SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

1-October-2014

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

September 2014 Standards Navigator Overview

Medical device software

The IMDRF Management Committee approved the final N12 document, “Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations,” of the SaMD WG. The MC also approved a Work Item Extension, “Applicability of Existing Quality Management System Requirements as a Risk Control Measure.” The WG is continuing the development of risk control measures under the Work Item Extension, and welcomes comments from the public on the final N12 document. The approved final N12 document has not yet been posted on the IMDRF web site.

Medical Devices

- A final draft international standard ***IEC 60601-1-11: Medical electrical equipment - Part 1-11: General requirements for basic safety and essential performance – Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment*** has been circulated for vote. This International Standard applies to the basic safety and essential performance of medical electrical equipment and medical electrical systems for use in the home healthcare environment. It applies regardless of whether the medical electrical equipment or medical electrical system is intended for use by a lay operator or by trained healthcare personnel.

Health IT and mobile health applications

No new documents. The IMDRF SaMD classification includes mobile and health IT applications that meet the definition of a medical device.

Quality

- The IMDRF has approved a Work Item Extension for the SaMD Working Group, “Applicability of Existing Quality Management System Requirements as a Risk Control Measure.” No documentation on this new effort is available.

Security

- The FDA published their final guidance on pre-market cybersecurity. This guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management. The document can be found at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- Draft for vote of a new version of ***ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002*** has been released. This standard provides specific requirements for use of ISO/IEC 27002 for healthcare. The new version is updated to use the 2012 version of ISO/IEC 27002. ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002.

Software Engineering

- A final draft international standard of a new version of ***ISO/IEC 15288 Systems and software engineering — System life cycle processes*** has been circulated for vote. This International Standard establishes a common process framework for describing the full life cycle of man-made systems from conception through retirement. This new version will replace the 2008 edition.
- A committee draft of a new version of ***ISO/IEC 12207 Systems and software engineering — Software life cycle processes*** has been circulated for comments. This International Standard establishes a common process framework for describing the full life cycle of software products (including software elements of systems) from conception through retirement. It is fully aligned with the draft version of ISO/IEC 15288 so that one may select appropriate processes from both standards for use in systems with substantial software content. This new 3rd edition of ISO/IEC 12207 will replace the 2008 version.
- A committee draft of ***ISO/IEC 24748-5 Systems and software engineering — Life cycle management — Part 5: Software development planning*** has been circulated for comments. The acquisition or supply of a system is usually done within a project. A project prepares and implements the technical plans and schedules necessary to guide the project toward accomplishment of its objectives and proper conclusion. Given the project's authorization and objectives, the project should establish plans for the technical management of activities as necessary for the software development effort. This International Standard unifies technical and management requirements and guidance from several sources to specify the requirements for the content of technical management and development plans, and provides common document formats. This International Standard also identifies the processes as defined in ISO/IEC 12207 to perform the necessary project planning activities to accomplish the project's technical effort and to develop the project's technical management and development plans.

Activity – September 2014

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC 60601-1-11 FDIS	Medical devices	Manufacturers	*IEC 60601-1-11: Medical electrical equipment - Part 1-11: General requirements for basic safety and essential performance – Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment* The FDIS can be found on the SoftwareCPR Standards Navigator web page.
ISO 27799 DIS	Security	Manufacturers	*ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002* ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. The DIS can be found on the SoftwareCPR Standards Navigator web page.
ISO/IEC 15288 FDIS	System Engineering	Manufacturers	*ISO/IEC 15288 Systems and software engineering — System life cycle processes* This International Standard establishes a common process framework for describing the full life cycle of man-made systems from conception through retirement. This new version will replace the 2008 edition. The FDIS can be found on the SoftwareCPR Standards Navigator web page.
ISO/IEC 12207 CD	Software Engineering	Manufacturers	*ISO/IEC 12207 Systems and software engineering — Software life cycle processes* This International Standard establishes a common process framework for describing the full life cycle of software products (including software elements of systems) from conception through retirement. The CD can be found on the SoftwareCPR Standards Navigator web page.

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
ISO/IEC 24748-5 FDIS	Software Engineering	Manufacturers	*ISO/IEC 24748-5 Systems and software engineering — Life cycle management — Part 5: Software development planning* This International Standard unifies technical and management requirements and guidance from several sources to specify the requirements for the content of technical management and development plans, and provides common document formats. The FDIS can be found on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

AAMI TIR 38 CDV	Medical devices	Manufacturers	TIR 38 - Medical Device Safety Assurance Case Report Guidance The draft TIR can be found on the SoftwareCPR Standards Navigator web page.
IEC 60601-4-3 DTR	Medical devices	Manufacturers	*IEC 60601-4-3 Guidance and interpretation – Considerations of unclear or unaddressed safety aspects in the third edition of IEC 60601-1 and proposals for new requirements* The draft TR can be found on the SoftwareCPR Standards Navigator web page.
ISO 9000 DIS	Quality	Manufacturers	*ISO 9000 - Quality management systems — Fundamentals and vocabulary.* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 9001 DIS	Quality	Manufacturers	*ISO 9001 - Quality management systems — Requirements.* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 25011 CD	Quality	Manufacturers	*Information technology – Service Quality Requirement and Evaluation (SQuaRE) – Service Quality Model* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO/IEC 26531 FDIS	Software	Manufacturers	*Software and system engineering — Content management for product lifecycle, user, and service management documentation* The draft standard can be found on the SoftwareCPR Standards Navigator web page.

