



REGULATING CONNECTED HEALTH: PATHWAYS, TECHNOLOGY AND THE PATIENT



BY
SILVANA TOGNERI MACMAHON



&
ITA RICHARDSON

REGULATING CONNECTED HEALTH: PATHWAYS, TECHNOLOGY AND THE PATIENT

By Silvana Togneri MacMahon & Ita Richardson



TRAPS FOR THE UNWARY TELEHEALTH PROVIDER

By Carol K. Lucas & Jennifer M. Guerrero



WHAT'S AHEAD FOR CONNECTED HEALTH POLICY: STATE & FEDERAL POLICIES IMPACTING TELEHEALTH ACCESS, PRIVACY LAWS & POLICYMAKER INTERESTS

By Amy Durbin



APPLE HEALTH'S APPROACH TO PATIENT SELF-REPORTED DATA - A GAME CHANGER OR JUST MORE NOISE?

By David Voran



CONNECTING THE MODERN WORLD OF APIS TO LEGACY HEALTHCARE INFRASTRUCTURE

By Heinz Joerg Schwarz



TOWARD A SUSTAINABLE HEALTH ECOSYSTEM FIXED ON THE DEEPEST PROFESSIONAL VALUES

By Gabriëlle Speijer & Peter Walgemoed



PATENT LAW CONSIDERATIONS FOR DRUG DISCOVERY INNOVATIONS UTILIZING ARTIFICIAL INTELLIGENCE

By Carl Kukkonen, Patricia Campbell & Gurneet Singh



Visit www.competitionpolicyinternational.com
for access to these articles and more!

REGULATING CONNECTED HEALTH: PATHWAYS, TECHNOLOGY AND THE PATIENT

By Silvana Togneri MacMahon & Ita Richardson

In this paper, we discuss how technology is changing the world around us, particularly focusing on how the introduction of Connected Health solutions can continue providing patient-centered care. We present a definition of Connected Health, which includes five components - Technology, Healthcare Pathways, People, Regulation and Data. Our article focuses on just one of these – that of regulation - presenting the importance of recognizing how Connected Health solutions, given that they are Medical Devices in many cases, must be regulated. We summarize different regulations, discussing how they should be included as a requirement when designing and developing, implementing, and using a connected health solution. Although not specifically focused on Medical Devices, we include some information on the European Union Accessibility Directive. Our conclusion focuses on the need for developers and end users to understand the importance of regulation when designing and developing health solutions.

Scan to Stay Connected!

Scan here to subscribe to CPI's
FREE daily newsletter.



01

INTRODUCTION - CONNECTED: A CHANGING WORLD

Through the use of technology, consisting of hardware and software, the world around us is changing dramatically. It is not unusual in many of our everyday environments to use smart phones, internet, mobile technology, integrated software systems and ubiquitous computing.

How has the advent of technological connectedness changed our everyday lives? Air travel has changed – one can now reach the airport security checks without ever having to interact with a person. Retail has changed – consumers can shop (and auction) online, use personal avatars to visualise how clothes would look, pay using credit cards and track their deliveries. Education has evolved. Students have access to information via the internet. Technology allows students to interact with international peers, working on team projects through discussion via e-mail, skype and similar systems.

And what of healthcare? This is also going through an evolution where healthcare is becoming increasingly computerised. This evolution is happening within hospitals and in the community. Technology is being used by people who are well and those who are ill. However, regardless of technology used, it is important that, within the medical domain, the patient will continue to be the most important consideration. *Healthcare pathways* propose the process for the efficient delivery of care to the patient, and there is a need for this to result in quality outcomes for the patient, and to do this, *patient-centred care* must be provided.² In some cases, the traditional healthcare pathway or sections of it will continue to be followed. But, introducing Connected Health solutions will often require it to change. For example, a surgeon will continue to carry out operations, but we see that sections of the traditional pathway can be replaced. For example, robots carry out surgery, while being controlled by surgeons through computerisation.³ This combination of the traditional with the technological pathway requires well-defined healthcare pathways, ensuring that each person linked to the pathway understands all roles within that pathway.

Following the healthcare pathway can be carried out by one or all of the groupings – *healthcare professionals, patients and/or carers*. There may be a Connected Health system where the healthcare professional is required, such as when medicine needs to be prescribed. There are others, where that professional input is not required, as their knowledge has been included in a decision support system. An example of this would be when a patient monitors physiological symptoms, the decision support system can automatically track inputs, and highlight deviations directly to the patient. Once this has been highlighted, the patient can then make a decision to involve the healthcare professional if they so wish. For this healthcare to be “connected,” it must be supported by *technology*.

