

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

Internet of Everything in Healthcare: Reconciling the Risks and Benefits of Data Sharing in IoT-Enabled Telehealth Environments

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

Rak, R. (2021). Internet of Everything in Healthcare: Reconciling the Risks and Benefits of Data Sharing in IoT-Enabled Telehealth Environments. IEEE [10.1109/ICEDEG52154.2021.9530853].

Availability:

This version is available at: <https://hdl.handle.net/11585/832179> since: 2023-02-23

Published:

DOI: <http://doi.org/10.1109/ICEDEG52154.2021.9530853>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

This is the final peer-reviewed accepted manuscript of:

R. Rak, "Internet of Everything in Healthcare: Reconciling the Risks and Benefits of Data Sharing in IoT-Enabled Telehealth Environments," *2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG)*, Quito, Ecuador, 2021, pp. 223-225,

The final published version is available online at: **doi: 10.1109/ICEDEG52154.2021.9530853**

Rights / License:

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>)

When citing, please refer to the published version.

Internet of Everything in Healthcare: Reconciling the Risks and Benefits of Data Sharing in IoT-Enabled Telehealth Environments

Richard Rak

Research Associate, Law, Science and Technology – Rights of Internet of Everything
(Horizon 2020 Marie Skłodowska-Curie Actions Innovative Training Networks) European Joint Doctorate
University of Vienna (Austria), University of Bologna (Italy) and University of Turin (Italy)

Abstract—The promise of Internet of Everything in healthcare (‘Internet of Healthcare’) is that Internet of Things (IoT)-enabled devices and concomitant enabling technologies could be used to leverage data concerning health in order to increase medical intelligence and support decisions affecting health. Remote diagnosis, monitoring and treatment of citizens/patients by use of IoT-enabled solutions, and the tracking of citizens/patients along the healthcare continuum could facilitate the transformation of healthcare from a merely reactive system to a data-driven and person-centred system that provides integrated real-time response solutions, as well as prospective insights. Despite the clear advantages, these developments have raised concerns about risks posed by unjustified interferences with privacy and/or illicit access to or improper processing of data concerning health. These concerns stem from the inherent tension that stakeholders in health data ecosystems need to collect, share, access and analyse vast amounts of sensitive data to generate increased value. To overcome these challenges, this research aims to identify *lex ferenda* measures, state-of-the-art technical tools and good datagovernance practices, which could be deployed in a European legal context to maximise the benefits and minimise the risks of sharing data concerning health in IoT-enabled telehealth environments.

Keywords—Internet of Everything, Internet of Healthcare, Internet of Health Things, telehealth, data concerning health

I. INTRODUCTION: VISION GAINED FROM RELATED CONCEPTS

Internet of Everything (IoE) is a concept that describes the next wave of Internet growth and aims to look at the context in which Internet of Things (IoT) fits from a more holistic perspective. The term ‘IoE’ is defined as “a network of networks” that “brings together people, process, data, and things to make networked connections more relevant and valuable than ever before” [1]. IoE rests on an enormous number of unique and complex connections and interactions between heterogeneous technologies, machines and a variety of stakeholders. Fig. 1. presents a broader conceptual view of IoE that encompasses representations of machine-to-machine (M2M), people-to-machine (P2M) and technology-assisted people-to-people (P2P) communications. It also illustrates how IoE can enhance the transformation of user-generated raw data collected by ‘things’ into “smart”, “actionable” data, “meaningful” knowledge and added value.

The promise of IoE in healthcare (‘Internet of Healthcare’) is that the use of IoT-enabled devices (‘Internet of Health Things’, IoHT) and concomitant enabling technologies (such as scalable distributed computing, AI-driven data science and distributed ledger technologies) could interconnect health data

ecosystems and leverage data concerning health. Data is a critical enabler for developing and delivering better and more personalised health diagnosis, monitoring and treatment services. As demonstrated by the COVID-19 pandemic, data is also an essential asset in tackling public health emergencies. The development of Internet of Healthcare could help to increase medical intelligence and support decisions affecting health by delivering the right information to the right person (or machine) at the right time and in the right place [2]. The availability, interoperability, portability and analyses of data concerning health and the tracking of citizens/patients along the healthcare continuum could facilitate the transformation of healthcare from a merely reactive system to a value-based system that provides integrated real-time response solutions, as well as prospective insights [3].

