SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

# Standards Navigator

## Standards Navigator Monthly Report

## 5-June-2015

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

# May 2015 Standards Navigator Overview

**Medical device software**

- The IEC 62304 amendment was approved with no negative votes. There were some editorial comments which will be considered by the IEC editors. Once the editorial changes are made and reviewed, the amendment will be published. Expect publication of the amendment by July, followed by a consolidated version that incorporates the amendment into the full standard. Adoption by CENELEC as an EN is happened concurrently, so harmonization by the EU should happen late this year or early next year. Normal procedure is to allow an 18 month transition period, but the standard writers suggested a 36 month transition. The length of the transition period will be decided by the European Commission. During the transition period, either the first edition or the amended version can be used to demonstrate conformity with the MDD and AIMD essential requirement for software. After the transition period, only the amended version will be accepted.
- The consultation period for the IMDRF SaMD draft of a quality system for Software as a Medical Device closed on June 1. The SaMD working group will now consider the comments received and create a final draft which will be submitted to the IMDRF steering committee this fall for approval. A final document should be published by the end of the year. It is likely that this document will have considerable influence on notified bodies that are auditing the quality system of a manufacturer that is developing software only medical devices.

  A draft for ballot of *IEC 82304-1 Health Software: General requirements for safety* was sent to IEC in early May. The draft will be translated into French before being circulated for review and voting. This normally takes two months, but final editing of the English and French versions by IEC may result in the draft not being available until after the IEC August break. This standard will be voted on concurrently by CENELEC and is expected to become a harmonized EN document. Conformance to this standard is expected to provide assumption of conformity to the software validation portion of the MDD essential requirement on software for those products that are only software.
- The working group developing the second edition of IEC 62304 met in April and is planning to meet again in September. Their schedule calls for a first committee draft to be available for review by the end of October.

**Medical Devices**

- The second DIS of the third edition of ISO 13485 passed in ISO but was not passed in the concurrent CEN ballot. This is a serious issue because the standard must be an EN adopted by CEN to be harmonized for the EU. The working group developing this standard will meet in June to discuss how to resolve the issues and proceed. One major concern is that the schedule for ISO 13485 has fallen behind the schedule for the next version of ISO 9001, which is expected in September, 2015. The third edition of ISO 13485 is being aligned with ISO 9001:2008, but the 2015 revision of ISO 9001 changes the structure to align with the ISO common management standards structure and also incorporates risk into the quality management system. Companies needing to conform to both ISO 13485 and ISO 9001 (and other management standards such as ISO 14001 or ISO 27001) are concerned about having a period where ISO 13485 deviates significantly from the others.
- *ISO/IEC Guide 63 - Guide to the development and inclusion of aspects of safety in International Standards for medical devices* is being revised. The work is to reflect current developments in applying risk management to medical devices considering the concepts in ISO/IEC Guide 51:2014 and ISO 31000:2009. A committee draft has been developed and circulated for comment. The purpose of Guide 63 is to provide practical guidance to standards writers on how to include safety aspects in the development of medical device standards including management system standards related to medical devices. This Guide impacts all standards for medical devices that include aspects related to safety.

  *The draft Guide is available on the SoftwareCPR Standards Navigator web page.*

- A new technical information report (TIR) has been proposed in AAMI. The new TIR is titled “Factors to consider when multi-vendor devices interact via an electronic interface; Practical applications and examples”. It is intended to assist stakeholders in considering risk factors when designing, testing, installing, and maintaining devices that are connected into a multi-vendor system via an electronic interface. A new work item proposal and a partial draft that illustrates the type of content being proposed have been created. This work has not yet been approved by the AAMI Standards Board and only preliminary work has been done.

  *The NWIP and draft are available on the SoftwareCPR Standards Navigator web page.*

**Health IT and mobile health applications**

- Work has begun on two recommendations of the ISO TC 215 ad hoc group on Health Software. The recommendations are to develop 1) a proposal for new work on health software and health IT common definitions, concepts and principles between medical electric equipment and health informatics; and 2) a proposal for revising the IEC 80001 series:
  - to expand the scope from networks incorporating medical devices to IT infrastructure incorporating medical devices or health software
  - to expand the scope to address risk management within the broader context of IT service management
  - to address the necessary key properties
  - to address the sociotechnical context of use
  - to clarify that these standard address the implementation and clinical use of health IT systems; and
  - to explore the need for applying system engineering concepts to health IT life cycle processes.

