Journal of Systems and Information Technology

Software-as-a-Medical Device: demystifying Connected Health regulations
Noel Carroll Ita Richardson

Received 10 July 2015
Revised 20 January 2016
Accepted 22 January 2016

Software-as-a-Medical Device: demystifying Connected Health regulations

Noel Carroll
ARCH – Applied Research for Connected Health Technology Centre, University of Limerick, Limerick, Ireland, and
Ita Richardson
Lero – the Irish Software Research Centre, University of Limerick, Limerick, Ireland

Abstract

Purpose – Connected Health is an emerging and rapidly developing field never before witnessed across the healthcare sector. It has the potential to transform healthcare service systems by increasing its safety, quality and overall efficiency. However, as healthcare technologies or medical devices continuously rely more on software development, one of the core challenges is examining how Connected Health is regulated – often impacting Connected Health innovation. The purpose of this paper is to present an understanding of how Connected Health is regulated. Many of these regulatory developments fall under "medical devices", giving rise to Software-as-a-Medical Device (SaaMD).

Design/methodology/approach – Through an extensive literature review, this paper demystifies Connected Health regulation. It presents the outcome of expert discussions which explore the key regulatory developments in the context of Connected Health to provide a practical guide to understanding how regulation can potentially shape healthcare innovation.

Findings – Several key issues are identified, and the authors present a comprehensive overview of regulatory developments relating to Connected Health with a view to support the continued growth of IT-enabled healthcare service models. The authors also identify the key challenges in Connected Health and identify areas for future research.

Originality/value – A key outcome of this research is a clearer understanding of the opportunities and challenges that regulation and standards present to Connected Health. Furthermore, this research is of critical importance in a first attempt towards recognising the impact of regulation and standards compliance in Connected Health.

Keywords Regulation, Healthcare, Connected Health, Software-as-a-Medical Device

Paper type Literature review

1. Introduction

Connected Health is an emerging and rapidly developing field which has the potential to transform healthcare service systems by increasing their safety, quality and overall efficiency. While considered a disruptive technological approach (Christensen *et al.*, 2000) in healthcare, it is used by different industries in various sector contexts (e.g. healthcare, social

This work was supported, in part, by ARCH – Applied Research for Connected Health Technology Centre (www.arch.i.e.), an initiative jointly funded by Enterprise Ireland and the IDA, SFI Lero Grant (www.lero.i.e.) 13/RC/2094 and SFI Industry Fellowship grant Number 14/IF/2530.

Journal of Systems and Information Technology
Vol. 18 No. 2, 2016
pp. 186-215

1328-7265
DOI 10.1108/JSIT-07-2015-0061

care and the wellness sector). Thus, various definitions for Connected Health exist with different emphasis placed on healthcare, business, technology and support service providers, or any combination of these. Within the research community, Connected Health is not well-defined and remains an ambiguous concept. The ECHAlliance (2014) group promote the concept of Connected Health to act as "the umbrella description covering digital health, eHealth, mHealth, telecare, telehealth and telemedicine". In addition, described by Caulfield and Donnelly (2013), Connected Health refers to:

> […] a conceptual model for health management where devices, services or interventions are designed around the patient's needs, and health related data is shared, in such a way that the patient can receive care in the most proactive and efficient manner possible.

Connected Health has been defined by Richardson (2015) as:

> […] patient-centred care resulting from process-driven health care delivery undertaken by healthcare professionals, patients and/or carers who are supported by the use of technology (software and/or hardware).

Therefore, Connected Health can be considered to be a socio-technical healthcare model that extends healthcare services beyond healthcare institutions (Carroll *et al.*, 2016). Through the exploitation of technological innovations, healthcare providers can generate accurate and timely information for patients and clinicians to make better decisions. Improved decision-making tools can improve the likelihood of saving lives, saving money and ensuring a better quality of life during and post treatment (Hunink *et al.*, 2014). Regardless of the various definitions, the key here is the process of connectedness and the manner in which technological solutions enable healthcare solutions. In addition, the Food and Drug Administration (FDA) (2014) describes Connected Health as:

> […] electronic methods of health care delivery that allow users to deliver and receive care outside of traditional health care settings. Examples include mobile medical apps, medical device data systems, software, and wireless technology.

Thus, Connected Health aims to utilise the connectivity of technologies to support independent living to maximise its effects on society and, ultimately, to improve the lives of citizens. In some cases, these technologies may be also considered as medical devices. The regulatory environment is a critical aspect of all healthcare technologies and one which presents the greatest challenge for many companies to understand its use to guide healthcare innovations. From a Connected Health perspective, it is often unclear as to what constitutes as a "wellness device" and a "medical device". Even the concept of "connected" health implies, for example, that peripheral devices may be considered to be the medical devices, but the connectivity or the process of integrating them into one service solution may not. Thus, the concept of "intended use" often determines whether a product is a medical device or a general health wellness support service. Intended use or intended purpose refers to "the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials" (Article 1(2)g of Directive 93/42/EEC). While this is merely an example of some of the day-to-day issues companies face with various healthcare innovations, we identified the need to undertake a study to examine the regulatory landscape and how it potentially influences Connected Health developments. We attempt to demystify Connected Health regulation and focus on Software-as-a-Medical Device (SaaMD) to guide our understanding of the regulatory environment in Connected Health.

2. Software development process

Medical devices have become increasingly sophisticated due to software capabilities and applications becoming increasingly important. Failure in software functionality can have a fatal consequence or cause serious injury to patients. Therefore, the software development process is of vital importance and regulating this across medical devices is considered a fundamental core element of medical device manufacturing. To regulate the software development process, IEC 62304 defines the software development and verification activities which medical device manufacturers must comply with. Such activities include software development planning, requirement analysis, architectural design, software design, unit implementation and verification, software integration and integration testing, system testing and, finally, software release (Figure 1). The software development life cycle includes risk management, configuration management and problem resolution processes which are guided by IEC 62304 at each stage of the software development process.

Mitigating risk is crucial throughout the risk analysis stage to identify and remove issues which present a potential to contribute towards a hazardous situation and their causes. The potential causes should be documented in the risk management file on which a risk control measure must be defined, implemented, verified and documented. This provides greater transparency on software issues and adds greater traceability between the hazardous situation, software items, software cause, risk control measures and verification of risk control measures. The safety classification of the medical device also influences the software development planning and management processes while demonstrating a risk management protocol which enables developers and evaluators to trace the risk control measures to the software requirements. Under IEC 62304, responsibility of the manufacturer also goes beyond the release of the software product, with particular emphasis on product maintenance. The maintenance process requires that the manufacturer monitors the feedback of the released product from both within the organisation and from the user. This feedback must be documented and analysed to determine whether a problem exists. Therefore, quality is a key factor which may involve additional upfront costs and potential change of current practices; compliance to IEC 62304 produces higher quality. However, a safer product deduced the cost associated with recalls, development and maintenance. In addition, it enhances the company's overall credibility and reputation. Many software developers adopt the V Lifecycle Model to support the medical device software development (and possible an agile development ethos) which may be more suitable for Class II and III devices (McHugh *et al.*, 2012). It offers an approach which complements both the product development and software development phases, for example:

- *Definition phase*: Identify the requirements and specifications of the medical device.
- *Design phase*: High-level (software architecture) and low-level (unit and/or object) design.
- *Code*: Develop code to meet the intended use.
- *Unit and integration tests*: Examine the structure (white-box) of the software to ensure the application operates as designed.