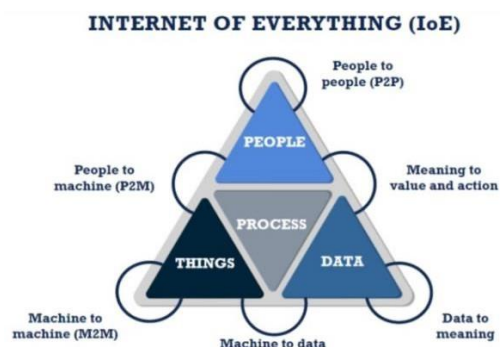


Fig. 1. Conceptual framework of Internet of Everything: interconnecting things, people, data and process

In order to generate increased value from data in healthcare or health-related non-healthcare settings (such as occupational health), stakeholders need to collect, share, access and analyse vast amounts of sensitive data [4]. These efforts are dependent on the uptake of IoT-enabled applications, which can provide increased sensing, communications and processing capabilities. In addition to these, intelligent connections in eHealth can enable the sharing of sufficient amounts of data that are necessary to conduct health analyses. Although the potential of data use is enormous, the problem is that this potential is not realised, because a number of significant barriers stand in the way of sharing data concerning health [5]. In this respect, according to a public consultation carried out by the European Commission, individuals are most concerned with risks of privacy breaches and cybersecurity risks [6]. This underpins a hypothesis that benefits from sharing data concerning health in the context of an emerging Internet of Healthcare cannot be maximised, unless the risks posed by unjustified interferences with privacy and/or illicit access to or improper processing of data concerning health are minimised.

Acknowledgment: This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska Curie grant agreement No. 814177.

II. RESEARCH SCOPE, FRAMEWORK AND METHODOLOGY

The focus of this research is on privacy, data protection and data governance challenges posed by the use of IoHT devices and underlying systems for sharing data concerning health. The scope of this research covers telehealth, a fundamental pillar of Internet of Healthcare and an area of healthcare, which has become highly relevant in the fight against the COVID-19 pandemic. The public health crisis has accelerated the transformation of health systems to become more closely tied to citizens/patients and increasingly dependent on the provision and use of telehealth services [7]. Since the beginning of the pandemic, providers have rapidly scaled telehealth services, while consumer adoption of telehealth solutions has increased at an unprecedented pace [8]. By explanation, telehealth services utilise information and communications (enabling) technologies and digital communications networks to deliver healthcare, promote health and transmit data concerning health (and other types of data) between a citizen/patient and healthcare provider (or other stakeholders), who are located at the communications endpoints and are separated by distance [9–10]. ‘Telehealth’ is different from ‘telemedicine’, because it refers to a broader scope of remote healthcare services: while ‘telemedicine’ stands specifically for remote clinical services delivered by medical professionals, ‘telehealth’ denotes all remote healthcare services provided to advance the health and well-being of citizens/patients [11].

The research aim is to identify *lex ferenda* measures, state-of-the-art technical tools and good data governance practices, which could be deployed (under the framework of European privacy, data protection and health laws) to maximise the benefits and minimise the risks of sharing data concerning health in IoT-enabled telehealth environments. These findings could help to strengthen the legal protection of citizens/patients (including persons acting in the capacity of consumers or employees) and the trust of stakeholders in exploiting the potential benefits of IoT-enabled telehealth solutions in an emerging Internet of Healthcare. In accordance with the foregoing aim, the main research question asks:

How could privacy, data protection and data governance measures and mechanisms reconcile the risks and benefits of sharing data concerning health in the context of IoT-enabled telehealth data ecosystems?

