Proceedings of the 2019 Health IT Workshop on

Emerging Technologies in Healthcare: Legal, Ethical & Social Aspects

7th & 8th November 2019
Middlesex University, London, UK

Proceedings of the 2019 Health IT Workshop on

Emerging Technologies in Healthcare: Legal, Ethical & Social Aspects

7th & 8th November 2019
Middlesex University, London, UK

Editors:
Carlisle GEORGE (*Middlesex University, UK*),
Diane WHITEHOUSE (*The Castlegate Consultancy, UK*),
Penny DUQUENOY (*Middlesex University, UK).*

ISBN 978-1-64713-330-6

Foreword

This sixth health IT workshop signals the growing importance of ethics, law and governance of emerging technologies and of the power of sustained international collaborations.

The stakes could not be higher. From the evolution of learning healthcare systems and ever-new and tricky privacy challenges, to identification of appropriate uses and users of intelligent machines, the need to ensure that we get it right is of the highest importance. People cannot "get it right" without the kind of research and scholarship brought to bear in forums like this one.

This year's programme is thematically and professionally diverse. It addresses the development and applications of extraordinarily powerful machines, and features speakers who have made ethics and health information technology their focus. The speakers' contributions document the breadth and creativity of the emergence of one of the world's leading forums for addressing ethical and legal issues raised by a health technology with unprecedented global reach and effect.

It is said that science and technology often outstrip ethics and the law, and that people's ability to design new tools is superior to, or at least more rapid than, their capacity to ensure that these tools are used wisely.

This workshop and its antecedents are important counterexamples to such a position. With speakers from academia, government and industry, the workshop continues a decade-long initiative. It makes plain a collective commitment to the kind of values and governance that both advance the benefits of new technology, and protect human rights and honour universal values.

This transcontinental partnership, linking the University of Miami with Middlesex University, The Castlegate Consultancy and The European Centre for Ethics, Law and Governance in Health Information Technology, is perhaps unique in its topics and foci. It has simultaneously fostered innovative scholarship and provided rare opportunities for students to participate in an exciting new area of inquiry and practice.

It seems clear that this is not solely a valuable partnership, it might even be a fundamentally necessary one. The flow of both data and discovery has been enough to render the world a very different place in a very short time. As that world is too often a place of conflict and discord, these kinds of collaborations point the way to doing things better. This, precisely, is how we will get it right.

Prof Kenneth W. Goodman
Professor of Medicine and jointly of Philosophy
Director, University of Miami Miller School of Medicine Institute for Bioethics and Health Policy
Director, WHO Collaborating Centre in Ethics and Global Health Policy
Chair - Ethics Committee of the American Medical Informatics Association

Contents

Welcome from the Interim Vice-Chancellor

Technology has incredible power to transform healthcare. In my own time with an NHS Ambulance Service, I saw the introduction of triage systems, vehicle tracking, electronic patient care records, on-line training as well as technology deployed directly to give clinicians new options in providing care. However, technology can also be associated with a seductive belief that deployment is easy and that benefits, be they clinical or operational, outweigh the risks or costs. It is easy to see when poor technology is a cause of problems; but good technology deployed without thought for the consequences carries just as many risks. Technology relies on people and people are fallible; whether this is making mistakes or being unwilling to recognise the cause of problems.

The law provides a framework to resolve some of these challenges. Ethics provides a potentially stronger opportunity to avoid or sidestep problems. Any healthcare system must operate within a social context. These three complimentary lenses provide a framework to ensure that technology meets its promise to transform.

At Middlesex University we are proud of our world-class team of people who improve healthcare outcomes by educating the healthcare professionals of tomorrow in an environment in which we advance technology and clinical practice. As a University, we have an important role to play in providing the opportunity to share knowledge and challenge ideas in order to advance understanding. The topic of eHealth is one which will modify clinical outcomes and therefore transform lives.

I am very grateful to Dr Carlisle George, Ms Diane Whitehouse, Prof Kenneth Goodman and Dr Penny Duquenoy for organising this workshop and assembling this group of expert and distinguished speakers for two days.

I welcome you to Middlesex University. I also hope that you leave challenged, having shared and listened to new and different perspectives that you can then carry forward into your important work in this field!