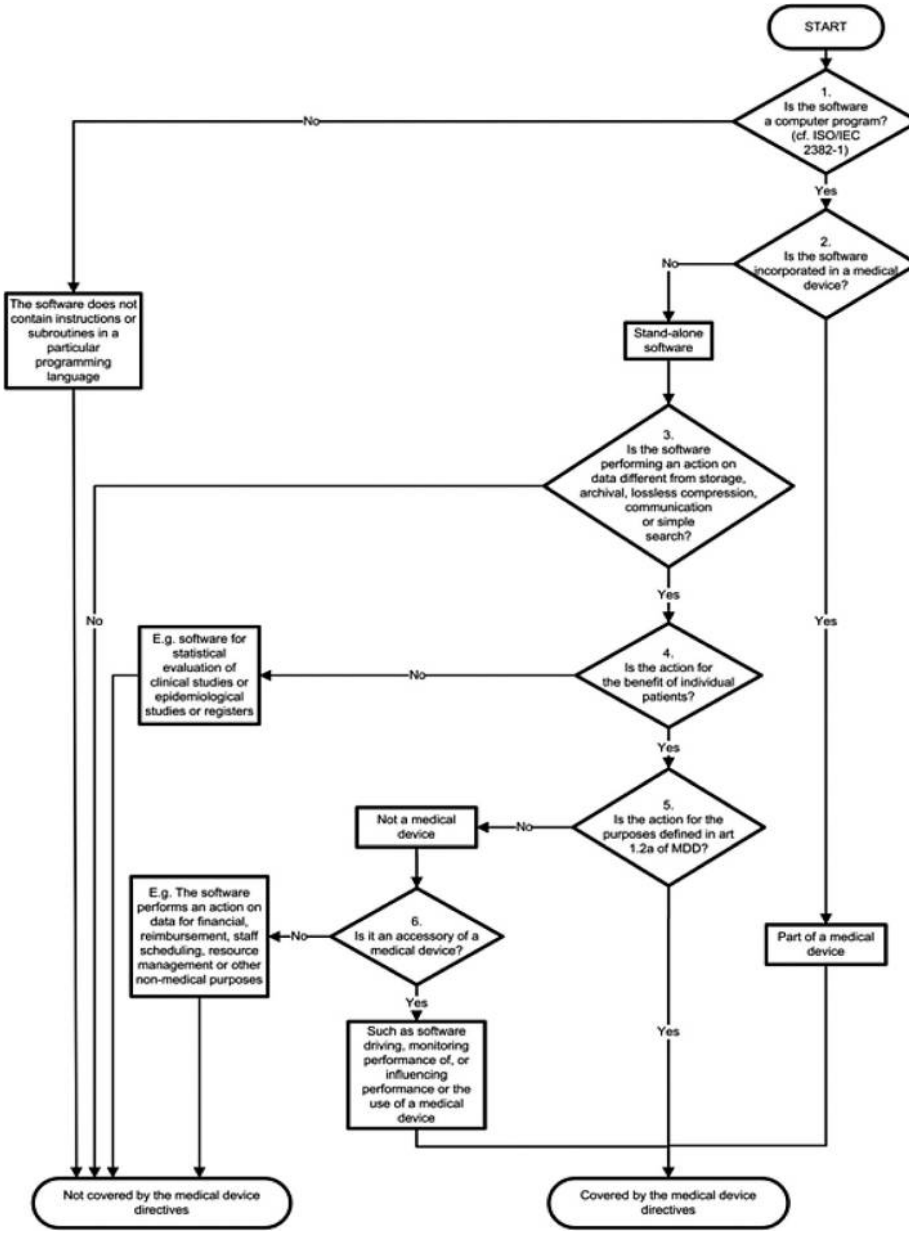


Figure 1.
Overview of software development processes and activities in IEC 62304[1]

- *System and user's acceptance testing*: Examine the functionality (black-box) to determine whether it meets its goals and supports the intended use of the medical device.

There have been some new developments in this area, for example the development of MDevSPICE (formally known as MediSPICE) (McCaffery and Dorling, 2009; McCaffery *et al.*, 2010; Clarke *et al.*, 2014). The MDevSPICE framework is one of the first attempts to address the safety concerns faced by medical device producers and presents a software safety assessment process. Verification and validation activities are very important in software development and can consume much of a project's costs and effort. While verification and validation is addressed by process models and standards for both generic and safety critical software development, there are still challenges in undertaking its successful implementation as part of the software development process. The process of verification and validation requires a clear understanding of how each activity is undertaken and related to each other, which is important in a Connected Health environment. Process model can also support the verification process and is defined by the Capability Maturity Model® Integrated (CMMI) as:

- "Confirmation that work products properly reflect the requirements specified for them."
- "Verification refers to the process determining whether or not the products of a given phase of a software development process fulfil the requirements established during the previous phase."

The CMMI also guides organisations and ensures that the correct system is being developed throughout each stage in the development cycle and conforms to their specification. However, it is important to realise that software process models, such as CMMI, do not cover medical device regulations, and that they need to be used in conjunction with the regulations (Burton *et al.*, 2006). Any review of the software development process should involve a number of key stakeholders, including project personnel, healthcare practitioners, managers, users/patients, customers or other interested parties, to review, comment or approve the Connected Health technology. This can comprise using both informal and formal processes (e.g. reviews, walkthroughs, inspections and audits). Validation may be described as a process of evaluating software at the end of its development to ensure that it is free from failures and complies with its requirement. This validation occurs through the utilisation of various testing approaches, that is that the software, as provided, will fulfil its intended purpose. Changes are often required to support software improvements. There are guidelines to support this also. For example, the development of an international software process improvement (SPI) framework for the medical device industry acts as a key enabler of best practice for the healthcare sector. SPI techniques offer a continuous cycle of performing an assessment and restarting the cycle (McHugh *et al.*, 2012) with the aim of reducing defective software. Software may also be vulnerable to outside attack. Many hospitals and healthcare facilities use various threat management software and firewalls to monitor their mobile device applications to ensure that they are secure and safe. In most cases, within the USA, this is a requirement of Health Insurance Portability and Accountability Act (HIPPA).

HIPAA is a framework which is followed by number of organisations for maintaining the security and privacy of the health information. HIPAA came into action in 1996 to address a number of concerns, most notably the need for increased protection of the medical records of the patients against unauthorised access (Wu *et al.*, 2012). HIPAA provides a national standard for electronic healthcare transactions. It also provides regulations regarding healthcare information security and privacy (Jepsen, 2003). HIPAA covers entities such as healthcare providers, insurers and providers of health plan. Healthcare organisations are now required to individually assess their security and privacy requirements using various auditing tools. Healthcare technology systems have access to personal identifiable information. Our traditional view of privacy protection methods through various anonymisation techniques does not provide an efficient way to deal with privacy of technological healthcare solutions. For example, in response to growing concerns on privacy and data security, in 2014, the European Commission published a Green Paper on mHealth (European Commission, 2014b). Through wide stakeholder consultation, the paper discusses the main barriers and issues related to mHealth deployment. They highlight a number of key topics including data protection, security of health data, informed consent, big data management, patient safety and transparency of information across the EU and, ultimately, on the need to regulate mHealth applications. The rationale of this work was to uncover the main issues which hamper the uptake of mHealth solutions. However, it is worth noting that the Commission acknowledges that many of the healthcare technology issues, such as with mHealth, are within the competence of national rather than EU law. The Green Paper provides an overview of best practice and ideas which can help to stimulate mHealth innovation (European Commission, 2014a, 2014b). In addition, within the report, the Commission also presents a working document on the EU legal framework on mobile apps (European Commission, 2014a). In summary, the report highlights that apps and other mHealth solutions installed and/or used in the EU should comply with the Data Protection Directive (Directive 95/46/EC) and the e-privacy Directive (Directive 2002/58/EC), regardless of the location of the developer or store from which they were obtained. Similar efforts have been exerted by the FDA. For example, back in 2013, the FDA drew our attention towards various stakeholders, including medical device manufacturers, hospitals, medical device user facilities and other relevant users, and explained that they should have specific safeguards in place to reduce the risk of cyber-attacks (FDA, 2013a, 2013b). The FDA explain that device manufacturers are responsible for being vigilant about identifying risks associated with their medical devices to improve patient safety and device performance. In summary, this highlights that regulation is a growing concern on a global scale, particularly in technological healthcare innovation, and becomes a core focus for organisations now operating in the field of connected heath. To support organisations, this research identifies the key regulatory guidance which Connected Health practitioners must be aware of; it also highlights the need for a regulatory intelligence system.

3. Research objective and approach

We examined how Connected Health encompasses terms such as wireless, digital, electronic, mobile and tele-health and refers to a conceptual model for health management where devices, services or interventions are designed around the patient's needs. Considering the broad and emerging nature of Connected Health, demystifying

the regulatory environment to identify which regulations apply to Connected Health technologies is a complex task. Our experience with healthcare companies in Ireland informs us that the introduction of regulation to the development process potentially has a major impact on healthcare companies' ability to innovate new healthcare solutions. Often burdened by the uncertainty associated with healthcare technology regulation, companies typically have to invest significant resources to assess their compliance with regulatory developments, re-strategise their core business focus to avoid regulation constraints or redesign healthcare innovations to address different healthcare needs. Thus, there is an apparent lack of insight on what this regulatory landscape "looks like" and how companies can potentially use regulation as the "rules of the game" to guide healthcare innovations. To address this gap, we formulate the following research question:

RQ1. What are the key regulatory standards which guide the provision of Connected Health solutions?

To explore this question, we undertook a literature review with a particular emphasis on medical devices and SaaMD literature, for example EU Commission, FDA, Irish Medical Devices Association (IMDA), Regulatory Affairs Professionals Society (RAPS), National Standards Authority of Ireland (NSAI) and academic publications. As part of our research developments within ARCH – the Applied Research for Connected Health Technology centre – we undertook a consultation process with key stakeholders of four Connected Health companies and four academic experts to provide feedback of the results of this research. The consultation process was executed twice with all groups to finalise the presentation of the research to support companies and researchers with a clearer understanding of the Connected Health regulatory environment. A presentation on the Connected Health regulation landscape was also given to 40 industry members and feedback was provided.