In order to answer this question, the research employs interdisciplinary legal research methods to explore, describe and explain privacy, data protection and data governance challenges posed by Internet of Healthcare. The general value of conducting interdisciplinary legal research is that it can lead to a more informed and balanced judgment, and therefore, one may be able to better grasp the forces which act upon the relevant rules and how legal norms operate in this context, rather than just being interested only in the ‘law as such’ [12]. The research is qualitative in nature, and is based on the formulation of a theory-driven model (IoE in healthcare) followed by analyses of three key topical challenges that affect data sharing in IoT-enabled telehealth environments. The research is positioned at the intersections of: a) privacy and data protection law; b) health law; c) information and communications technology law; d) technoethics; e) health informatics; and f) health data governance and information management. Sources encompass: (i) legal acts and accompanying authoritative legal interpretations adopted by the EU; (ii) national health laws of selected EU Member States

concerning specific rules on the protection of data concerning health; (iii) policy and sector-specific expert guidance documents drafted at EU level; (iv) international and European technical standards; and (v) scientific papers and non-academic literature (studies prepared by consulting firms, industrial organisations and representative bodies).

III. PRELIMINARY FINDINGS

The first research objective was to conceptualise IoE in the domain of healthcare (and, in particular, telehealth) with the aim of drawing inferences as to whether *lex lata* concepts are adequately defined to deal with the structures and dynamics of newly emerging IoT-enabled health data ecosystems. The analysis focused on legal and technological matters relating to the four dimensions of IoE (things, data, people and process) in healthcare. This conceptual framework has shed light on shortcomings in the clarity and/or applicability of current legal concepts in EU privacy, data protection and health law:

- IoT-enabled embodied (body-centric) computing has turned the human body into a new ‘data platform’. IoHT devices have evolved from “first-generation” externally body-affixed devices to “second-generation” body-internal (implantable, embeddable or ingestible) devices, and “third-generation” neurotechnology devices (including brain-computer interfaces and non-invasive detection of bioelectric signals). This evolution poses significant challenges to ‘informational privacy’ and ‘informational self-determination’, which are prerequisites to exercising rights derived from ‘human/patient’s autonomy’. For this reason, it would be essential to protect cerebral activity and data, and to adopt a new set of ‘neuro-rights’ in order to safeguard the individual’s cognitive liberty, mental privacy, mental integrity and psychological continuity [13].
- As consumer IoHT devices have blurred the borderline between ‘medical’ and ‘non-medical’ devices, an alternative (or supplementary) regulatory model to the ‘intended purpose’ threshold set by Article 2(1) of the Medical Devices Regulation (MDR) [13] could be the adoption of a ‘risk-based case-by-case’ approach, the regulatory model used in the US.
- IoHT devices and IoT-enabled telehealth systems empowered by data science methods (ranging from cloud-based techniques to AIoT) carry the potential to transform ‘raw big data’ into ‘smart data’ and insights. However, there are currently overlaps and inconsistencies between the MDR [14], the GDPR [15] and the proposed AI Act [16] in terms of the risk management requirements for AI-enabled IoHT devices.
- Shared computing resources are key to the functioning of IoT-enabled telehealth systems. It is important that the notion of ‘cloud infrastructure service providers’ is clarified in the proposed Data Governance Act (DGA) [17]; it is unclear whether this proposed new legal notion would encompass other, more scalable and distributed (e.g. fog, edge) computing services.
- Distributed ledger technology (DLT)-based health data interoperability schemes can better integrate IoT-enabled telehealth systems and allow citizens/patients to have greater control over sharing and permitting

access to their data concerning health. The integration of DLTs into IoT-enabled telehealth systems requires tensions between DLTs and data protection and data governance laws to be resolved, such as the proper allocation of responsibilities, compliance with the principle of data minimisation or the effective exercise of the rights of the data subject (e.g. right to erasure).

- The boundaries of ‘data concerning health’ have become obscure in IoT-enabled telehealth. With references to Article 4(15) and Recital 35 of the GDPR, it is unclear what the parameters are for determining the ‘degree of revelation’, especially in case of ‘quasi health data’ (when inferences can be drawn about a person’s health from their lifestyle).
- Internet of Healthcare is dependent on enhancing sharing of and access to data concerning health. However, the definitions of ‘data sharing’ and ‘access’ given by the proposed DGA are dubious, especially in light of the complexities of IoT-enabled telehealth ecosystems. Furthermore, the interplay between data protection-based functional roles (under the GDPR) and data governance-based functional roles (under the proposed DGA) lack legal clarity.

IV. FUTURE ORIENTATION AND RESEARCH CHALLENGES

The following steps of this research will focus on analysing three topical privacy, data protection and data governance challenges that affect the sharing of data concerning health in IoT-enabled telehealth environments.

