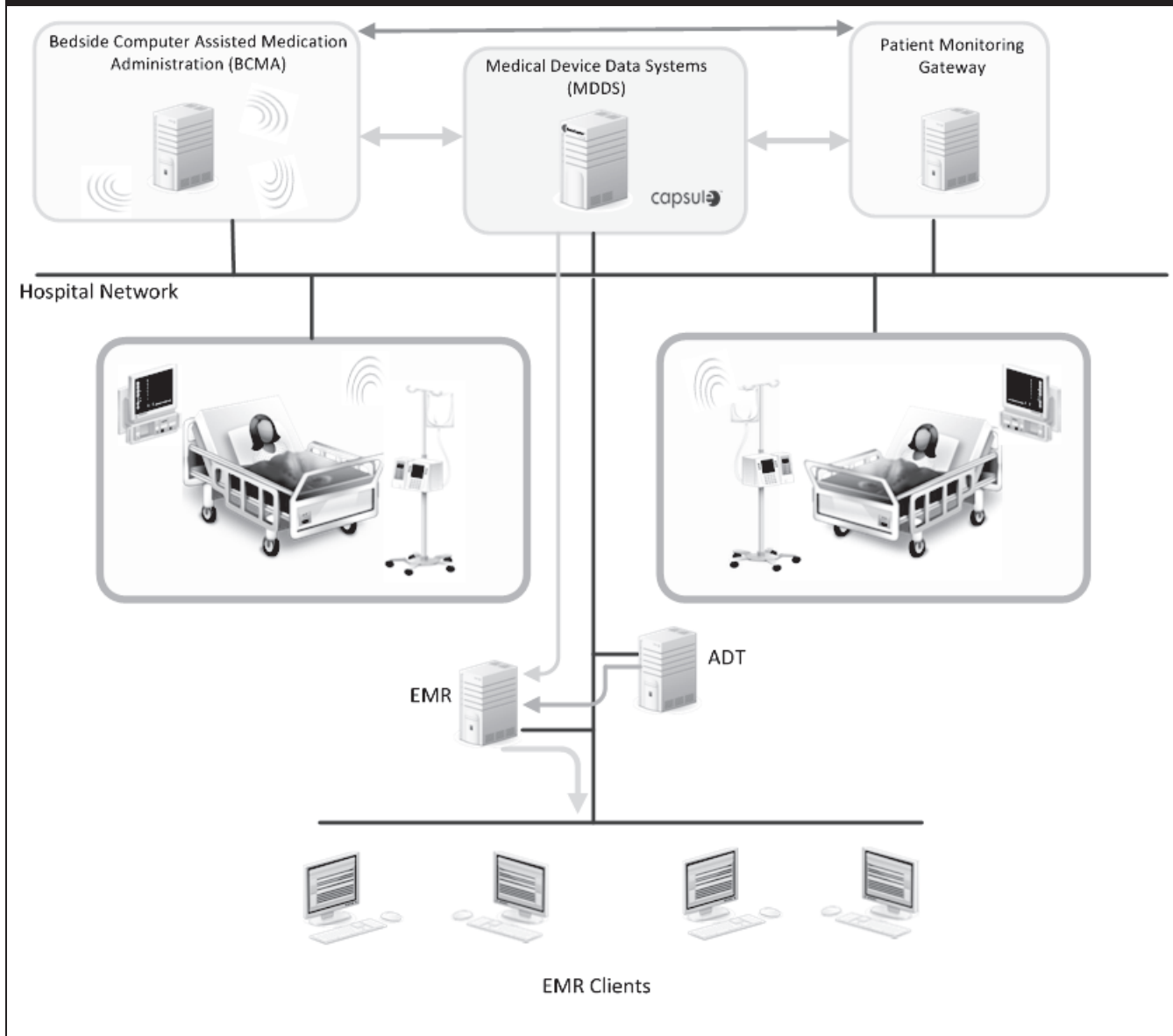
The scenarios are assessed according to ISO-14971. Each scenario identifies a hazard and associated harm. Multiple hazardous situations may be identified that would trigger the hazard and the probability of the situation occurring is determined. The resulting harm is then evaluated to determine its severity and the probability that harm would occur in the presence of the hazardous situation, and the risk is categorized according to its acceptability. If the risk is unacceptable, risk control measures are identified which will reduce the risk to an acceptable level.