4. Do I have a medical device?

A common question amongst Connected Health practitioners is "do I have a medical device?" In a general sense, a medical device implies that a solution can support good or improved health. The World Health Organisation refers to good health as "adding years to life". The maintenance of wellness can enable people to live longer and more fulfilled lives. This is largely due to medical technology innovation which enhances health, quality of care and, ultimately, quality of life. There are governing bodies such as the European Commission (EC) and the FDA to ensure the safety of citizens and enforce regulatory obligations on manufacturers of medical devices so that they are safe and fit for their intended purpose. Regulations provide an instrument to protect against risk. This is particularly important in the context of medical devices and in the context of SaaMD. According to the FDA, a medical device is (emphasis added):

> […] an instrument, apparatus, implement, *machine*, contrivance, implant, in vitro reagent, or other similar or related article, *including a component part*, or accessory which is:
>
> Intended for the use in the *diagnosis* of disease or other conditions, or in the *cure, migration, treatment*, or *prevention* of disease, in man or other animals, or

> Intended to affect the structure of any function of the body of man or other animals, and *which does not achieve any of it's primary intended purposes through chemical action* within or on the body of man or other animals and which is not dependent upon being metabolized for their achievement of any of its primary intended purposes".

Medical device software as described within the Medical Device Directive (EU directive 2007/47/EC, European Union Council, 2007/EU directive 93/42/EEC, European Union Council, 1993) is defined as (emphasis added):

> […] any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, *including the software* intended by its manufacturer to be used specifically *for diagnostic and/or therapeutic purposes and* necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:
>
> - diagnosis, prevention, monitoring, treatment or alleviation of disease;
> - diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
> - investigation, replacement or modification of the anatomy or of a physiological process; and
> - control of conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means."

Therefore, the intended use statement is important, as it determines the usage and classification of a product and the regulation associated with it, for example "in vitro diagnostic medical device" implies it may be any medical device. A "medical device" refers to any instrument, apparatus, appliance or software. Therefore, software can be classed as an in vitro diagnostic medical device. SaaMD must be regulated to reduce the risk of harm on people's health. The main stakeholders who support the development and implementation of medical device regulations include Component Authorities (e.g. Health Products Regulatory Authority), Notified Bodies (conformity assessment of medical devices in Europe) and the manufacturers of devices. Manufacturers demonstrate this assurance through compliance with internationally recognised standards, for example the conformité européenne (CE) mark. Such standards indicate that high quality standards are met and information can be shared within a common context through standards. As many devices now increasingly rely on software capabilities to deliver various medical functionalities, various software and medical device guidelines, standards and directives influence the development of Connected Health solutions. Many of these terms are used interchangeably and to clarify:

- guidelines provide assistance in implementing standards;
- standards demonstrate compliance with directives; and
- directives are derived from legislation.

Two key concepts which are often used in discussions regarding regulatory developments are "regulations" and "directives". A regulation is a binding legislative act which must be applied in its entirety, for example across the EU. A directive is a legislative act that sets out a goal that all countries must achieve, for example, within the

EU. However, it is for individual countries to decide how, for example using national law. The current Medical Device Regulatory Framework comprises three primary European medical device Directives and related Statutory Instruments (an order, regulation, rule, scheme or bye-law made in exercise of a power), outlined in Table I.

In recent times, there are continued efforts to move towards a revised Medical Device Regulatory Framework using two directives rather than three (Table II). Narrowing the various sources of regulatory information is important from a software industry perspective. We have identified that software may be regarded as a medical device and specifically when one or more of the following circumstances apply:

- the software is for the purpose explicitly mentioned in a Medical Device Directive, that is software within an in vitro diagnostic medical device;
- software intended to control or influence the functioning of a medical device; and
- software intended for the analysis of patient data generated by a medical device with a view to diagnosing and monitoring.

Organisations developing Connected Health technologies must clearly state the "intended use" of the medical device innovation before they can begin to identify and assess its conformity with associated regulations. In addition, there is a regulatory expectation for software which is outlined in the Council Directive 2007/47/EC that:

> For devices which incorporate software or which are medical software in themselves, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification.

By state-of-the-art for medical device software development, this Directive is referring to IEC 62304 and aligned standards (i.e. ISO 13485, ISO 14971 and IEC 60601-1). We will examine individual software-related standards in more detail throughout this article (see Section 5). The intended use of a medical device focuses around a technology's innovation. Therefore, transitioning from a feasibility study to a product development phase requires some informed decision-making on a "go/no go" outcome based on a feasibility study (what is my technology?), product development (life cycle) (how will I

Table I.
Medical device regulatory framework

Device	Directive	Statutory instrument
General medical devices	93/45/EEC	S.I. No. 252 of 1994
In vitro diagnostic medical devices	98/79/EEC	S.I. No. 304 of 2001
Active implantable medical devices	90/385/EEC	S.I. No. 253 of 1994

Table II.
Proposed revisions to medical device regulatory framework

Device	Regulation
General medical devices + active implantable medical devices	A proposal for regulations on medical devices (to replace: Directive 90/385/EEC regarding active implantable medical devices and Directive 93/42/EEC regarding medical devices)
In vitro diagnostic medical devices	A proposal for a regulation on *in vitro* diagnostic medical devices (to replace Directive 98/79/EC regarding in vitro diagnostic medical devices)

develop the medical device?) and market launch (what is my target market?). This highlights the importance of regulating medical device software to ensure its safety and the development integrity of the software development processes. Software within a medical device may be also classified as standalone. Standalone software is software which drives or influences medical device functionality. According to the implementing rules of Annex IX of 93/42/EEC, "software, which drives a device or influences the use of a device, falls automatically in the same class". Standalone software is guided by Directive 2007/47/EC, which amended the definition of a medical device:

> […] software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes (diagnostic and/or therapeutic) set out in the definition of a medical device, is a medical device.

MedDev 2.1/6 defines standalone software as software which is not incorporated in a medical device at the time of its placement in the market or it being made available. This Directive defines the criteria for the qualification of standalone software, when used in healthcare settings, as a medical device and the application of the classification criteria to such software. Figure 2 presents a decision diagram which assists how we qualify software as a medical device.

Software of unknown provenance (SOUP) is software that has not been developed with a known software development process or methodology or which has unknown or no safety-related properties. Examples of SOUP include:

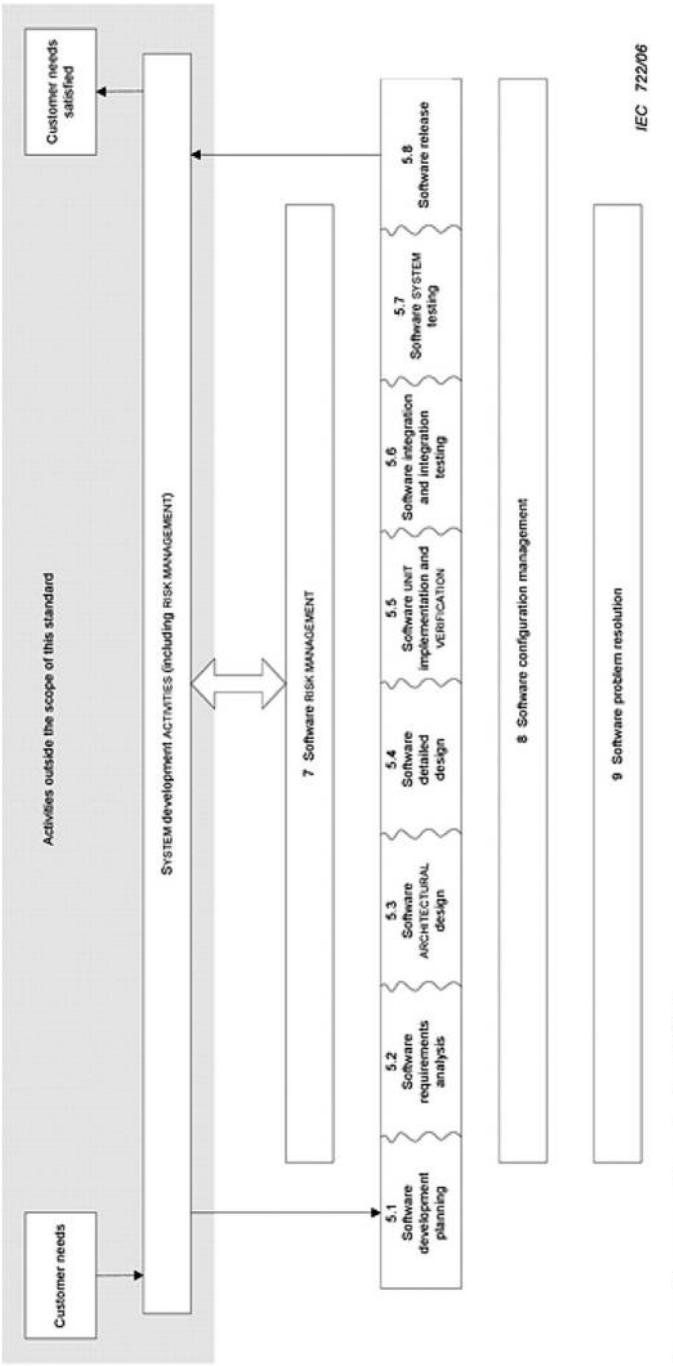
- commercial off-the-shelf (OTS) software;
- public domain software; and
- legacy software components with limited information on development process or inadequate process.