Using technology is what allows significant changes to be made to the healthcare pathway. And, there is an external stakeholder who must be considered – *regulation*. In many countries, software and hardware used as Medical Devices have to be regulated before they can be marketed. Our particular interest is in regulation within the European Union (“EU”), which is similar to other countries such as the U.S. Depending on the safety classification of the product, different regulations apply. In addition, in providing care, there is an increased need for data to be shared between patients and care providers, within and beyond the traditional healthcare setting and often across borders. Data must be shared appropriately ensuring that the dual goals of privacy and accessibility are met.

Health professionals are making increasing use of technology to monitor, diagnose, prescribe, maintain patient records, and generally enhance their healthcare practice. This use of technology within healthcare is now commonly known as Connected Health (see Figure 1) which we define as:

Connected Health is where patient-centred care results from following defined healthcare pathways undertaken by healthcare professionals, patients and/or carers who are supported by the use of technology (software and/or hardware), regulated when used as a Medical Device, and facilitating appropriate health data sharing.

2 Noel Carroll, Catriona Kennedy & Ita Richardson, "Challenges towards a Connected Community Healthcare Ecosystem (CCHE) for Managing Long-Term Conditions," *Gerontechnology*, 14.2 (2016), 64–77 <https://doi.org/10.4017/gt.2016.14.2.003.00>.

3 Christina A. Fleming and others, "A Review of Clinical and Oncological Outcomes Following the Introduction of the First Robotic Colorectal Surgery Programme to a University Teaching Hospital in Ireland Using a Dual Console Training Platform," *Journal of Robotic Surgery*, 14.6 (2020), 889–96 <https://doi.org/10.1007/s11701-020-01073-8>.

02

WHAT ARE THE DOMAIN SPECIFIC/ DEFINING FEATURES OF THE REGULATION OF CONNECTED HEALTH?

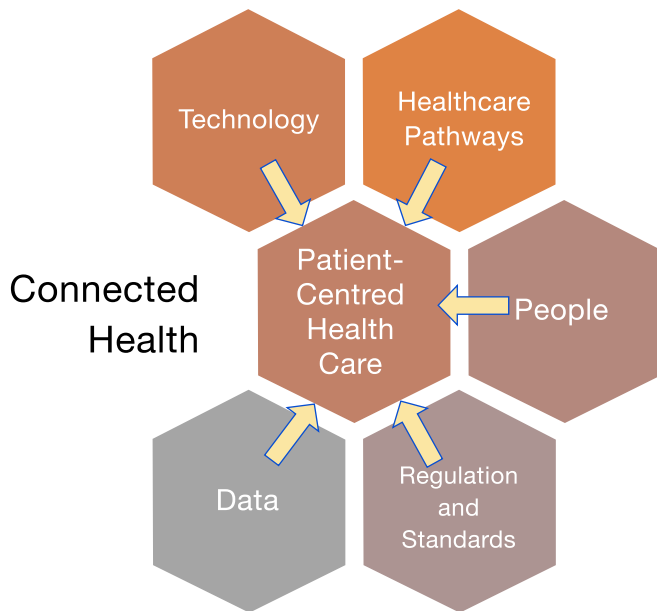


Figure 1 – Connected Health components provide Patient-Centred Health Care

For Connected Health to be implemented successfully and efficiently, each of these five components (Technology, Healthcare Pathways, People, Regulation, and Data) must work together. Therefore, it is incumbent on healthcare professionals, patients, carers (formal and informal), and technologists to develop solutions together. And for solutions to work, processes have to be defined within the Healthcare Pathways. Connected Health solutions have the ability to improve care for the patient – but to do this, all components need to be included. In this article, we focus on regulation (and standards), as it is important to consider these. This discussion of regulation that follows is not intended to be exhaustive but indicative of the considerations of manufacturers and healthcare delivery organisations implementing Connected Health systems.

“Using technology is what allows significant changes to be made to the healthcare pathway.”