  *The TC 215 ad hoc group Health Software and Health IT report is available on the SoftwareCPR Standards Navigator web page.*

- The AAMI Health IT organizing committee held a meeting to discuss scope and stakeholders for two new standards on Health IT risk management and Health IT quality principles and practices. A call for committee members for the new Health IT committee will be issued in June and a stakeholder meeting is planned for October.

**Security**

- The draft of the 2nd edition of *ISO 27799 Health informatics — Information management in health using ISO/IEC 27002* passed unanimously and will be published following a short review of the resolution of comments that were received on the draft.

  *The draft with comment resolutions is available on the SoftwareCPR Standards Navigator web page.*

- AAMI circulated a draft of a technical information report on *Principles for medical device information security risk management – Risk management.* The objective of this TIR is to provide guidance on how medical device manufacturers can manage risks from security threats that could impact the confidentiality, integrity and/or availability of the device or the information processed by the device. Since medical device manufacturers are already familiar with ANSI/AAMI/ISO 14971:2007, this guidance follows the basic structure of that standard.

  The draft is available on the SoftwareCPR Standards Navigator web page.

**Software Engineering and Information Technology**

- No new documents this month.

## STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

| | Topic | Use / Users | Description |
|---|---|---|---|
| ISO/IEC 29919-5 DIS | Software engineering | Manufacturers | ISO/IEC 29119-5 - Systems and software engineering. Keyword driven testing. Draft for vote. |
| ISO/IEC/IEEE 12207 DIS | Software Engineering | Manufacturers | *ISO/IEC 12207 - Systems and software engineering — Software life cycle processes*<br>Draft for vote.<br><br>This new revision of ISO/IEC/IEEE 12207 is the product of a coordinated effort by IEEE and ISO/IEC JTC 1/SC 7 to completely harmonize life cycle process standards for systems and for software. |

# REFERENCE LIBRARY

| | Topic | Use / Users | Description |
|---|---|---|---|
| ONC 10-Year Vision | Health IT | Health IT infrastructure | *ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure*<br><br>The document can be found on the SoftwareCPR Standards Navigator web page or at http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf |
| BSI white paper | Medical devices | Manufacturers | *"The proposed EU regulations for medical and in vitro diagnostic devices"*<br><br>The white paper can be found on the SoftwareCPR Standards Navigator web page |

| | | | |
|---|---|---|---|
| EC green paper | Health IT | Manufacturers | *"Green Paper on mobile Health (mHealth)"*<br><br>The green paper can be found on the SoftwareCPR Standards Navigator web page |
| IMDRF SaMD Definitions | Software | Manufacturers | Software as a Medical Device (SaMD): Key Definitions<br>Report on international harmonization of definitions for software as a medical device. Adopted by IMDRF in November 2013.<br><br>***The report can be found on the SoftwareCPR Standards Navigator web page.*** |
| Euro Commission | Medical Devices | Manufacturers | Commission recommendation of 24 September 2013 on the audits and assessments performed by notified bodies in the field of medical devices.<br><br>***The document can be found on the SoftwareCPR Standards Navigator web page.*** |
| FDA Safety communication on cybersecurity | Security | Manufacturers and hospitals | FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations. This safety communication recommends that medical device manufacturers take steps to limit opportunities for unauthorized access to medical devices and hospitals take steps to evaluate network security and protect the hospital systems. The FDA also recommends prompt reporting of events that have impacted the performance of a medical device or hospital network. |
| ICS-CERT Alert regarding medical devices with hard-coded passwords | Security | Manufacturers, hospitals | ICS-CERT is issuing this alert to provide early notice of a report of a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware. The alert also identifies baseline mitigations for reducing risks to these and other cybersecurity attacks. |

