RISK ASSESSMENT & MDS2 IN YOUR FACILITY

MDS2 Background

In 2003, under the HIPAA Security Rule, healthcare organizations were required to complete thorough risk assessments in all places where electronic protected health information (ePHI) resides. Needing to comply with this new regulation, healthcare providers began flooding medical device manufacturers with requests related to the security of their products. With no standard in place, manufacturers were responding in a variety of formats with varying degrees of information, making it difficult for healthcare organizations to compile responses and complete a proper security assessment. This prompted the Healthcare Information and Management Systems Society (HIMSS) to develop the first iteration of the MDS2 form, with the intent of providing information in a standard format to allow for consistent security assessments across manufacturers.

In 2011, the ANSI/AAMI/IEC 80001 international standard, *Application of risk management for IT networks incorporating medical devices – Part 1: Roles, responsibilities and activities*, was approved. The standard outlines a process for how healthcare organizations can manage risk and consider potential impacts on patient safety in an environment where more medical devices are being attached to information technology (IT) networks.[1] With 80001 in place, HIMSS and the National Electrical Manufacturers Association (NEMA) published a new version of the MDS2 form that includes key security information elements that healthcare providers need when conducting their 80001 risk assessments.[2]

MDS2 Overview

The intent of the MDS2 for is to supply healthcare providers with important information to assist them in assessing the vulnerability and risks associated with protecting private data transmitted or maintained by medical devices and systems.[3] The form is made up of a comprehensive set of medical device security questions that are divided into 19 categories. With limited free-text capabilities, MDS2 responses remain universal, facilitating the easy comparison of security features across different devices and different manufacturers.

MDS2 and AIMS

For proper risk assessment under HIPAA and in accordance with 80001, MDS2 forms should be associated with all medical devices that maintain or transmit private data. Completed MDS2 forms for many devices and systems are available directly from device manufacturers via their website. If the forms are not available there, organizations will need to contact a manufacturer representative and request they fill out the form.

In order to stay compliant and reduce the amount of printed MDS2 forms in your facility, the most efficient way to document your risk assessment efforts is to associate your MDS2 forms with their corresponding equipment in AIMS. The best way to do this is to download/scan the document from the manufacturer, and upload it as a document attachment directly to the model for which it applies.

Best Practices: Documenting MDS2 in AIMS

AIMS Version 2.6.0.0 is expected to be released in Fall 2016. This version will include enhancements that allow you to efficiently record and track your MDS2 forms in AIMS. As we get closer to the launch of 2.6.0.0, we will publish a MDS2 Best Practices document detailing the process of associating MDS2 forms with equipment in AIMS.

[1] http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HT_Interoperability/2011JF.cover.pdf
[2] http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HT_Interoperability/2011JF.cover.pdf
[3] http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx#download