These are often referred to as OTS or commercial off-the-shelf software (COTS) in other standards. SOUP validation is very important (and time-consuming) particularly in a Connected Health context, as it is a growing field which needs regulatory guidance support.

5. What classification of medical device do I have?

Having determined whether you have a medical device or a health wellness solution can be a difficult task. Yet, this is critical to classify what a healthcare technology is, as it will also determine which regulations are associated with it. Healthcare technologies are classified into classes, depending on their intended use and the associated risk to humans. The classification based on perceived risk is influenced by:

- pre-market requirements;
- reusable versus single-use product;
- duration of contact with a user;
- active versus non-active (active medical device relies on its functioning on a source of electrical energy or any source of power other than directly generated by the human body or gravity);
- degree of invasiveness; and
- part of body affected.



Source: European Commission (2012)

Figure 2.
A decision diagram to assist qualification of software as medical device: MedDev 2.1/6

The four general medical device classifications range from Class I, IIa, IIb and III. There are four *in vitro* diagnostic medical device classification rules:

(1) General;
(2) Self-test;
(3) Annex II List A; and
(4) Annex II List B.

Medical device software is also classified under IEC 62304. This defines software classification (A, B and C) based on the potential hazards in the case of software failure. A medical device software system is assigned one of the three safety classes according to the possible effect on the patient, operator or other people resulting from a hazard to which the software system can contribute:

- *Class A*: No injury or damage to health is possible.
- *Class B*: Non-serious injury is possible.
- *Class C*: Death or serious injury is possible.

It is worth noting that there is no direct mapping of medical device classification and software safety classification. For example, a company may develop a medical device which is a Class IIB device but operates with a Class A software system. In addition, there are 18 medical device classification rules for general medical devices of which only four apply to software: rules 9, 10, 11 and 12 of Annex IX are applicable. The classification and rules associated with SaaMD also determine the performance requirements or the essential requirements. The essential requirements aim to ensure medical devices are designed, manufactured and used such that unnecessary risks to patients and users are avoided. In addition, there are 13 essential requirements made up of 79 parts covering, design, construction, performance, usability, chemical, physical and biological properties and labelling. These parts support medical device companies to ensure that the device conforms with the essential requirements and to established standards in design and production. There are significant implications of the classification on software development activities in which software plays, ultimately, impacts on the level of concern attached to the software outcomes. This should be indicated in the 510K database(s). The 510K is a pre-market submission made to the FDA to demonstrate that the device to be marketed is at least as safe, effective and substantially equivalent to a legally marketed device. Classification of medical devices within an end-to-end Connected Health system can have peripherals of the system with different medical device classifications. For example, consider a remote monitoring system including personal health devices, mobile phone, mobile applications, cloud-based repository, clinician applications and data analytics applications. All of the components have various individual "intended uses" but now the overall system may offer a healthcare monitoring service as its primary solution, thus changing the intention of use.

6. Medical device software standards

Considering that medical software solutions may contain vital information and directions, for example patient medication dosages, regulation plays a vital role in governing the software lifecycle in bringing software products and services to

international markets. For example, medical device companies who market their products in the USA must ensure that they comply with medical device regulations as governed by the FDA (McCaffery *et al.*, 2010). Similarly, medical devices intended for use within the EU must have achieved a CE conformance mark. Due to the growing reliance on software to provide medical device solutions, medical diagnosis and medical treatments, regulation is required to ensure improved safety (McHugh *et al.*, 2011). To summarise, we present a checklist which attempts to summarise and categorise the key regulations associated with medical devices and Connected Health field (Tables III-VIII). We categorise these as follows:

- Regulations Guiding Performance and Product Standards;
- Regulations Guiding Development Standards;
- Regulations Guiding Quality Systems;
- Regulations Guiding Patient-Reported Outcome (PRO) Regulations;
- Regulations Guiding Ethics Standards; and
- Regulations Guiding Systems and Interoperability and Data Standards.

Tables III-VIII provide an overview of the various regulations and standards associated with medical devices which also impacts on software development processes. While these regulations offer us a checklist to support software development for the Connected Health market, it is also important to consider wider legislations guidance, for example data protection and from a technical viewpoint, and other software development practices to align regulations which are regularly updated.

6.1 From ISO/IEC 15504 to ISO/IEC 33001:2015

It is important to tailor a project to develop a Connected Health solution by identifying and mapping regulations through a tiering process to operate a lean approach to SaaMD. In essence, there ought to be a process to support organsiations to align various starndards and regulations with healthcare innovations. For example, establishing a regulations intelligence framework could support this process to enable software developers and manufacturers to become more aware of regulations and regulatory updates by monitoring sources (e.g. FDA, EU Commission, IMDA, NSAI and academies developments). Such updates could feed into an organisations innovation design and development strategy. However, while this may be a complex undertaking, there are some efforts to guide organisations through software development processes. For example, one approach to improving software process which is widely implemented and regulated by the ISO and the IEC is ISO/IEC 15504 and ISO/IEC 15504 comprising a guide to assess software development projects and has recently been replaced by ISO/IEC 33001:2015. It includes a description of this assessment process, a model for performing an assessment, a description of tools that may be used as part of the assessment process and a discussion of factors that contribute to the success of such an assessment. The standard seeks to describe the preferred order in which activities should occur in a software development project, with particular emphasis on an organisation's management and process definition structures and with a goal of achieving process improvement. ISO/IEC 33063:2015 defines the process assessment model which addresses the requirements of ISO/IEC 33004. This also supports the performance of an assessment of process capability using the process measurement

Table III.
Regulations guiding performance and product standards

Focus	Associated standard	Short description
Requirements and information	IVDD 1998/79/EC – In vitro diagnostic medical devices directive	In vitro diagnostic directive which governs the sale of medical devices
	IEC/CD 82304-1 – Health software – Part 1: General requirements for product safety	Health software standard on product safety: under development
	EN60601-1: 2006 (safety and effectiveness of medical electrical equipment)	Series of technical standards for the safety, requirements and effectiveness of medical electrical equipment. This is a harmonised standard under the Medical Devices Directive 93/42/EEC. This means that compliance with ISO 60601-1: 2006 now provides a presumption of conformity with the MDD
	AIMD 1990/385/EEC – The Council Directive 90/385/EEC on active implantable medical devices	Giving patients, users and other persons a high level of protection and achieve the intended level of performance when implanted in human beings
	EN60601-1-2: 2007 (safety and essential performance)	General requirements for basic safety and essential performance of medical electrical equipment
	EN 22248:1993 (vertical impact by dropping transport packages and impact test)	Complete, filled transport packages. Method for determination of resistance to vertical impact by dropping
	EN ISO 15223-1 (medical device labelling)	Identifies requirements for symbols used in medical device labelling that convey information on the safe and effective use of medical devices
	EN1041:2008 (information supplied by the manufacturer of medical devices)	Describes requirements for information to be supplied by the manufacturer of medical devices
	IS EN 50419:2005 (marking of electrical and electronic equipment)	Marking of electrical and electronic equipment in accordance with article 11(2) of Directive 2002/96/EC Waste Electrical and Electronic Equipment Directive (WEEE). This sets out collection, recycling and recovery targets for all types of electrical goods
	IEC 61508 – Functional safety electrical/electronic/programmable electronic safety-related systems	An international standard of rules applied in industry. It is titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE or E/E/PES)
	IEC 62366:2007: Medical devices – Application of usability engineering to medical devices	Process for a manufacturer to analyse, specify, design, verify and validate usability, as it relates to safety of a medical device. This usability engineering process assesses and mitigates risks caused by usability problems associated with correct use and use errors, i.e. normal use
	IEC 60601-1-11:2010 – 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	Basic safety and essential performance of medical electrical equipment and medical electrical systems Requirements of the general standard IEC 60601-1:2005 and to serve as the basis for particular standards