ISO 29119-5 DIS	Software	Manufacturers	*Software and Systems Engineering — Software Testing — Part 5: Keyword-Driven Testing* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 25022 CD	Quality	Manufacturers	*Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of quality in use* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 23026 FDIS	Software	Manufacturers	*Systems and software engineering — Engineering and management of websites for systems, software, and services information* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 33050-4 PDTS	Security	Manufacturers and hospitals	*Information Technology — Process Assessment — Part 4: A process reference model for information security management* The draft technical specification can be found on the SoftwareCPR Standards Navigator web page.
ISO 33070-4	Security	Manufacturers and hospitals	*Information technology — Process assessment — Part 4: A process capability assessment model for Information Security Management* The draft technical specification can be found on the SoftwareCPR Standards Navigator web page.
ISO 16350 FDIS	Software	Manufacturers and hospitals	*Systems and Software Engineering - Application management* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 12182 DTR	Systems and software	Manufacturers	*Systems and software engineering — Framework for categorization of IT systems and software, and guide for applying it* The draft technical report can be found on the SoftwareCPR Standards Navigator web page.

NBRG Consensus paper on the interpretation and application of EN 14971:2012	Risk management	Manufacturers	This working draft provides background on the issues related to the Annexes Z in the EN version of ISO 14971 released in 2012. It attempts to bridge the gap between the wording in the Essential Requirements of the MDD and the use of ISO 14971 to develop medical devices that are "compatible with a high level of protection of health and safety" as required by the MDD. The draft makes recommendations for the seven "content deviations" between the wording in the MDD and the wording in ISO 14971. The working draft can be found on the SoftwareCPR Standards Navigator web page. **NOTE that this working draft has not yet been adopted by the entire NBRG.**
FDA draft guidance for MDDS	Medical devices	Manufacturers	*Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices – Draft Guidance for Industry and Food and Drug Administration Staff* In this draft guidance FDA notifies MDDS manufacturers that it does not intend to enforce compliance with regulatory controls for this type of medical device. The draft FDA guidance is available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm401785.htm

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
ISO TC 215 standards framework for health software Safety	Health software	Manufacturers	*Health Software Ad hoc group Interim Report – May 2014* *Health Software Safety Standards* *FUTURE STATE Architecture/Framework – DISCUSSION DRAFT* The report can be found on the SoftwareCPR Standards Navigator web page.
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 draft premarket cybersecurity guidance	Security	Manufacturers	Recommendations for security controls to assure medical device cybersecurity and documentation to submit in a premarket review to demonstrate effective cybersecurity management. Recommends identifying cybersecurity risks and providing a traceability matrix that links cybersecurity controls to cybersecurity risks that were identified. Also recommends documentation to demonstrate that the device will be provided to purchasers free of malware and a plan for providing updates and patches to provide up-to-date protection.
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.
NIST draft outline of a cybersecurity framework for critical infrastructure	Security	Hospitals, manufacturers	NIST was directed to prepare a cybersecurity framework for critical infrastructure in Presidential Executive Order 13636. Healthcare was identified as one of the areas with critical infrastructure. This draft for comment is only an outline of the framework. NIST intends the framework to take a risk management approach at a high level, focusing on key functions of cybersecurity management which are broken down into categories and subcategories. References such as existing standards, guidelines and practices will be provided for each subcategory. A draft of the framework will be released in October.
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
Presentation	Research	Medical device manufacturers	Medical Device Innovation Consortium (MDIC) Presentation from FDA and MDIC FDA and Life Science Alley have been collaborating on establishing a public-private partnership for research into regulatory science. A non-profit organization called the Medical Device Innovation Consortium has been created. This presentation by the FDA and the temporary director of the non-profit describes the need and the plans for this organization. ***This presentation can be found on the Standards Navigator web page.***

Announcement	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/UL collaboration on interoperability standards AAMI and UL have announced that they will collaborate on a series of standards for medical device interoperability. The press release announces the collaboration and its benefits. This announcement can be found at http://www.aami.org/news/2012/091712_press_AAMI_UL_Interoperability.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. This report can be found at http://www.gao.gov/products/GAO-12-816

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 first CD are being resolved. Next step: Second CD or CDV will be circulated. Expected completion: January 2014
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: Second CD has been circulated. Ballot closing February 28, 2014. Next step: Comments on second CD will be resolved and a CDV circulated. Expected completion: 2015

IEC 62366-1	Medical devices	Medical device manufacturers, Regulators	The standard on human factors engineering is being revised and divided into two documents. The first is a standard that includes requirements for the process. The second will be a technical report providing information about good practices for implementing the human factors process. This document is the first part. Current status: Comments have been resolved on the first CD and a second CD circulated. Next step: Comments received on the second CD. Expected completion: 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. Current status: Comments have been received on the first CD and are being resolved. Next step: Second CD or DIS. Expected completion: 2015