In order to understand the impact of regulations on Connected Health, we focus on the impact of regulation on Medical Device technology. Medical Devices must comply with the regulations of the geographical location in which the device is to be marketed. These devices are often systems of systems and are composed of, for example, hardware, software, networks, interfaces to other systems, Medical Devices and data. They are strictly regulated before they can be placed on the market to ensure their safety. While many Medical Devices were originally designed to be standalone, but ultimately, it was recognised that Medical Devices could be used more efficiently if they were connected to a network so that information could be passed between devices and other systems.

Therefore, when a Medical Device was designed to be connected to a network, generally the manufacturer would supply and control the network. This limited the “connectedness” of the device but was done so that the regulated Medical Device was part of a manufacturer-controlled system. This meant that manufacturer could ensure that the placing of the device onto the network did change the device in any way from the regulated version, thus not compromising the safety of the device. However, there has been an increased requirement for the integration of software and hardware systems, thus removing the possibility of continued use of manufacturer-controlled systems. This means that regulation must not only be considered during design and development of Medical Devices, but also during the integration of devices when implementing them for use.

Today’s sophisticated Connected Health systems provide advanced levels of decision support and integrate patient data between systems, across organizational lines, and across the continuum of care. In addition to these benefits, there is also increased likelihood of software-induced ad-

verse events.^{4,5} The organizations involved in developing, implementing and operating the many connected health components and services in order to support patient-centred care must ensure that three key properties are preserved across the lifecycle of the system – Safety, Effectiveness and Security.⁶

Safety is defined as “freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment.” Effectiveness is defined as “the ability to produce the intended result for the patient and the responsible organisation.” In this case, the responsible organisation is the organisation developing, implementing and operating the system. Security is defined as “an operational state of a medical information technology network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability.” In order to preserve these properties, the organisation must consider the use of the Connected Health technology in the context of the Medical Device regulation. It should be noted also that there is an interdependence between these three properties. For example, exercising a security vulnerability within a Medical Device could ultimately compromise the safety and therefore, the effectiveness of the device. As such, all three properties must be addressed together.

03

HEALTHCARE SYSTEM REGULATIONS – REGULATIONS AND STANDARDS FOR CONNECTED HEALTH

To understand the interplay of regulations and standards for Connected Health, we need to consider the lifecycle for the development of Health Information Technology (Health IT lifecycle).

The Health IT lifecycle is broken down into three broad phases⁷: Design and Development, Implementation and Clinical Use. Different standards and regulations apply to different phases of this lifecycle.

During the *Design and Development phase* Medical Devices that are designed to be marketed in the EU must comply with Regulation 2017/745 on Medical Devices (“MDR”) and Regulation 2017/746 on In-Vitro Diagnostic Devices (“IVDR”). The MDR became fully applicable on 26 May 2021 and the IVDR became fully applicable on 26 May 2022, after a five-year transition period. The MDR and IVDR represent a significant development and strengthening of the existing regulatory system for Medical Devices in Europe and the legislation now being in the form of a Regulation, rather than a Directive, means that the EU law is directly applicable at national level. Thus there is no longer a requirement for transposition through specific national legislation which should prevent variation in the approach taken. These regulations also apply to other phases of the lifecycle.

4 Silvana Togneri MacMahon, Fergal McCaffery & Frank Keenan, "Development of the MedITNet Assessment Method - Enabling Healthcare Delivery Organisation Self Assessment against IEC 80001-1," in *First International Conference on Fundamentals and Advances in Software Systems Integration (FASSI 2015)*, ed. by Chris Ireland and Petre Dini (Venice, Italy: IARIA, 2015) <https://doi.org/ISBN: 978-1-61208-448-0>.

5 S.T. MacMahon, F. McCaffery & F. Keenan, "Development and Validation of the MedITNet Assessment Framework: Improving Risk Management of Medical IT Networks," in *ACM International Conference Proceeding Series*, 2015, xxiv-xxvi-AUGU <https://doi.org/10.1145/2785592.2785599>.reduced costs of care and a reduction in adverse events. Traditionally, medical devices were placed onto a proprietary IT network provided by the manufacturer of the device. Today, medical devices are increasingly designed for incorporation into a hospital's general IT network enabling devices to exchange critical information. However, this can introduce risks and negate the potential benefits to patients. While the IEC 80001-1 standard has been developed to aid Healthcare Delivery Organisations (HDOs).

6 IEC, "IEC 80001-1 - Application of Risk Management for IT-Networks Incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities" (Geneva, Switzerland: International Electrotechnical Commission, 2010).

