SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

8-June-2016

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

Standards and regulatory activity overview

A lot of standards and regulatory activity is expected in 2016. Here are some of the areas to watch. Changes to status since the last report are in red text.

- IEC 82304-1 *Health Software: General requirements for safety* will be completed during the first half of 2016. It is intended that this standard be harmonized in the EU, but it is not clear when this may happen.

  Status: The FDIS has been submitted to IEC and will be circulated when the French translation is complete. The FDIS should be circulated by the end of July for final approval. This is a two month up or down vote so the approval should occur by October and publication late in 2016 or early 2017.

- A first committee draft of the second edition of IEC 62304 will be circulated for review in the first half of 2016. The second edition will expand the scope of the standard to health software.

  Status: The first CD is ready to be circulated in June.

- New standards for health software covering all parts of the life cycle will be proposed in 2016.

  Status: A proposal for a new standard, Health software and health IT systems safety, effectiveness and security – Foundational principles, concepts, and terms has been circulated to ISO and IEC for approval to begin developing the standard.

- AAMI will move its work on HIT quality management systems and HIT risk management forward. The goal is to complete these by the end of 2016.

  Status: Drafting of these standards has begun. An HIT committee has been established in AAMI. The next meeting of the committee to review a draft of the standards will be in June. The AAMI standards board approved new work on EHR Usability. This will be added to the work of the AAMI HIT committee.

- A revision of IEC 80001-1 will begin in 2016.

  Status: The proposal for extending the scope of the 80001 series and for revising 80001-1 has been submitted to ISO and IEC for approval to begin the revision. Work on the revision is expected to start in October.

- The revision to ISO 13485 will be published in the first half of 2016.

  Status: The 2016 edition of ISO 13485 has been published by ISO.

- ISO 14971 is currently under review. It is likely that a revision (amendment or new edition) will be started in 2016.

  Status: The review of 14971 has been completed with mixed results. A meeting of the working group will be held in June to discuss whether a revision is necessary. It seems likely that some changes will be proposed.

- A second amendment to IEC 60601-1 will be started in the second half of 2016. This amendment is scheduled to be completed in 2019. A fourth edition of 60601-1 will be started following the completion of the amendment and will be scheduled for completion in 2024. Discussions about the structure of the fourth edition will likely begin in 2017 and decisions made before work is started on the fourth edition.

  Status: A meeting of the advisory group for the second amendment was held in February. This meeting identified the most important changes that are needed to be made in the amendment. The proposed changes will be discussed and an approved list finalized at a meeting of SC 62A in October.

- Agreement has reportedly been reached on the issues in the proposed EU Medical Device Regulation and IVD Regulation. The texts of the regulations are expected to be made available in June.

- The first deliverables from UL/AAMI 2800 on medical device interoperability should be completed in 2016.

  Status: The committee is meeting in June to review the work to date.

- AAMI TIR 57 on medical device cybersecurity risk management will be published in 2016.

  Status: The TIR has been approved for publication. The published document should be available in the next few months.

- Many documents, both standards and regulations, on security and privacy will be in process during 2016.

  NIST has announced that it will be revising SP 800-53, the most complete compilation of security controls.

  UL has begun publishing a series of standards on security, UL 2900.

  A group in Germany active in medical device standards has expressed an intention to propose an international standard for medical device security risk management.

  The new General Data Privacy Regulation has been approved in the EU.

  The second edition of *ISO 27799 Health informatics -- Information security management in health using ISO/IEC 27002* has been submitted for publication. The published standard should be available before the end of 2016.

  A new standard has been released by the Diabetes Technology Society - Standard for Wireless Diabetes Device Security (DTSec).

May 2016 Standards Navigator New Documents

Medical device software

- A draft technical report (DTR) of *ISO 80002-2 Validation of software for medical device quality systems* has been circulated for ballot. This technical report provides guidance for validation of process software used in medical device quality systems using a risk-based approach. This includes software used in the quality management system, software used in production and service provision, and software used for the monitoring and measurement of requirements, as required by subclauses 4.1.6, 7.5.6 and 7.6 of *ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes*.

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

Medical Devices

- A committee draft for comment has been circulated for *IEC/TR 60601-4-4: Medical electrical equipment – Part 4-4: Guidance and interpretation – Guidance for writers of particular standards – Creating alarm system-related requirements*. This guidance is addressed to writers of medical device standards when alarm system requirements are included in the standard. It includes suggested model language for common alarm system requirements. This guidance is considered necessary because of inconsistency in the references to alarm system-related requirements in various medical device standards. The goal is to provide a consistent model language that can be used in any medical device standard that includes alarm system requirements.

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

Health IT and mobile health applications

- A new project for a standard on *Health software and health IT systems safety, effectiveness and security – Foundational principles, concepts, and terms* has been proposed. The intent of this new proposal is to provide a common explanation of the principles, concepts and terms for health software and health IT systems across the entire lifecycle, from concept to disposal. The need for this standard became apparent when it was recognized that different communities in healthcare had different understandings of same or similar terms. This document will provide a unifying foundation for other standards that collectively address all lifecycle stages, the context of use, and focus areas necessary to ensure the safety, effectiveness, and both data and system security (including privacy) of health software and health IT systems. This work is intended to complement existing established standards.

  The new proposal is available on the SoftwareCPR Standards Navigator web page.