The first research challenge concerns the mapping of moral and legal requirements that developers and service providers must satisfy in order to ensure responsible design and trustworthy (ethical and robust) implementation of IoT-enabled telehealth systems. In connection with these requirements, the research aims to identify appropriate technical and organisational measures (best practices), which could facilitate the implementation of data-protection principles in IoT-enabled telehealth systems in an effective manner. In particular, the research seeks to explore whether the integration of DLT-based technical and organisational measures into IoT-enabled telehealth systems could help to implement the concept of data protection (and privacy) by design and by default.

The second research challenge concerns the integration of AI into IoHT devices and IoT-enabled telehealth systems. The research will analyse the management of risks relating to data processing operations in AI-augmented IoHT devices and telehealth systems. The research will compare risk management compliance requirements (as part of medical device conformity assessments, data protection impact assessments and AI risk assessments) across four use cases: AI-augmented medical devices; AI-augmented non-medical IoHT devices; cloud-based AI-augmented IoT-enabled telehealth systems; and “embedded” AI-augmented IoHT devices. By analyses of these use cases, the research aims to draw inferences about the lack of harmonisation between the MDR, the GDPR and the proposed AI Act, and their practical implications and shortcomings.

The third research challenge concerns the interpretation of the legal framework regulating the use of IoHT devices at the workplace. This problem reflects on the legal challenge posed by the monitoring of the health and well-being of employees

by use of wearables for the purposes of human resource management, work capacity assessment, occupational medicine and/or provision of corporate well-being programs. The research will compare the national laws of three EU Member States (Belgium, Finland and Hungary) to analyse the differences between legal conditions for processing data concerning health in the context of employment.

V. REFERENCES

- [1] D. Evans, The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. CISCO Internet Business Solutions Group, 2012, pp. 2–3.
- [2] CISCO Systems, White Paper: The Internet of Everything (IoE) and the Delivery of Healthcare. CISCO Systems, 2015, pp. 1–2.
- [3] J. Chanchaichujit, A. Tan, F. Meng, et al., Healthcare 4.0: Next Generation Processes with the Latest Technologies. Singapore: Palgrave Pivot, 2019, p. 10.
- [4] P. Spence, J. Evans, and E. Licking, Unlocking the power of data to improve health outcomes: five trends to watch. Ernst & Young, 2019, p. 4.
- [5] European Commission, Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final – SEC(2020) 405 final – SWD(2020) 296 final, SWD(2020) 295 final, 25 November 2020, pp. 8,11.
- [6] European Commission, College of Europe, *Consultation: Transformation Health and Care in the Digital Single Market*. Synopsis Report. Luxembourg: Publications Office of the European Union, 2018, pp. 7–9.
- [7] PwC Health Research Institute, *Acceleration of the New Health Economy: The pandemic edits the DNA of the health system*. PwC, 2020, pp. 1–3.
- [8] O. Bestsennyy, G. Gilbert, A. Harris, et al., Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company, 29 May 2020.
- [9] International Organization for Standardization, ISO/TS 13131:2014: Health informatics — Telehealth services — Quality planning guidelines, Geneva, International Organization for Standardization, 2014, para. 3.6.2.
- [10] S. Sood, V. Mbarika, S. Jugoo, et al., “What Is Telemedicine? A Collection of 104 Peer-Reviewed Perspectives and Theoretical Underpinnings,” *Telemedicine and eHealth* vol. 13, no. 5, 2007, pp. 573–590 at 580–586
- [11] World Health Organization Global Observatory for eHealth, *Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth*, Report of the third global survey on eHealth. Geneva: World Health Organization, 2010, pp. 8–9.
- [12] M. M. Siems, “The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert,” *Journal of Commonwealth Law and Legal Education* vol. 7, no. 1, 2009, pp. 5–17 at 12.
- [13] Ienca M and Andorno R, “Towards new human rights in the age of neuroscience and neurotechnology,” *Life Sciences, Society and Policy* vol. 13, no. 5, 2017.
- [14] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance), OJ L 117, 5.5.2017, pp. 1–175.
- [15] 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 (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1–88.
- [16] 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, COM/2021/206 final, 21.04.2021.
- [17] Proposal for a Regulation of the Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, 25.11.2020.