| | | | |
|---|---|---|---|
| ONC Patient Safety Action & Surveillance Plan | Health IT safety | Health IT manufacturers, hospitals | The final version of the ONC plan that has the objectives to use health IT to make care safer and to continuously improve the safety of health IT. |
| *ONC contract with the Joint Commission to investigate health IT-related safety events* | Health IT safety | Hospitals, health IT manufacturers | The purpose of this contract is to ensure that there is an early detection system on health IT-related safety issues, including those associated with EHRs. |
| ONC guidance on annual surveillance plans by authorized certification bodies | Surveillance of certified EHRs | Authorized EHR certification bodies | Authorized Certification Bodies are expected to conduct surveillance on EHRs that they have certified. This guidance provides the priorities for topics to assess in the surveillance plan. Safety-related capabilities and security capabilities are two of the four areas for priority identified in this guidance. |
| TEAM-NB position paper on use of ISO 14971:2012 | Risk management | Manufacturers | Describes the steps TEAM-NB members plan to verify where relevant if requirements of EN ISO 14971:2012 have been met. This should help manufacturers update their risk management procedures and files to maintain compliance with the Essential Requirements of the directives, when building on the presumption of conformity.<br><br>***The position paper can be found on the SoftwareCPR Standards Navigator web page.*** |

| | | | |
|---|---|---|---|
| TEAM-NB "Vision on Revision" | Regulation | Regulators, Manufacturers, Notified bodies | This document forms the input of TEAM-NB into the debate on The Revision of European Legislation on Medical Devices. Contributions came from BSI Germany, BSI UK, DEKRA Netherlands, TUV Austria, and TUV Sud.<br><br>***The report can be found on the SoftwareCPR Standards Navigator web page.*** |
| Report | Interoperability | Medical device manufacturers, Hospitals, Regulators | AAMI/FDA Interoperability Summit report<br><br>An AAMI/FDA sponsored summit meeting on medical device interoperability was held in late 2012. This report documents the discussion and identifies themes from the summit.<br><br>This report can be found at http://www.aami.org/interoperability/Interoperability_Summit_publication.pdf |
| Report | Wireless | Hospitals, Medical device manufacturers | AAMI Wireless Workshop report<br><br>A workshop with approximately 80 invited medical wireless experts was held in late 2012. This report documents the discussion and outcomes of this workshop. A follow-up meeting is planned for March 2013.<br><br>This report can be found at http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf |

| | | | |
|---|---|---|---|
| Report | Security | Medical device manufacturers, Regulators | GAO report on FDA review of certain medical devices<br><br>The General Accounting Office does investigations for the US Congress. In this report they reviewed how FDA reviewed implanted medical devices that used wireless communications for security vulnerabilities that could cause safety concerns. They looked at two devices that researchers had shown could be controlled by use of off-the-shelf radio devices. In their findings, they criticized FDA for not reviewing security capabilities in these devices, even though they determined that FDA had the authority to do so. This will certainly result in FDA increasing their scrutiny of security for these type of devices. Since a security vulnerability in a device that is wirelessly communicating over a network seems to surely pose a risk as well, it is likely that FDA will also increase security scrutiny of all devices that use wireless communications.<br><br>Dr. Kevin Fu testified to the National Institute of Standards and Technology Information Security & Privacy Advisory Board that "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches."<br><br>A report of the meeting can be found in the MIT Technology Review<br>http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/<br><br>The article states that “In September, the Government Accountability Office issued a report warning that computerized medical devices could be vulnerable to hacking, posing a safety threat, and asked the FDA to address the issue. The GAO report focused mostly on the threat to two kinds of wireless implanted devices: implanted defibrillators and insulin pumps. The vulnerability of these devices has received widespread press attention (see "Personal Security" and "Keeping Pacemakers Safe from Hackers"), but no actual attacks on them have been reported.<br><br>Fu, who is a leader in researching the risks described in the GAO report, said those two classes of device are "a drop in the bucket": thousands of other network-connected devices used for patient care are also vulnerable to infection. "These are life-saving devices. Patients are overwhelmingly safer with them than without them. But cracks are showing," he said. (Fu was *Technology Review's* Innovator of the Year in 2009.)”<br><br>One of Dr. Fu’s collaborators in research that showed an implanted defibrillator could be hacked was Dr. William Maisel who is now the Deputy Director for Science at CDRH. FDA staff has indicated that they are in the process of revising the FDA Cybersecurity Guidance. This guidance will likely include recommendations for manufacturer’s security programs for devices and additional recommendations for security information to be provided during pre-market review of devices that are intended for use on a network. In addition, the guidance is now expected to provide information on when a security issue is reportable to the FDA and when a security event will result in a recall.<br><br>Another interesting bit of information in this report was the FDA response that they had hired a consultant (later determined to be McKinsey) to assess how they review software and make suggestions for improvements. This assessment is supposed to be completed by the end of 2012. |