Manufacturers would implement the control measures and then publish statements declaring their implementation. Depending upon the severity of the risk, certain risk profiles might require more rigorous verifications, perhaps through a notified body approach. Hospitals would be able to configure their own systems of systems and identify the manufacturers who are capable of meeting their risk management needs. An example will help to illustrate the mechanism.

### **RISK PROFILE EXAMPLE: PATIENT ASSOCIATION**

A risk case scenario in this profile identifies a hazard which is an

**Fig. 1: Risk profile example: Patient association.**



incorrect association between a patient and a monitor. One hazardous situation in this scenario is as follows. Two patients in a cardiac care unit are connected to a closed-loop system wherein a bedside computer assisted medication administration (BCMA) application is controlling an infusion pump in response to data it is receiving from a cardiac monitor. In this situation one patient is receiving a vasodilator and the other a vasopressor. The BCMA, monitors and infusion pumps are all communicating through a MDDS which is also providing data from the pumps and monitors to the EMR. The EMR interacts with other applications including ADT systems. All components are resident on the hospital's IT network.

An ADT transaction takes place which incorrectly associates the vasodilator patient with the vasopressor patient's monitor in the EMR. This is communicated to the BCMA which incorrectly chang-

es the titration of the vasodilator patient's medication. The patient goes into dysrhythmia and dies. Severity of the harm is catastrophic.

The risk profile contains a standard control measure for mitigating this risk. In this simple example it would be to make sure every transaction with the pump includes the patient ID associated with transaction. The pump would verify the ID with the ID it is associated to and raise an alert if there is a discrepancy. The verification would be a standard test protocol the manufacturer of the pump would perform. The manufacturer would then publish a declaration indicating they implemented and verified the risk profile.

**WHAT DOES ALL OF THIS MEAN FOR MDDS'**

This brings us back to MDDS. Given the definition provided by the FDA that specifically excludes altering the functions or param-

eters of any connected devices, how will a system incorporating an MDDS be used for interoperability? How will the FDA classify and regulate “systems of systems?” With MDDS’ playing such a central role it seems the definition would need to cover much more than “a device that provides one or more of the following uses: electronic transfer, exchange, storage, retrieval, display or conversion of medical device data without altering the function or parameters of any connected device.” A system of systems spans a much broader spectrum of connectivity and interoperability and could include any of the following:

- A system with a one way flow of data from a device.
- A more complex system where data is retrieved from a device in response to a request.
- A more sophisticated system where one device is controlling the operation of another device under the direction of a clinician.
- A very intricate closed loop system where one device is automatically controlling another in response to data it is receiving from a third device.

So, if the FDA implements its proposal and classifies MDDS’ as class I devices the question that remains is “will this provide the proper level of safety and effectiveness when MDDS’ are incorporated into the more complex systems of systems?” If the answer is “no,” then what? Will there be another classification of Medical Device Interoperability Systems? Will it be class II? What if it is interoperating with a class III life supporting device?

## **WHAT CAN HOSPITALS DO?**

Obviously the debate is ongoing and there is a lot to be worked out to effectively regulate MDDS’ and other “systems of systems.” The FDA knows it needs to be done. The challenge is getting it done right so it will not only work today but will be effective in the future as the technology evolves.

For a hospital, the safest thing they can do while all of this is being sorted out is to choose a manufacturer of MDDS’ that has already implemented their Quality and Risk Management Systems and received all available clearances and certifications. It is the only way for a hospital to really ensure that they are protected and insulated from all the regulatory discussions. It should, after all, be up to the manufacturer to design, develop, and bring their products to market in the safest way possible. A complete quality and risk management system is the only way to ensure this and therefore is an important consideration all hospitals should make when looking into any devices or technologies deployed in their facility. **JHIM**

---

**Peter Kelley** is Director of Quality Assurance and Regulatory Affairs. Mr. Kelley brings more than 20 years of experience developing and manufacturing medical devices under FDA GMP regulations, and delivering healthcare information systems. He has a strong technical background in design controls, management controls, CAPA and GMP.