Mr James Kennedy
Interim Vice-Chancellor, Middlesex University, UK

Welcome from the Pro-Vice Chancellor and Executive Dean

Technological developments in healthcare have saved countless lives and improved our quality of life; however, complex challenges arise when considering the legal, ethical and social aspects of emerging technologies. The rapid development of technologies, such as artificial intelligence and blockchain, have the potential to deliver better patient outcomes. Yet they need careful consideration in light of concerns about privacy, cyber security, patient rights, political decisions on national and international regulatory frameworks, and questions of equity in access to care and information.

Universities have an important role to play amid this complexity, since they can create platforms for discussion and exchange that bring together different disciplinary insights, national and international perspectives, theory and practice, and knowledge of the latest and likely future developments in both healthcare and information technology.

Middlesex University, with our reputation for educating the healthcare practitioners of the future and for innovating in computer and data science, is an ideal venue for bringing together thought leaders who are grappling with these challenges.

I wish to thank Dr Carlisle George, Ms Diane Whitehouse, Prof Kenneth Goodman and Dr Penny Duquenoy, for organising such an important event.

I hope that you have an enjoyable and stimulating event in one of the world's most exciting cities and at one of the UK's most progressive and international universities.

Prof Sean Wellington
Pro Vice-Chancellor and Executive Dean
Faculty of Science and Technology, Middlesex University, UK

Workshop Introduction

Emerging technologies in healthcare continue to play an important role in improving the provision of services for patients; however, they raise many concerns that require careful analysis and discussion.

This workshop will primarily focus on legal, ethical and social aspects of new and emerging technologies in healthcare as well as developments regarding regulatory and ethical frameworks including:

- AI (Machine learning) and data science in healthcare
- Blockchain technologies in healthcare
- Mobile Health Apps – development of guidelines and regulatory framework
- Advances in eHealth, mHealth, Telemedicine, Telecare and Telehealth
- Privacy and Data Protection
- Data Sharing
- Wider access to (personal) health data (e.g. in terms of personalised health; population health)
- Threats to healthcare IT infrastructure (e.g. cyber security, network security)

Workshop Organising Committee

- **Dr Carlisle George**: Associate Professor and Barrister, Middlesex University, UK.
- **Ms Diane Whitehouse**: eHealth Consultant, The Castlegate Consultancy, UK.
- **Prof Kenneth Goodman**: Director, Institute for Bioethics and Health Policy, University of Miami, USA.
- **Dr Penny Duquenoy**: Chair-BCS ICT Ethics Specialist Group, Visiting Researcher, Middlesex University, UK.

Workshop Sponsors

- **Faculty of Science and Technology,** Middlesex University, UK.
  http://www.mdx.ac.uk/about-us/our-faculties/faculty-of-science-and-technology

- **Institute for Bioethics and Health Policy,** Millar School of Medicine**,** University of Miami, USA.
  https://bioethics.miami.edu

- **The Castlegate Consultancy,** UK.

- **The European Centre for the Study of Ethics, Law and Governance in Health Information Technology (ECELGHIT),** Online.
  http://ecelghit.org

Workshop Programme
Town Hall - Committee Room 3

Day 1 – Thursday, 7th November 2019

TIME	SESSION	Page Number
13.00 – 13.15	Registration, mix-and-mingle	
13.15 – 13.20	**Welcome, Middlesex University**	
	KEYNOTE - 1	
13.20 - 13.50	***Patient-Generated Health Data and Healthcare Information Fiduciaries*** *Dr Paul R. DeMuro, Attorney - Nelson Mullins Riley and Scarborough, Florida, USA.*	09
	Theme 1 - Data, Governance and Privacy	
13.50 - 14.10	***Privacy-respecting Approach to Data Analytics for Health Care Purposes*** *Mr Marc van Lieshout and Dr André Boorsma, Senior Researchers - Netherlands Organisation for Applied Scientific Research (TNO), The Netherlands.*	13
14.10 – 14.30	***Data Governance in International Neuroscience Research*** *Mr George Ogoh, Research Fellow - Centre for Computing and Social Responsibility, De Montfort University, UK.*	15
14.30 – 14.50	***Data Protection, Privacy and Data Sharing for Health: Ethics and Legal Framework*** *Dr Joana Namorado, Medical Doctor and Project Manager - Fraunhofer Institute for Biomedical Engineering, Germany.*	19
14.50 – 15.05	**Coffee Break (15 mins)**	
	Theme 2 - Digital Health and Communities	
15.05 -15.25	***Digital Health Europe: Collaborating with People and Patients Through Platforms and Spaces*** *Ms Diane Whitehouse, Director - The Castlegate Consultancy, UK.*	22
15.25-15.45	***Digitalisation in Maternity: Improving the patient experience*** *Dr Jasmine Leonce, Consultant Obstetrician, Clinical Director (Obstetrics) - Lister Hospital, UK.*	25
15.45-16.05	***Exploring The Societal Impacts of Emerging eHealth Technologies with High-School Students*** *Mr Richard Taylor, Subject Manager - International Baccalaureate Organisation, UK.*	27
16.05-16.45	**Discussion/Panel Session (40 mins)**	
16.45-17.00	**Roundup of the day**	
19.30	**Dinner**	