Table IV.
Regulations guiding development standards

Focus	Associated standard	Short description
Risk management, software development and security	ISO 14971:2007 – Medical devices – Application of risk management to medical devices	Process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks and to monitor the effectiveness of the controls
	ISO/IEC 15504-5:2012: revised by ISO/IEC 33001: 2015 Information technology – Process assessment – Concepts and terminology	A set of technical standards documents for the computer software development process and related business management functions
	IEC/TR 80002-1:2009 – Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software	Provides guidance for the application of the requirements contained in ISO 14971:2007, Medical devices – Application of risk management to medical devices to medical device software with reference to IEC 62304:2006, Medical device software – Software life cycle processes Aimed at risk management practitioners who need to perform risk management when software is included in the medical device/system and at software engineers who need to understand how to fulfil the requirements for risk management addressed in ISO 14971
	ISO 14971:2012 (risk management to medical devices)	The application of risk management to medical devices and examines how risk/benefit is assessed and how medical devices are designed
	ANSI/AAMI/IEC 62304:2006 – medical device software – software life cycle processes	Medical device software – Software life cycle processes. Specifies life cycle requirements for the development of medical software and software within medical devices. The set of processes, activities and tasks described in this standard establishes a common framework for medical device software life cycle processes
	IEC TR 80002-1: 2009 (Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software)	Provides guidance for the application of the requirements contained in ISO 14971:2007, Medical devices – Application of risk management to medical devices to medical device software with reference to IEC 62304:2006, Medical device software – Software life cycle processes
	IEEE 829.1998 (IEEE Standard for Software Test Documentation)	An IEEE standard that specifies the form of a set of documents for use in eight defined stages of software testing and system testing, each stage potentially producing its own separate type of document
	GAMP/GAMP 5 (guidance to achieve compliant computerised systems fit for intended use)	A set of guidelines for manufacturers and users of automated systems in the pharmaceutical industry. Provides a guide for validation of automated systems. GAMP 5 provides pragmatic and practical industry guidance to achieve compliant computerised systems fit for intended use in an efficient and effective manner

(*continued*)

Table IV.

Focus	Associated standard	Short description
	Software Systems Guidance	General principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002. Provisions of the medical device quality system regulation apply to software and the agency's current approach to evaluating a software validation system Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 11, 2005. This provides information to industry regarding the documentation that is recommend to include in premarket submissions for software devices, including stand-alone software applications and hardware-based devices that incorporate software Guidance for Industry- 21 CFR Part 11, Electronic Records; Electronic Signatures – Scope and Application. Defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records Guidance for Industry – Computerized Systems Used in Clinical Investigations. Provides recommendations regarding the use of computerised systems in clinical investigations. The computerised system applies to records in electronic form that are used to create, modify, maintain, archive, retrieve or transmit clinical data required to be maintained or submitted to the FDA Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices. Describes the information that generally should be provided in a medical device application involving OTS software. This information is in addition to the documentation described in the Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices FDA 21 CFR 880 Subpart G, Sec: 880:6310, Medical Device Data Systems. Describes General Hospital and Personal Use Miscellaneous Devices Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, Jan 14, 2005. Outlines general principles that is considered to be applicable to software maintenance actions required to address cybersecurity vulnerabilities for networked medical devices – specifically, those that incorporate OTS software
	FDA draft guidance	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and FDA Staff, June 14, 2013. Provides recommendations to consider and information to include in FD medical device premarket submissions for effective cyber-security management. Effective cybersecurity management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity

Table V.
Regulations guiding quality systems

Focus	Associated standard	Short description
Design, manufacturing and distribution of connected health devices	2007/47/EEC – Directive 2007/47/EC of The European Parliament and of the council	Intended to harmonise the laws relating to medical devices within the EU. The MD Directive is a "New Approach" Directive and consequently in order for a manufacturer to legally place a medical device on the European market the requirements of the MD Directive have to be met
	ISO13485: 2003 QMS for Medical Devices – Quality management systems – Requirements for regulatory purposes	Specifies requirements for a quality management system. Organisation needs to demonstrate ability to meet customer requirements and regulatory requirements
	21 CFR 820 and 803 FDA Quality System Regulations	Current Good Manufacturing Practice (CGMP) that govern the methods, the design, manufacture, packaging, labelling, storage, installation and serving of all finished devices intended for human use
	93/42/EEC – European Medical Devices Directive (MDD)	Mandatory Directive for medical devices for manufacturers to be awarded the CE mark for the European market
	JPAL MHLW Ministerial Ordinance No.169-2004	JPAL (the Japanese equivalent to the FDA).These are standards for Manufacturing Control and Quality Control for Medical Devices and In-Vitro Diagnostic Reagents
	Canadian Medical device Regulation CMDR. SOR/98-282	Support ISO 13485 which are assessed by Notified Bodies under a review audit known as CMDCAS (Canadian Medical Device Conformity Assessment System)
	FDA Pre-market Approval (PMA)	FDA PMA of scientific and regulatory review to evaluate the safety and effectiveness of medical devices
	CE Mark	A mandatory conformity marking for certain products sold within the European Economic Area (EEA) to indicate a product's compliance with EU legislation and so enables the free movement of products within the European market
Clinical project management, customer support and connected health device service	International Conference on Harmonisation and Good Clinical Practice (ICH GCP)	Unified standard for the EU, Japan and the USA to facilitate the mutual acceptance of clinical data. Provides a quality standard for designing, conducting, recording and reporting trials that involve the participation of human subjects
	ISO13485: 2003 QMS for Medical Devices	Specifies requirements for a quality management system. Organisation needs to demonstrate ability to meet customer requirements and regulatory requirements
	ISO9001:2008 – Quality management systems – Requirements	Specifies requirements for a quality management system where an organisation product must meet customer and applicable statutory and regulatory requirements
	2005/28/EC – GCP Directive	Principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products

Table VI. Regulations guiding patient-reported outcome (PRO) regulations

Focus	Associated standard	Short description
FDA guidance	Guidance for industry Patient-reported outcome measures: use in medical product development to support labelling claims	Used to support claims in approved medical product labelling. A PRO instrument (i.e., a questionnaire, information and documentation) captures data used to measure treatment benefit or risk in medical product clinical trials
	Guidance for industry Part 11, Electronic Records; Electronic Signatures – Scope and Application	Provides guidance to persons who, fulfils requirement of FDAs regulations to maintain records or submit information, chosen to maintain the records or submit designated information electronically
	Guidance for industry computerised systems used in clinical investigations	Recommendations regarding the use of computerised systems in clinical investigations. The computerised system applies to records in electronic form that are used to create, modify, maintain, archive, retrieve or transmit clinical data required to be maintained or submitted to the FDA
	Guidance for industry electronic source data in clinical investigations	Provides recommendations on the capture, review and retention of electronic source data in FDA-regulated clinical investigations to ensure the reliability, quality, integrity and traceability of data from electronic source to electronic regulatory submission
	General principles of software validation; final guidance for industry and FDA staff	Outlines general validation principles that the FDA considers to be applicable to the validation of medical device software or the validation of software used to design, develop or manufacture medical devices
	Guidance for industry, FDA reviewers and compliance on OTS software use in medical devices	Describes the information that generally should be provided in a medical device application involving OTS software. This information is in addition to the documentation described in the "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices"
	Mobile medical applications guidance for industry and FDA staff	Informs manufacturers, distributors and other entities about how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms (mobile applications or "mobile apps")
	Guidance for industry E6 GCP: consolidated guidance	This ICH guidance provides a unified standard for the EU, Japan and the USA to facilitate the mutual acceptance of clinical data by the regulatory authorities in those jurisdictions
The European Medicines Agency (EMA)	Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials	Collection of accurate clinical trial data is essential for compliance with GCP (CPMP/ICH/GCP/135/95). This presents the opinion of the EU GCP Inspectors Working Group on the use of electronic data capture in clinical trials and on related inspections
	Reflection paper on the regulatory guidance for the use of health-related quality of life (HRQL) measures in the evaluation of medicinal products	Reflection paper discusses the place that a HRQL, a specific type of PRO, may have in drug evaluation process and to give some broad recommendations on its use in the context of already existing guidance documents

framework defined in ISO/IEC 33020. This standard was updated in March 2015 and highlights the dynamic nature of regulations and how they can impact on Connected Health innovation.

6.2 MedDev

MedDevs are guidelines aimed at promoting a common approach by manufacturers and notified bodies involved in the conformity assessment procedures according to the relevant annexes of the Directives[2] and by the competent authorities charged with safeguarding public health. The guidelines apply to member states to ensure uniform application of relevant Directive provisions. MedDev2.1/6 also presents six key steps for the qualification criteria across general medical devices (Table IX) and In Vitro diagnostic medical devices (Table X). In the case whereby a product is considered as an active medical device, rules 9, 10, 11 and 12 of Annex IX to Directive 93/42/EEC can apply. Clause 2.3 of the implementing rules in Annex IX states that software which drives a medical device or influences the use of a device, falls automatically into the same class as the device it drives. Within MedDev2.1/6, there are also modules. Modules may be described as computer systems used in healthcare settings which may consist of both medical device and non-medical device modules. Only the modules which have a medical purpose require CE marking, not the whole system (discussed further in Section 6).

