SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

15-May-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

April 2015 Standards Navigator Overview

Medical device software

- The ballot on the final draft of the IEC 62304 amendment closes in May. Expect publication by July, followed by a consolidated version that incorporates the amendment. Adoption by CENELEC as an EN is happening 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. During the transition period, either the first edition or the amended version could be used to demonstrate conformity with the MDD and AIMD essential requirement for software. After the transition, only the amended version will be accepted.

  The draft amendment is available on the SoftwareCPR Standards Navigator web page. IEC is expected to publish a consolidated version following approval and publishing of the amendment.

- The IMDRF SaMD draft of a quality system for Software as a Medical Device is available for public comment on the IMDRF website.

  A draft for ballot of *IEC 82304-1 Health Software: General requirements for safety* has been sent to IEC and should be available soon.

- Work on the second edition of IEC 62304 has begun and a committee draft is expected by the end of this year.

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 a standard must be an EN adopted by CEN to be harmonized for the EU. Discussions will be held at the next WG meeting in June on how to resolve the issues and proceed. One major concern is that the schedule for ISO 13485 now has it not being published until after 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) are concerned about having a 5 year period where ISO 13485 deviates significantly from the others.

- The Notified Bodies Recommendation Group has updated the draft of their document on Interpretation and Application of Annexes Z in EN ISO 14971: 2012. This is still a draft document and has not been adopted by the NBs. The document intends to bridge the gap between the interpretation of the relevant Essential Requirements of the Medical Devices Directives, as given in the Annexes ZA, ZB, and ZC of EN ISO 14971:2012, and the practice of placing safe medical devices on the market in the EU. Specific recommendations for medical device manufacturers in relation to the “content deviations” between the MDD and ISO 14971 are included.

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

Health IT and mobile health applications

- ISO TC 215 accepted the final report of their ad hoc group on Health Software. The report is titled “Health Software and Health IT Safety Standards FUTURE STATE Architecture/Framework and Roadmap. Following the acceptance of the report, TC 215 created two groups to develop proposals for new work on 1) health software and health IT common definitions, concepts and principles between medical electric equipment and health informatics; and 2) for revising the IEC 80001 series to expand the scope in several dimensions.

- 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 Health Software and Health IT report is available on the SoftwareCPR Standards Navigator web page.

Security

- The DIS 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 on the DIS.

  The post-DIS 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
IEC 62304 FDIS	Medical devices	Manufacturers	The final draft for vote (FDIS) of an amendment to IEC 62304 has been circulated. Major changes in the amendment are in how software safety classification is to be determined, how legacy software can conform to IEC 62304 and identifying and removing common software defects.
ISO/IEC 29919-5 DIS	Software engineering	Manufacturers	ISO/IEC 29119-5 - Systems and software engineering. Keyword driven testing. Draft for vote.
ISO/IEC 33010 pDTR	Software engineering	Manufacturers	ISO/IEC 33010 - Information Technology. Process Assessment "Guidance for performing an assessment." Preliminary draft technical report.
ISO/IEC/IEEE 12207 DIS	Software Engineering	Manufacturers	*ISO/IEC 12207 - Systems and software engineering — Software life cycle processes* Draft for vote. 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.

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 25011 CD	Information technology	Manufacturers	*ISO/IEC 25011 Information technology — Service Quality Requirements and Evaluation (SQuaRE) — Service Quality Model* Committee draft for comment. This International Standard defines a quality model for services that use IT made up from a combination of resources including people, processes, technology, facilities and information. The model is composed of characteristics (which are further subdivided into subcharacteristics) that can be used to support the requirements definition, design, deployment, delivery and improvement of services that use IT.

REFERENCES

	Topic	Use / Users	Description
ONC 10-Year Vision	Health IT	Health IT infrastructure	*ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure* 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"* 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)"* 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 Report on international harmonization of definitions for software as a medical device. Adopted by IMDRF in November. ***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. ***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. ***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. ***The report can be found on the SoftwareCPR Standards Navigator web page.***
Report	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/FDA Interoperability Summit report 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. 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 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. 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 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. 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." A report of the meeting can be found in the MIT Technology Review http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/ 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. 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.)” 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. 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 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: Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption. Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication. Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare. Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies. Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector. Recommendations include: • greater collaboration with other US Federal agencies • promoting the availability of broadband for healthcare • harmonizing spectrum allocations for healthcare internationally • industry use of standards based technologies for transmitting authenticated messages and encrypted health information ***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 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. ***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 These draft regulations can be found at http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices 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. Current status: Comments received on the CDV have been resolved and the FDIS is being edited by IEC. Expected completion: mid 2015
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. Current status: Comments received on the second CD are being resolved. Next step: A CDV is expected to be circulated in early 2015. Expected completion: end of 2015
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. Next step: Second DIS is currently out for ballot. Expected completion: 2016