Day 2 – Friday, 8th November 2019

TIME	SESSION	Page Number
9.30-9.40	Welcome and introduction to the day	
	KEYNOTE - 2	
09.40 – 10.10	***Digital Healthcare and the Ethical Principle of Dual Effect Applied to Digital Healthcare*** *Prof Harold Thimbleby, Professor of Computer Science – Swansea University, UK.*	29
	Theme 3 - AI in Healthcare	
10.10 – 10.30	***Big Data, Analytics and AI for Health – Benefits and Risks: A Short History*** *Mr John Crawford, Managing Director and Health IT consultant – CrawfordWorks, UK.*	32
10.30 – 10.50	***Artificial Intelligence for Health and Care in the EU*** *Dr Carlisle George, Associate Professor and Barrister – Middlesex University, UK.*	34
10.50 – 11.10	***Standards for the Ethics of AI*** *Mr Brian Tranter, ANEC representative on IEC, UK.*	37
11.10 – 11.30	**Coffee Break (20 mins)**	
11.30 – 11.50	***How Data-driven AI can Benefit from Formalized Knowledge to Become More "Explainable": An Experience from Medical Process Mining*** *Prof Stefania Montani, Professor of Computer Science, University of Piemonte Orientale Alessandria Area, Italy.*	38
11.50 – 12.10	***The Language of Automated Medicine*** *Mr Chris Zielinski, Visiting Fellow – University of Winchester, UK.*	40
12.10 – 12.50	**Discussion/Panel Session 1 (40 mins)**	
12.50 – 14.00	**LUNCH**	
	Theme 4 - Emerging Technologies in Healthcare – Blockchain and mHealth	
14.00 – 14.20	***Quality Audits with Blockchain for Healthcare in the UK*** *Dr Ian Mitchell, Associate Professor and Ms Sukvhinder Hara, Senior Lecturer – Middlesex University, UK.*	42
14.20 – 14.40	***A Novel Privacy Framework for mHealth when Managing Chronic Diseases*** *Mr Farad Jusob, PhD Student - Middlesex University, UK.*	44
14.40 – 15.00	***A Comprehensive Information Security Framework for mHealth and Prototype Development*** *Ms Nattaruedee Vitanwattana, PhD Student – Middlesex University, UK.*	47
15.00 – 15.20	***Securing eHealth and mHealth: Moving from Frameworks to Prototypes*** *Dr Glenford Mapp, Associate Professor – Middlesex University, UK.*	50
15.20 – 16.00	**Workshop Overview, Discussion, Next Steps, Farewell (40 mins)**	

Patient-Generated Health Data and Healthcare Information Fiduciaries

Dr Paul R. DeMuro[a] and Dr Hannah K. Galvin[b]

[a] Attorney - Nelson Mullins Riley and Scarborough, Florida, USA.
(paul.demuro@nelsonmullins.com)

[b]Medical Director of Informatics - Lahey Health, Massachusetts, USA.
(hannah.galvin@lahey.org)

Abstract
Patient-Generated Health Data is proliferating along with the commercialization of such data. Given the proclivity to re-identify de-identified or pseudonymized data, it is becoming increasingly important to protect the privacy of individuals who have such patient-generated health data. The authors suggest some guidelines for holders of these kinds of Patient-Generated Health Data to be treated as healthcare information fiduciaries.