Table VII.
Regulations guiding ethics standards

Focus	Associated standard	Short description
Code of ethics	EUCOMED	Provides guidance on the interactions of EDMA members with individuals or entities that purchase, lease, recommend, use, arrange for the purchase or lease of or prescribe members' IVD medical devices ("Health Care Professionals") in Europe and, generally, elsewhere

Table VIII.
Regulations guiding systems and interoperability and data standards

Focus	Associated standard	Short description
Data management	GDT Protocol [Geräte-Daten-Träger (Device Data Carrier)] – Connecting medical measuring instruments	Interface description has been compiled by QMS (Qualitätsring Medizinische Software) to define a standardised interface between electronic Data Processing Systems in Surgeries and medical measuring instruments. The interface GDT is therefore designed to be device-manufacturer
	95/46/EC Data Protection Directive	The protection of individuals with regard to the processing of personal data and on the free movement of such data
	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules	Strengthen the privacy and security protections for health information

Step	Criteria
1	Must be considered to be a computer program as per ISO/IEC 2382-1:1993 (Part 1: Fundamental terms). Digital document (e.g. image files) not medical devices
2	Must not be considered as an integral part of an existing medical device
3	Must perform an action on data, for example create or modify medical information Storage, archival, communication, simple search and compression is not considered a medical device
4	Must be for the benefit of individual patients, that is support/influence medical care Generic treatment pathways, medical atlas and population aggregation are not considered a medical device
5	Must have a medical purpose as per definition of medical device (Article 1(2)a)
6	Accessory to medical device and/or software made available over the Internet (direct/download) are also subject to MDD

Table IX.
Qualification criteria across general medical devices

Step	Criteria
1	Fulfil definition of a medical device
2	Must have an expert function, that is analyse existing information to generate new specific information within the scope of the IVD directive
3	Data obtained from IVD devices only using software is considered in vitro diagnostic Data obtained from vitro diagnostic device and general medical devices where derived information under vitro diagnostic device using software is considered a vitro diagnostic medical device
4	Must be for the benefit of individual patients, that is support/influence medical care Generic treatment pathways, medical atlas and population aggregation are not considered a medical device

Table X.
Qualification criteria across in vitro diagnostic medical devices

7. Clinical investigation

Standards harmonise the technical specifications to meet essential requirements to enforce conformity at an international level. Standards may be broadly categorised as vertical (specific to a medical device) or horizontal (common across a range of devices). From a software perspective, the EN 62,304:2006 – Medical Device Software – Software Life-Cycle Processes provides horizontal specifications which prescribe the conformity of software development processes. In addition, all medical devices require an assessment of clinical data or otherwise known as clinical evaluation (Class I, IIa, III and AIMD). Clinical evaluation should be assessed on a number of different levels including a medical device's:

- *Intended use*: The clinical condition being treated, the severity and stage of disease, the site of application to/in the body and the patient population.
- *Technical characteristics*: The design, specification, physiochemical properties including energy intensity, development methods, critical performance requirements, principles of operations and conditions of use.
- *Biological characteristics*: The biocompatibility of materials in contact with the same body fluids/tissues.

Clinical investigations are systematic in or on one or more human subjects, undertaken to assess the safety and/or performance of a medical device. A "clinical trial" or "clinical study" is synonymous with clinical investigations. Clinical investigations should not be undertaken unless it is justified to rely on existing clinical data (for active implantable, implantable and Class III medical devices). Clinical investigations should be undertaken in-line with the harmonised standard ISO 14155:2011. There are two main Directives associated with clinical investigations (Table XI).

There are a number of studies and ethical considerations which companies should examine to undertake a clinical investigation. There are some circumstances whereby a clinical investigation is not required. For example, in a case whereby clinical or academic research with no regulatory purpose or whereby post-market studies carried out within the scope of the existing CE mark, a clinical investigation is not required. It is worth noting that both the competent authority and the ethics committee approval are required before commencing a clinical investigation.

8. Conformity assessment and CE marking

Conformity assessment is the procedure to which a company assesses whether a medical device meets the applicable requirements of the Directive. These differ depending on the classification of the medical device, for example general medical device (GMD), including in vitro diagnostic (IVD) or active implantable medical devices (AIMD). The technical file or design dossier to support the conformity assessment process provides details on the medical device including:

- product description and intended use;
- design specification and drawings;
- essential requirements and standards;
- labelling and instruction for use;
- pre-clinical evaluation; and
- clinical evaluation.

The technical details are typically managed using a Quality Management System (QMS) as outlined in EN ISO 13,485. Securing a CE mark is a quality approval sign which indicates conformance with the essential requirements of the appropriate Directive. It enables the free movement of products, such as medical devices, within the EEA without specific further control (unless there is a safety issue). It offers companies between three and five years of validity for their products. This highlights the importance of having a QMS in place to support and monitor these processes to achieve a CE mark and comply with software development and manufacturing regulations. The Conformity Assessment and CE Marking are set out in ISO 13,485 – Quality Management System. According to ISO 13485 (based on ISO 9001:1994), a QMS must have the ability to

Table XI.
Clinical investigation directives

Directive	Clinical investigation	Statement concerning devices for special purpose	Clinical evaluation
93/42/EEC	Art. 15	Annex VIII	Annex X
90/385/EEC	Art. 10	Annex 6	Annex 7

provide medical devices and related services that consistently meet customer requirements and regulatory requirements applicable to medical devices and related services. These must also link to Directives with reference to "harmonised standards" as a means of meeting requirements rather than a description of specific standards listed in the Directive (e.g. EN ISO 13,485:2003).

9. Quality management system

For medical device software development, companies must become aware of the need to implement practice or procedures using a QMS to enable compliance. This can be achieved using a Design Control Standard Operating Procedure (or Design Control SOP) which offers a best fit to an organisation. In addition, this enables companies to easily align standard compliance with medical device audits. Design Control SOP provides companies with a structured development by guiding the design efforts through well-defined input and output phases. To ensure compliance with regulatory agencies (for example FDA, EMEA, ISO and similar regulatory groups), it is imperative that a company uses SOP software for managing various document control, change control and employee training processes. The Design Control SOP should provide details of regulatory requirements. An SOP is also used to support software developments to maximise efficiency and safety. Within the regulatory environment, it is important to maintain and update appropriate and effective management of SOPs. SOP software can support companies in the form of document control and management, change control and employee training. Such a management structure enables a company to ensure they are compliant with regulatory requirements and supports them to meet their goals faster (including safety compliance) and saving them both time and money by reducing waste or process inefficiency (i.e. a lean approach to regulatory requirements and software processes).

10. Software issues and potential threats

Innovation in Connected Health and medical devices is becoming increasingly software-led through various feature-enriched capabilities. Medical devices can now be standalone softwares. In more recent years, due to software capabilities, medical devices are becoming increasingly networked. While networking medical devices may be a welcome evolution of Connected Health innovation, it does add greater complexity and concerns around regulations. One of the main concerns across industry is the lack of a unified framework which can incorporate all of the best practices for medical device software development. In addition, traditionally, personnel who are responsible for the qualification of medical devices lack software expertise. This is a growing issue because of the growing dependency on software in medical devices and the challenges this presents in terms of quality and regulation compliance; for example, an FDA Medical Device Recall Report. FY2003 to FY2012 report highlights the growing problem associated with software and demonstrates that software failures cause the majority of recalls associated with these devices. According to the *Biomedical Instrumentation Technology Journal* (Simone, 2013) between 2005-2011, approximately 19.4 per cent of medical device recalls were related to software issues. Highlighting the growing threat which software in medical devices now presents to healthcare, this warrants the need to identify how other safety-critical sectors which require software have evolved in recent years, for example automotive, nuclear and space exploration. All of these sectors have

used the IS015504 framework to enable software process assessment (i.e. ISO/IEC 33001: 2015). In addition, considering the increasing use of networked medical devices, this has presented new threats ranging from data protection to cyber security against threats from hackers (Finnegan *et al.*, 2013a, 2013b; Finnegan and McCaffery, 2014).

Organisations face challenges due to regulation requirements. For example, while regulations adopt a risk-adverse stance, they often bring additional research and development costs, slow the time to market and can hamper innovation. One of the many challenges faced by medical device software companies is to understand the current state of the software development processes in relation to the requirements of the medical device regulations (McHugh *et al.*, 2011). To reduce the risk of failure of software used in Connected Health systems, regulatory bodies need to enforce regulations for healthcare software systems and medical device manufacturers (McHugh *et al.*, 2012). While the healthcare industry has made great efforts in reducing the inefficient paper records and adopting new automated patient record system, technology also introduces new problems, for example data being stored on different systems which lacks communication and are incapable of amalgamating data for usage (Halevy, 2011). This challenge is not confined to a single office or organisation, but rather all the information requirements must be integrated to optimise its outcome as a key resource through standardised healthcare structure. However, such challenges also present opportunities for Connected Health organisations. The integration of patient details from patient's record can only be possible if the data are interoperable with national or international structure this permitting linked data access, data privacy and system security. By semantically harmonising the data, it minimises waste in costs and time associated with healthcare services and increases patient safety and service quality (Halevy, 2011).