- AAMI has approved new work on EHR usability. Two new projects have been approved.
  - *Process Guide for Designing EHR User Interfaces* – This standard is intended to help EHR developers plan and implement a user-centered design process that results in safe, effective, and usable application.
  - *EHR User Interface Design Guidance* – This technical report will provide guidelines for designing user interfaces for electronic health records and will help EHR developers create safe, effective, and usable EHRs.

  Work on these new projects will begin at the AAMI HIT committee meeting in late June.

  The new proposals are available on the SoftwareCPR Standards Navigator web page.

- A draft of the EU mHealth privacy Code of Conduct is available for review. This document is the result of an industry-led initiative of the European Commission. It is targeted at app developers and its purpose is to foster justified trust among users of mHealth apps which process personal data.

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

- A draft of *EU guidelines on assessment of the reliability of mobile health applications* is available for review. The purpose of the mHealth app assessment guidelines is to establish a framework of safety, quality, reliability and effectiveness criteria to improve the use, development, recommendation and evaluation of mHealth apps.

  The draft guidelines are available on the SoftwareCPR Standards Navigator web page.

Medical device and Health Security

- The Diabetes Technology Society has release a standard *Diabetes Technology Society Standard for Wireless Device Security (DTSec).* The purpose of DTSec is to establish a standard used to provide a high level of assurance that electronic products for the treatment of diabetes deliver the security protections claimed by their developers and required by their users. The standard utilizes international standards ISO/IEC 15408:2009 (Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model) and ISO/IEC 18045:2005 (Security techniques -- Methodology for IT security evaluation).

  The standard is available on the SoftwareCPR Standards Navigator web page and is also available from the Diabetes Technology Society.

- The European Union General Data Protection Regulation (GDPR) has been published in the Official Journal. The Regulation entered into force in May 2016, and will apply from May 2018 following transposition into national law by the Member States of the EU. This regulation applies to all companies collecting and processing personal data in the EU and does include medical devices. It specifically lists genetic data and biometric data as sensitive personal data. Developers (both medical device and health products that are not regulated as medical devices that collect or process personal data) will be under specific obligations to introduce data protection by design and default into their systems. The GDPR also introduces an obligation to report data breaches to data protection authorities and to affected individuals if the personal data breach is likely to result in a risk to individuals. It also includes the “right to be forgotten” which means that companies will need to be able to erase upon request any personal health data that they collect or process. There is also a “right of data portability” which allows a patient to request their data or request that their data be provided to another provider. There is no grandfathering under the GDPR, so in May 2018 all existing systems must be able to meet these requirements.

  The regulation is available on the SoftwareCPR Standards Navigator web page and is also available at http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

Software Engineering and Information Technology

- A draft for ballot (DIS) of *ISO/IEC 20246 - Software and Systems Engineering Work product reviews* has been circulated. The purpose of ISO/IEC 20246 Work Product Reviews is to provide an International Standard that defines work product reviews, such as inspections, reviews and walkthroughs that can be used at any stage of the software and systems life cycle. It contains a generic process, activities, tasks, review techniques and documentation templates that are applied during the review of a work product.

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

- A proposal has been made for a new ISO Technical Committee on *Blockchain and electronic distributed ledger technologies.* The scope of the proposed new committee is “Standardization of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems”. While this new field of technical activity is not specific to healthcare, the ability for secure interoperability and data exchange is essential for healthcare.

  The new proposal is available on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO 30754 DIS	Software engineering	Manufacturers	This specification identifies five aspects of software trustworthiness: safety, reliability, availability, resilience and security, and defines a framework of principles and techniques which can be tailored to suit the context and intended use. This is a draft for vote.
ISO 33053 NP	Quality management	Manufacturers	This technical specification defines a process reference model (PRM) for the domain of quality management. The scope of the quality management domain is determined by the requirements in ISO 9001:2015. The model specifies a process architecture for this domain, and comprises a set of processes, with each described in terms of process purpose and outcomes. This is a new proposal for vote.
ISO 33073 NP	Quality management	Manufacturers	This Technical Specification defines a process capability assessment model (PAM) for quality management based on the PRM defined in ISO/IEC TS 33053. It defines an exemplar PAM that supports the performance of an assessment by providing indicators for guidance on the interpretation of the process purposes and outcomes as defined in ISO/IEC TS 33053 and provides guidance, by example, on the definition, selection and use of assessment indicators of process performance and process capability.
ISO 11633-1 NP	Software engineering	Manufacturers	This document focuses on remote maintenance services (RMS) for information systems in health care facilities as provided by vendors of medical devices or health information systems (RMS providers) This is a new proposal for vote.
ISO 26513 DIS	Software engineering	Manufacturers	This standard provides the minimum requirements for testing and reviewing user documentation, including both printed and online documents. This is a draft for vote.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO 24748-5 DIS	Software engineering	Manufacturers	This standard provides a common framework for planning and controlling the technical processes and activities to produce and sustain software products. This is a draft for vote.
ISO/IEC 29119-5 FDIS	Software Engineering	Manufacutrers	This standard defines a unified approach for describing test cases in a modular way, which assists with the creation of items like keyword-driven test specifications and test automation frameworks. Keywords are elements used to compose test cases, such as building blocks. The standard defines the main concepts and application of keyword-driven testing and defines attributes of frameworks designed to support keyword-driven testing.