7 ISO, *ISO 81001-1: Health Software and Health IT Systems Safety, Effectiveness and Security – Part 1: Principles and Concepts* (Geneva, Switzerland, 2021).

The EU also states that for the new regulation that “Compliance with a harmonised standard confers a presumption of conformity with the corresponding essential requirements set out in Union harmonisation legislation from the date of publication of the reference of such standard in the Official Journal of the European Union.”⁸ This means that manufacturers that comply with the requirements of the recognised standards can also claim conformity to the regulations. To date, 14 standards have been recognised and it is expected that the Commission will issue further implementing decisions to add to the list of Harmonised standards later in 2022. Some standards (such as IEC 62304:2006 Medical device software — Software life cycle processes) which conferred a presumption of conformity with the previous Medical Device Directive have not yet been recognised.

During the *Implementation Phase*, Medical Device manufacturers and healthcare delivery organisations (“HDOs”) will collaborate to ensure that the three key properties are protected. This phase consists of:

- Acquisition of the device (including manufacturer compliance);
- Installation, customisation and configuration;
- Integration, data migration, transition and validation;
- Implementation, workflow optimisation and training.

HDOs may wish to implement the requirements of the IEC 80001-1:2021 (Application of risk management for IT-networks incorporating Medical Devices — Part 1: Safety, effectiveness and security in the implementation and use of connected Medical Devices or Connected Health software) family of standards. In addition, HDOs will also need to consider regulation related to the data that is being transmitted along with the consideration of the 3 key properties that have previously been discussed. Privacy issues will also need to be addressed. In the EU, the General Data Protection Regulation (“GDPR”) ⁹ recognises data concerning health as a special category of data

and provides a definition for health data for data protection purposes. It requires specific safeguards for personal health data which will need to be addressed in the context of Connected Health, including the facilitation of cross border care.

“*The Health IT lifecycle is broken down into three broad phases*”

Data standards such as FHIR¹⁰ and DICOM¹¹ are relevant in this context. In May, 2022, the European Commission published a proposal for a Regulation on the European Health Data Space (“EHDS”).¹² With the proposal, the European Commission aims to make significant progress towards a single market for digital health services and products with the overall objective being to ensure that electronic health data are as open as possible and as closed as necessary to facilitate research, innovation, policy-making, and regulatory activities. The aim is to have a single internal market for health data between the EU Member States.

The *Clinical Use phase* consists of Operations and maintenance and Decommissioning. The focus for both the Medical Device manufacturer and the HDO is to ensure that the connected health system continues to be compliant with the relevant regulations and standards as these activities take place. For example, when making a change to a device within an existing system, in order to address a security vulnerability, the manufacturer and HDO will need to ensure that the change is made within the existing risk management process and that the change does not impact the key properties of the system.

Connected Health systems are increasingly including Medical Devices that use sophisticated Artificial Intelligence. The

8 European Council, "Commission Implementing Decision (EU) 2021/1182 of 16 July 2021 on the Harmonised Standards for Medical Devices Drafted in Support of Regulation (EU) 2017/745 of the European Parliament and of the Council," *EUR-Lex*, 2021 https://eur-lex.europa.eu/eli/dec_impl/2021/1182/oj [accessed 27 July 2022].

9 European Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," *EUR-Lex*, 2016 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [accessed 27 July 2022].

10 HL7, "HL7 FHIR Release 4B," 2022 <https://hl7.org/FHIR/>.

11 Medical Imaging and Technology Alliance, "Digital Imaging and Communications in Medicine" (National Electrical Manufacturers Association, 2009) <http://medical.nema.org/standard.html>.

12 European Council, "European Health Data Space," *European Commission*, 2021 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en [accessed 27 July 2022].

European Commission published its Proposal for a Regulation on Artificial Intelligence (“AI”) in April of 2021,¹³ which aims to develop a comprehensive framework for the regulation of AI. Parts of the proposal address high risk AI applications, which would include the use of AI in Medical Devices and Connected Health systems. No international guidance, common specifications and/or harmonised standards currently exist for the use of AI in Medical Devices. Therefore, regulators continue to work to address the challenge of regulation of Medical Device software that include AI algorithms and to address the unique challenges that AI can give rise to in the context of healthcare including, for example, the issues related to the automated processing of data and compliance with GDPR which requires that “meaningful information about the logic” involved in decisions related to their care is provided by manufacturers to patients.