Similar challenges were faced in a business context where policies such as the Sarbanes-Oxley Act of 2002 (or SOX) were passed as legislation in the USA to protect shareholders and the general public from accounting errors and fraudulent practices and to improve the accuracy of corporate disclosures. In a Connected Health context, we need to uphold specific practice, technological and healthcare regulations to comply with legal obligations and enhance patient care. For example, the American Recovery and Reinvestment Act (ARRA) in the USA identifies the gaps in various rules and regulations which will be beneficial for the development of healthcare, including privacy protection of health information of the users, use of electronic health records for storing and retrieving patient's information, implementing health care information exchange, quality improvement and encryption of information to ensure the privacy and security (Halamka, 2010). However, access to information using web technologies is not an issue *per se*. Rather, access to the correct and/or accurate information is often a challenge for various diagnosis and treatments (Baujard *et al.*, 2010). Perhaps, from a Connected Health perspective, Web resource trust certification presents many opportunities similar to Utilisation Review Accreditation Commission (URAC) or Health On the Net Code of Conduct (HONcode[3]).

11. Connected medical devices: mobile apps

There is a wide variety of actual and potential healthcare functions of mobile software applications (commonly known as "apps"). The rapid growth of mobile apps innovation, coupled with the potential benefits and risks to public health have been well-documented in recent years. The use of mobile devices across the healthcare sector

for various health and wellbeing needs is beginning to transform how we view medical devices and the connectivity they offer between various healthcare stakeholders. Many mobile devices vary in their classification based on the potential risk they pose to our safety. Nevertheless, mobile devices are becoming more common in healthcare settings and have fuelled the growth of mobile medical software applications. Many of these apps support basic tasks such as tracing dietary habits or fitness regimes to supporting medical information and time management; health record maintenance and access; communications and consulting; reference and information gathering; patient management and monitoring; clinical decision-making; and medical education and training. Thus, depending on their intended use, healthcare mobile apps must also comply with medical device and software development regulations. Mobile apps developed may avoid regulatory controls if software applications developed to display medical data are not intended for diagnostic use or treatment. The FDA defines medical device data as "any electronic data that is directly available from a medical device or that was obtained originally from a medical device". There are a number of key processes which must be examined when describing medical device data including:

- *Transmit*: Systems connected directly or indirectly which transmit medical data. This includes a healthcare facility's IT network (refer to IEC 80001-2).
- *Store*: Any device which stores medical device data. Devices include hospital file servers and backup devices.
- *Convert (translate)*: Permitted to convert/translate medical device data but is not allowed to alter the content in any way. An example of such translation is conversion of a DICOM image to JPEG format.
- *Display*: Prior to the ruling, all devices used to display medical device data were considered to be accessories to the parent device or they had to undergo separate classification.

These processes are important in a mobile app context because much of the information exchanged via apps is transmitted, stored, converted and displayed through various means. The apps' intended purpose can become blurred and is often smudged within the app disclaimer which may suggest that an app is for "entertainment purposes" rather than "medical purposes" and thereby attempting to remove the need to comply with medical device regulations. Many companies have removed some feature-enriched capabilities from mobile devices and apps as a result such compliance issues. For example, Apple has removed sensors for health applications. However, Android is not as stringently regulated as Apple with apps that can be distributed on Google Play. The FDA identifies the need to clarify their regulatory stance on health-tracking wearables such as the smart watches. This also includes apps for similar consideration as medical device data system (MDDS). The FDA describes an MDDS as:

> […] hardware or software products that transfer, store, convert formats, and display medical device data. An MDDS does not modify the data or modify the display of the data, and it does not by itself control the functions or parameters of any other medical device. MDDS are not intended to be used for active patient monitoring.

The quality and performance of MDDS are critical to the safety and delivery of health care. Any potential defects in terms of quality and design, performance or functionality of MDDS can have drastic consequences on public health and safety. However, not all

medical-related software used are considered as MDDS. The device capabilities and software functionalities indicate whether or not specific software should be considered an MDDS (McHugh *et al.*, 2011). Thus, software is one of the most complex elements of a medical device. Regulations enable the development of safety-critical software-based systems in a disciplined and cost-effective way. Connected Health may also learn from good practice, such as that from developments in "bring your own device" (BYOD). BOYD has become increasingly acceptable across the world as the use of mobile devices continues to rise which may have consequences for healthcare practice. While this is a welcomed development in terms of enhancing the connectivity of various healthcare stakeholders, it does pose some potential downfalls, most notably in terms of privacy of patient care. According to the FDA (2015), it is estimated that there will be 500 million smartphone users worldwide using a healthcare application. They explain that by 2018, 50 per cent of the more than 3.4 billion smartphone and tablet users will have downloaded some form of mobile medical- or health-related applications. However, one of the key issues is that while various applications can be downloaded on BOYD, many may not be fully equipped with sufficient levels of protection to monitor and analyse third-party apps or their potential impact on patient care. As Connected Health solutions generally combine a number of medical devices, patient care in this context needs to be considered. This will present opportunities for Connected Health research and development in terms of regulation, standards and software development.

12. Need for regulatory intelligence system

As this research demonstrates, managing regulatory compliance within the medical device and Connected Health sector is a complex task. The rapid growth of technological and software development innovation to deliver innovative healthcare solutions makes it even more challenging to align regulation and technology conformity assessment practices and processes. However, managing current regulatory development is only part of the complete picture, as companies must also keep abreast of current and future regulatory developments which are continuously on-going. Organisations must be assured that they are informed of latest regulatory developments and that their operations (e.g. manufacturing and software development practices) are compliant with new and/or revised regulations. For example, in 2015 (between January and February) there have been a number of additions to the latest FDA guidance including:

- 2015-01-19 FDA publish draft guidance on "general wellness" devices;
- 2015-01-19 FDA publish draft guidance on regulation of medical device accessories;
- 2015-01-20 General Wellness: Policy for Low Risk Devices (draft);
- 2015-01-27 EU update list of harmonized standards;
- 2015-02-03 IEC/FDIS 62366-1 released;
- 2015-02-09 Mobile Medical Applications (Issued);
- 2015-02-09 Medical device data systems, medical image storage devices and medical image communication devices (issued); and
- 2015-02-09 FDA publish final medical device data system (MDDS) guidance.

Within a short timeframe (i.e. Juanary to Febuary), this highlights only some of the key medical device changes. This also indicated that there is a need to be aware of what regulatory changes are in the pipeline and potential implications and require a system to monitor multiple sources, for example EU Commission, FDA or academic developments. From a software perspective, there has been a newly proposed device regulation within the Essential Requirements Annex I §14, which is a specific section for software incorporated in devices and standalone software. We propose that such development in regulatory guidance warrants the need to introduce regulatory intelligence systems which will support organisations to make informed decisions about innovative Connected Health and medical device innovations, identify the pros and cons associated with various feature-enriched capabilities and overall, create a greater awareness of latest developments across the regulatory landscape to support software development in a Connected Health context.

13. Usability and connectedness

The FDA has put considerable efforts in requiring human factors/usability testing of medical devices. Human factors engineering embraces a wide spectrum of domains based on research, scientific method, statistics, human physiology and cognitive information processing. It is the combination of engineering, human physiology, behavioural performance and cognitive science. In a Connected Health context, it enables companies to examine how humans interact with devices, products and/or systems. Therefore, it encourages software engineers to design with the user/patient as the focal point. Within a Connected Health context, usability engineering plays a core role in medical devices which offer patients more pervasive healthcare technology solutions. From a regulatory perspective, companies are guided by IEC 62366:2007 which focuses on the application of usability engineering to medical devices. This specifies a process to analyse, specify, design, verify and validate usability relating to safety of a medical device. In essence, the IEC 62366:2007 assesses and mitigates risks caused by usability problems associated with correct use and use errors, that is "normal use", and identifies risks associated with abnormal use. Thus, IEC 62366:2007 has significant impact on software development. It does not, however, offer a guide on how to assess or mitigate risks associated with abnormal use. When a company complies with this standard in terms of usability validation, the residual risks, as defined in ISO 14971, associated with usability of a medical device are presumed to be acceptable. It is worth noting that IEC 62366:2007 does not apply to clinical decision-making relating to the use of a medical device. Therefore, it is important to promote a clear understanding of how best to optimise software processes to develop Connected Health solutions. Formative testing uses a prototype of the device to assess users' interactions and use of the product. It is centred in the development lifecycle to align the actual model of human interaction with the ultimate design of the device or system. The summative test is considered to be the final test which results in a pass/fail judgment on a device. The test should be designed to validate the device to be safe, effective and usable by all the intended user groups which are being launched in the market. Design validation should be focused on ensuring successful mitigation of critical use failures that can be attributed to the device, those that can lead to unacceptable patient harm which would be identified through a risk-management process and formative human factors testing. Use risks must be mitigated to an acceptable level. Therefore, data collection and

assessment are key processes to examine compliance with human factors and identify potential issues associated with usability through a use-based risk analysis testing strategy.

