SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

2-December-2013

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

October 2013 Standards Navigator Overview

Medical device software

- A second committee draft for comment of IEC 82304-1 has been circulated. This draft has additional and revised content from the first CD. The comment period ends February 28, 2014.
- The IMDRF has adopted document N10 Guidance “Software as a medical device (SaMD): Key Definitions”. The IMDRF management committee agreed on the continuation of the work on international harmonization of the approach to software as a medical device.
- The Japan Diet approved a new version of the PAL in November. The new version includes software as a medical device.

Health IT and mobile health regulation

- Legislation has been introduced in the US Congress to modify what health IT and mobile applications would be regulated by the FDA. The Sensible Oversight for Technology which Advances Regulatory Efficiency (SOFTWARE) Act seeks to establish three kinds of software—medical, clinical, and health—the latter two of which would not be subject to regulation under the Federal Food, Drug, and Cosmetic Act. The bill, also known as the “Blackburn Bill” because it was introduced by Congresswoman Marsha Blackburn can be found at http://blackburn.house.gov/uploadedfiles/blackb_044_xml.pdf

Usability

- No new documents

Security

- NEMA has published a revised edition of the Manufacturer Disclosure Statement for Medical Device Security. This new version is aligned with IEC 80001-2-2 and describes information intended to assist professionals responsible for security risk assessment processes in their management of medical device security issues. The standard and an Excel spreadsheet template are available from NEMA at http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
- IEC has issued a ballot for a new project on medical device security. It is for a technical report, *IEC 80001-2-x, Application of risk management for IT networks incorporating medical devices - Part 2-X: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*. This TR will provide guidance on which requirements of 6 existing security standards could be used to achieve the security capabilities of IEC 80001-2-2. The NP ballot and comments on the draft TR are needed by February 28, 2014.
- In addition to the final version of the FDA guidance “*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*”, FDA also expects to publish a draft guidance document on post market reporting of cybersecurity vulnerabilities. The approach is expected to be one of encouraging fast correction of identified vulnerabilities prior to their being exploited by not requiring reporting of these issues. If a cybersecurity vulnerability is exploited, then a report will be required and a possible recall needed.

Medical Devices

- A final draft of the IEC 60601-1-2 collateral standard on *Electromagnetic disturbances – Requirements and tests* has been circulated. This new version is a significant technical revision from the 2007 version. It includes specification of immunity test levels according to the environments of intended use, categorized according to locations that are harmonized with IEC 60601-1-11: the professional healthcare facility environment, the home healthcare environment and

special environments. It also recognizes that RF wireless communications equipment can no longer be prohibited from most patient environments because in many cases it has become essential to the efficient provision of healthcare. The ballot for the FDIS ends on January 31, 2014.

Software Engineering

- No new documents

Activity – November 2013

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC 82304-1 CD2	Software products	Manufacturers	*IEC 82304-1: Health Software - Part 1: General requirements for product safety.* This standard is intended to provide requirements for health software products. These are product requirements, and 82304-1 refers to 62304 for software process requirements. This standard is expected to cover the EU essential requirement for software validation when the product is only software (this essential requirement is covered by IEC 60601-1-1 for software that is a part of medical electrical equipment.) ***The draft standard can be found on the SoftwareCPR Standards Navigator web page. The ballot closes on February 28, 2014.***

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC 80001-2-x NP	Security	Manufacturers	*IEC 80001-2-x, Application of risk management for IT networks incorporating medical devices - Part 2-X: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2* This proposed technical report maps applicable requirements in six security standards to the security capabilities identified in IEC 80001-2-2. This provides guidance to medical device manufacturers as to which security standards and requirements are possibly useful in achieving the security capabilities. A supplemental document is provided to assist reviewers in assessing the appropriateness of the identified security requirements. ***The draft standard and supplemental document can be found on the SoftwareCPR Standards Navigator web page. The ballot closes on February 28, 2014.***

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC 60601-1-2 FDIS	Medical devices	Manufacturers	*IEC 60601-1-2: Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic disturbances – Requirements and tests* This revised standard will replace the edition of 2007. It includes technical changes such as: • specification of immunity test levels according to the environments of intended use, categorized according to locations that are harmonized with iec 60601-1-11: the professional healthcare facility environment, the home healthcare environment and special environments; • specification of tests and test levels to improve the safety of medical electrical equipment and medical electrical systems when portable rf communications equipment is used closer to the medical electrical equipment than was recommended based on the immunity test levels that were specified in the third edition; • specification of immunity tests and immunity test levels according to the ports of the medical electrical equipment or medical electrical system; • specification of immunity test levels based on the reasonably foreseeable maximum level of electromagnetic disturbances in the environments of intended use, resulting in some immunity test levels that are higher than in the previous edition; and • better harmonization with the risk concepts of basic safety and essential performance, including deletion of the defined term “life-supporting”; ***The draft standard can be found on the SoftwareCPR Standards Navigator web page. The ballot closes on January 31, 2014.***

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

ISO/IEC 25063 FDIS	Usability	Manufacturers	ISO/IEC 25063 *Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: Context of use description*. This International Standard specifies the contents of both high-level and detailed descriptions of context of use for an existing, intended, designed or implemented system, product or service. It also describes the purposes for which context of use descriptions are used, and identifies the intended users of context of use descriptions. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
IEC 62368 FDIS	Audio/Video and ICT equipment	Manufacturers	IEC 62368-1 *Audio/video, information and communication technology equipment - Part 1: Safety requirements*. This standard replaces IEC 60065 *Audio, video and similar electronic apparatus - Safety requirements* and IEC 60950-1 *Information technology equipment - Safety - Part 1: General requirements.* The safety requirements of these two standards are merged into a single standard as these types of equipment are merging. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO/IEC TR 12182 WD	Systems and software	Manufacturers	ISO/IEC TR 12182 *Categorization of systems and software products*. Describes a framework for categorizing and a scheme of classification axes. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***

REFERENCES

	Topic	Use / Users	Description
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. This is a draft for comment. Comments should be submitted before September 13.
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	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

infrastructure			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