While the EU Accessibility directive, EN 301 549 V3.2,¹⁴ which came into effect in June 2021,¹⁵ has not been specifically written with Medical Devices in mind, we believe that it should be considered in this discussion. We recognise that many national health services in European countries are public bodies, and the users of such devices will often have accessibility issues through disability, impairment or limitation, for example, visual impairment, intellectual and developmental disability. The Accessibility directive requires that all public sector bodies in the EU have accessible online websites and mobile apps, and many connected health solutions provided are implemented through these means. EN 301 549 is aligned to the [Web Content Accessibility Guidelines v2.1](#), published by the W3C and known as WCAG 2.1.¹⁶ These are internationally recognised requirements for producing web and mobile content, are considered best practice, and are very widely used. It should be noted that the directive also contains requirements not mentioned in WCAG 2.1, and so, there should not be a singular reliance on WCAG 2.1 when developing accessible software.

According to Tsvyatkovska et al.,¹⁷ accessibility is concerned with the quality of being “easy to reach and use.” This requires the developers to understand that the software should provide the correct functions for the user and that

the user interface should adhere to the directive. They also discuss the concept of accessible interaction, which would include, for example, features which support new users in understanding and using the software. Furthermore, designing of interactive elements which support low physical effort should also be considered.

04 CONCLUSION

Connected Health systems have a complex lifecycle as devices are added and removed, data is transferred within and beyond the system, and new types of technology such as AI are integrated. Different regulations apply to these phases and aspects of the lifecycle. The properties of safety, security and effectiveness are protected by these regulations and supported by the implementation of harmonised and voluntary standards. Implementation of these standards needs to be supported by all stakeholders within the broader healthcare socio-technical ecosystem. Those within HDOs, including Clinicians, Clinical Engineers, and Information Technology Specialists, need to be aware of their responsibilities under the regulations in how they design and develop, implement, and use Connected Health solutions.

Our thesis is that, given the wide variety of regulations and standards which should be considered when developing Connected Health solutions, some of which we have discussed in the previous section, developers should consider that regulations are an important stakeholder in the design and development phase of the Health IT lifecycle. Too often, it is seen that a Connected Health solution can solve a health care issue, software is developed, and yet, it cannot be used due to the lack of implementing regulations. Users of such systems also need to be aware of these requirements. Indeed, Wykes

13 European Council, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS," *EUR-Lex*, 2021 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> [accessed 27 July 2022].

14 European Union, "2016, Directive (EU) 2016/2102 of the European Parliament and the Council of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies, EN 301 549 V3.2.1, Web Accessibility Directive, No Title," 2016 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102>.

15 European Commission, "Web Accessibility Directive – Standards and Harmonisation," 2021 <https://digital-strategy.ec.europa.eu/en/policies/web-accessibility-directive-standards-and-harmonisation>.

16 WC3, "Web Content Accessibility Guidelines (WCAG) 2.1" <https://www.w3.org/TR/WCAG21/>.

17 Damyanka Tsvyatkovska and others, "Digital Contact Tracing Applications for COVID-19: A Citizen-Centred Evaluation Framework (Preprint)," *JMIR MHealth and UHealth*, 2021.

and Schueller¹⁸ suggested that app stores should take responsibility for providing information on, what they define as Transparency for Trust (“T4T”) principles - privacy and data security, development characteristics, feasibility data, and benefits.

Technology is changing rapidly and regulators are working to keep pace. Manufacturers and HDOs need to be aware that the regulations in the space are changing rapidly and that there is a need to stay up to date with the changing position regarding regulations but also regarding recognised harmonised standards in this area.

However, to ensure that standards can support regulation, and to ensure that the standards can be adopted and implemented within specific HDO contexts, Healthcare Stakeholders need to input into the development of standards. They can become involved by engaging with national standards groups relevant mirror committees and providing feedback on their experiences of implementing standards and on this basis provide recommendations for the development of new standards in the area. ■

“*Connected Health systems have a complex life-cycle as devices are added and removed, data is transferred within and beyond the system, and new types of technology such as AI are integrated*”

18 Til Wykes and Stephen Schueller, "Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces," *Journal of Medical Internet Research*, 21.5 (2019) <https://doi.org/10.2196/12390>. a light-touch approach to consumer protection is now warranted to give customers a modicum of information to help them choose from the vast array of so-called health apps. We suggest 4 guiding principles that should be adopted to provide the consumer with information that can guide their choice at the point of download. We call these the Transparency for Trust (T4T).

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