14. Discussion and conclusion

This research presents an overview of regulations associated with the medical device sector to inform Connected Health practitioners on relevant regulatory guidance. It identifies the importance of European and international standards and regulations. The concept of improved connectivity is a welcomed shift in healthcare, but it does not just support greater efficiency; it transforms how we do things and even what can be done, how we exploit smart grids and Connected Health using embedded sensor networks. Improved technology is enabling innovative collaboration and new types of partnerships, particularly between healthcare providers, governments and citizens. However, this can bring about both benefits and potential threats, social and economic alike, and regulations play a central role to ensure safe and quality care continues to be the primary objective of Connected Health and requires new evaluation approaches (Carroll *et al.*, 2016; O'Leary *et al.*, 2015).

Within a Connected Health environment, individuals are equally responsible as the healthcare professionals in the involvement for managing health and wellness innovation (O'Leary *et al.*, 2014). The primary goal for adopting health technologies is to provide patients the best service possible by gathering and interpreting accurate information which will help them to take correct decisions on time which reduces the cost, time and effort, thereby resulting in the timely treatment of the patient. Regulation acts as an overarching governance structure to ensure that safe outcomes are achievable. However, regulation can also dampen healthcare innovation, as it adopts a risk adverse approach to service delivery. Considering the complexity and challenges presented by various regulations associated with Connected Health, this equally presents an opportunity. Offering regulatory guidance and support can enable Connected Health innovation through clearer entrepreneurial and research and development capabilities and regulatory assessment tools. The key issues at stake for various stakeholders, when we consider the reach of Connected Health solutions, are a national and international competence to comply with various regulations, standards and ethical challenges to drive healthcare innovation. These should form part of our future research strategy using various case studies, for example. Issues and key challenges in Connected Health include:

- greater regulatory transparency on data protection, including security of health data;
- developing strategies towards realising the potential of big data in Connected Health;
- international regulatory and standards frameworks for export markets;
- assessment methodologies in Connected Health and safety performance requirements;
- requirements analysis on patient safety and improved transparency of information;
- establish good practice in Connected Health;

- examine quality in healthcare systems and equal access to Connected Health infrastructure;
- ensure interoperability of Connected Health system through new standards (technology and healthcare);
- examine issues around liability of Connected Health solutions and process in place to mitigate the risks posed by the use and prescription of technical solutions; and
- approach (as a priority) Connected Health in the context of international cooperation to increase solutions deployment and identify international and overlapping challenges to support Irish exports in this domain.

This research highlights the importance of aligning investment to Connected Health and regulations to support patient-focused and patient-empowerment research. Expanding on regulatory research capabilities to conduct quality research services can inform the ecology of Connected Health and the delivery of health services. Mobile apps will also play a more dominant role in the future of Connected Health.

Notes

1. ANSI/AAMI/IEC 62304, Medical device Software – Software life cycle processes, Association for the Advancement of Medical Instrumentation 19-July-2006.
2. http://ec.europa.eu/growth/sectors/medical-devices/documents/guidelines/index_en.htm
3. HonCode: www.healthonnet.org/HONcode/Conduct.html

References

Baujard, V., Boyer, C. and Geissbühler, A. (2010), "Evolution of Health Web certification, through the HONcode experience", *Swiss Medical Informatics*, Vol. 26 No. 69, pp. 53-55.

Burton, J., McCaffery, F. and Richardson, I. (2006), "A risk management capability model for use in medical device companies", *4th Workshop on Software Quality, International Conference on Global Software Engineering*, Shanghai, 21 May, pp. 3-8.

Carroll, N., Travers, M. and Richardson, I. (2016), "Evaluating multiple perspectives of a connected health ecosystem", *9th International Conference on Health Informatics (HEALTHINF)*, Rome, 21-23 February.

Caulfield, B.M. and Donnelly, S.C. (2013), "What is connected health and why will it change your practice?", *QJM: An International Journal of Medicine*, Vol. 106 No. 8, pp. 703-707.

Christensen, C.M., Bohmer, R. and Kenagy, J. (2000), "Will disruptive innovations cure health care?", *Harvard Business Review*, Vol. 78 No. 5, pp. 102-112.

Clarke, P., Lepmets, M., McCaffery, F., Finnegan, A., Dorling, A. and Flood, D. (2014), "MDevSPICE-a comprehensive solution for manufacturers and assessors of safety-critical medical device software", *Software Process Improvement and Capability Determination*, Springer International Publishing, pp. 274-278.

ECHAlliance (2014), "Connected health – white paper", available at: http://cht.oulu.fi/uploads/2/3/7/4/23746055/connected_health.pdf (accessed 9 March 2015).

European Commission (2012), *Medical Devices: Guidance Document-Qualification and Classification of Stand Alone Software (MEDDEV 2.1/6)*, Brussels.

European Commission (2014a), "Commission staff working document on the existing EU legal framework applicable to lifestyle and wellbeing apps", SWD 135 Final, Brussels, available

at: http://ec.europa.eu/digital-agenda/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and (accessed 19 January 2015).

European Commission (2014b), "Green paper on mobile health ('mHealth')", COM 219 final, SWD 135 Final, available at: http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth (accessed 19 January 2015).

FDA (2013a), "Content of premarket submissions for management of cyber security in medical devices", Guidance for Industry and Food and Drug Administration Staff, available at: www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm (accessed 19 January 2015).

FDA (2013b), "Cyber security for medical devices and hospital networks: FDA safety communication", available at: www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm (accessed 19 January 2015).

FDA (2015), "Mobile medical applications", available at: www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm (accessed 8 January 2015).

Finnegan, A. and McCaffery, F. (2014), "A security argument pattern for medical device assurance cases".

Finnegan, A., McCaffery, F. and Coleman, G. (2013a), "Development of a process assessment model for assessing security of IT networks incorporating medical devices against ISO/IEC 15026-15034".

Finnegan, A., McCaffery, F. and Coleman, G. (2013b), "Framework to assist healthcare delivery organisations and medical device manufacturers establish security assurance for networked medical devices", *Systems, Software and Services Process Improvement*, Springer Berlin Heidelberg, pp. 313-322.

Halamka, J.D. (2010), "Making the most of federal health information technology regulations", *Health Affairs*, Vol. 29 No. 4, pp. 596-600.

Halevy, A. (2011), "Game-changing interoperability for healthcare: bringing semantically harmonized clinical information into provider workflows from disparate health information technologies", *Emerging Technologies for a Smarter World (CEWIT), November 8th International Conference & Expo*, IEEE, pp. 1-3.

Hunink, M.M., Weinstein, M.C., Wittenberg, E., Drummond, M.F., Pliskin, J.S., Wong, J.B. and Glasziou, P.P. (2014), *Decision Making in Health and Medicine: Integrating Evidence and Values*, Cambridge University Press.

Jepsen, T. (2003), "IT in healthcare: progress report", *IT Professional*, Vol. 5 No. 1, pp. 8-14.

McCaffery, F. and Dorling, A. (2009), "Medi SPICE: an overview", available at: http://eprints.dkit.ie/125/ (accessed 15 January 2015).

McCaffery, F., Dorling, A. and Casey, V. (2010), "Medi SPICE: an update", available at: http://eprints.dkit.ie/48/ (accessed 12 January 2015).

McHugh, M., McCaffery, F. and Casey, V. (2011), "US FDA releases final rule on medical device data systems: what does this mean for device manufacturers", available at: http://arrow.dit.ie/scschcomart/27/ (accessed 12 January 2015).

McHugh, M., McCaffery, F. and Casey, V. (2012), "Software process improvement to assist medical device software development organisations to comply with the amendments to the medical device directive", *IET Software*, Vol. 6 No. 5, pp. 431-437.

O'Leary, P., Carroll, N. and Richardson, I. (2014), "The practitioner's perspective on clinical pathway support systems", *IEEE International Conference on Healthcare Informatics 2014 (ICHI 2014)*, Verona, 15-17 September.

O'Leary, P., Carroll, N., Clarke, P. and Richardson, I. (2015), "Untangling the complexity of connected health evaluations", *IEEE International Conference on Healthcare Informatics 2015 (ICHI 2015)*, Dallas, 21-23 October.

Richardson, I. (2015), "Connected health: people, technology and processes", Lero Technical Report Series Lero-TR-2015-03, University of Limerick.

Simone, L.K. (2013), "Software-related recalls: an analysis of records", *Biomedical Instrumentation and Technology*, Vol. 47 No. 6, pp. 514-522.

Wu, R., Ahn, G.J. and Hu, H. (2012), "Towards HIPAA-compliant healthcare systems", *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, ACM, pp. 593-602.

Corresponding author
Noel Carroll can be contacted at: noel.carroll@lero.ie