| | | | |
|---|---|---|---|
| Report | Mobile medical devices | Medical devices manufacturers, Hospitals, Regulators | FCC report on Mobile Medical Devices<br><br>The FCC created an independent mHealth Task Force, to research the barriers to rapid deployment of mHealth technology and develop recommendations to government and industry to address those barriers. This report documents the task force recommendations for achieving 5 goals:<br>Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption.<br>Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication.<br>Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare.<br>Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies.<br>Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector.<br><br>Recommendations include:<br>• greater collaboration with other US Federal agencies<br>• promoting the availability of broadband for healthcare<br>• harmonizing spectrum allocations for healthcare internationally<br>• industry use of standards based technologies for transmitting authenticated messages and encrypted health information<br><br>***This report can be found on the Standards Navigator web page*** |
| Report | Health IT | Hospitals, EHR vendors, MD manufacturers | Institute of Medicine report – Health IT and patient safety<br><br>The Institute of Medicine produced a report on the impact of Health IT on patient safety. The report had a number of recommendations for the Secretary of HHS.<br><br>***A presentation on the recommendations and the entire report are available at the SoftwareCPR Standards Navigator web page.*** |

| | | | |
|---|---|---|---|
| Regulation | Regulation | Medical device manufacturers, IVD manufacturers | EU draft proposed new Medical Device Regulation and In-Vitro Device Regulation<br><br>These draft regulations can be found at<br>http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices<br><br>http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_541_en.pdf - In-vitro devices |

## STANDARDS CURRENTLY UNDER DEVELOPMENT OR REVISION

| | Topic | Use / Users | Description |
|---|---|---|---|
| IEC 62304 Amendment 1 | Software Life Cycle | Medical Device manufacturers, Regulators | Amendment to the Medical Device Software Life Cycle standard. This standard is harmonized in the EU. The amendment addresses software safety classification and how to be compliant with legacy software.<br><br>Current status: FDIS has been approved and final edits are being done by IEC.<br><br>Expected completion: mid 2015 |
| IEC 62304 Edition 2 | Software Life Cycle | Health Software Vendors including medical device manufacturers | The second edition expands the scope of 62304 from medical device software to health software. Health software is any software that is developed with an intended purpose of being used for health services. This includes software developed for medical devices.<br><br>Current status: An initial committee draft is being developed.<br><br>Next step: A draft is expected to be circulated in October 2015.<br><br>Expected completion: 2018 |

| | | | |
|---|---|---|---|
| IEC 82304-1 | Health Software | Medical device manufacturers, Regulators | New standard on Health Software: General Requirements. This standard is intended to be for standalone software products and to cover the product level requirements such as product validation, labeling, documents to be provided to the user, etc.<br><br>Current status: CDV has been registered with IEC.<br><br>Next step: A CDV is expected to be circulated in fall 2015.<br><br>Expected completion: 2016 |
| ISO 13485 | Medical devices | Medical device manufacturers, Regulators | The Quality Management System standard is being revised to bring it into alignment with ISO 9001:2008.<br><br>Current status: Second DIS was approved in ISO but not in CEN.<br><br>Next step: Resolve issues with CEN.<br><br>Expected completion: 2016 |