Introduction
Patient-Generated Health Data are health-related data created, recorded, or gathered by or from patients or caregivers. [1] They can include "health history, symptoms, biometric data, treatment history, lifestyle choices, and other information—created, recorded, gathered, or inferred by or from patients or their designees . . . to help address a health concern." [2] Patient-Generated Health Data can be transmitted electronically to a patient's care team or to clinical researchers; in the process, the company hosting the data, e.g., the vendor of the data tracking device or third-party tracker, may also have access. [3]

Ownership of these data are a complex and often poorly understood concept and regulated by different laws in different jurisdictions. Many different stakeholders may claim ownership, including a patient's physician, medical institution, or a third party. [4] In certain cases, data can be owned by one entity and controlled by another. [5]

Commercialization of healthcare data
Protected health information (PHI), including Patient-Generated Health Data, is being commercialized by big data brokers [6], sold to pharmaceutical companies, and used for clinical research. Companies, such as Facebook, make billions of American dollars as a result of the use and monetization of people's data. [7] [3] Trust and privacy are important for health care and the use of personal health services. [8] The current eCommerce rules cannot really be appropriately applied in this area. [8] A small number of organizations hold massive amounts of data relating to countless individuals, with little policy or legal oversight to regulate their utilization. [9] The law has not kept up with the technological advances and one wonders whether it even can. [10]

Although the General Data Protection Regulation [11] appears to be the most comprehensive and stringent protection measure, it leaves ambiguity in certain areas, e.g. the terms "data protection by design and default" can be ambiguous as to their full implications. [12]

It is sometimes thought that the de-identification or pseudonymization of a person's data might protect an individual's privacy. The United States Department of Health and Human Services even provides Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Information Portability and Accountability Act (HIPAA) Privacy Rule. [13] Reidentification of data is not just theoretical but has been demonstrated in several contexts. [14] [15] [16] Machine learning can utilize physical activity data to improve reidentification schemes of both adults and children. [14] As data sets increase in volume and number, it should become easier to re-identify data. [17] Saying that data are anonymous does not make it so. [18]

Privacy also has a time-dependent element. [19] That is, over time, more data about an individual might be compiled and aggregated, and thus, data that might not be possible to identify today may be identified in the future, especially throughout the life-course of individuals. Although each person may have a different opinion on what he or she deems to be sensitive about his or her health information, most appear to lack awareness of the privacy risks. [19] [20] However, the privacy risks should be assessed in some form and in the context of any patient consents. In addition, certain regulatory schemes treat certain sensitive healthcare information such as mental health, genetics, sexual data, biometrics, and disability in a special or protected manner.

Although an individual may technically consent to share these data, that consent is often not knowing and informed. In a 2015 study of 600 of the most common mobile health (mHealth) apps, fewer than one-third had privacy policies and two-thirds of these (or approximately 20 percent of the total) did not specifically address the app itself, and those that did, often required college-level literacy to understand. [21] Of mHealth apps that do have appropriate "Terms and Conditions" attached to them, most are so onerous that few people read them before downloading the app. [22] Users of mHealth apps are almost always obliged to agree to the terms of use that the underregulated commercial entities supplying the services require. [23] However, the General Data Protection Regulation prohibits making consent to data processing a precondition of service unless the service is dependent on it. [11]

Healthcare Information Fiduciaries

As a result, the holder of the individual's data stands in a special position - arguably one of trust - with respect to that individual. The holder of the data or the entity that controls it can seek to monetize or profit from that individual's data by sharing the data to the detriment of the individual. Ariel Dobkin suggests "that many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries through their customers and end-users." [24]

A fiduciary has a legal obligation to act in the best interest of its client. [25] One might consider an entity that holds personal health data such as Patient-Generated Health Data as a healthcare information fiduciary. [3] As such, a detailed analysis of which entities might be considered to be a healthcare information fiduciary might be instructive. In making such a determination, one might consider the type of information that the would-be healthcare information fiduciary might possess, how the information was generated, who were the intended recipients, to whom was the information transmitted, and what was the purpose of the transmittal. [3]

Ownership of the data can be a complicated question. In healthcare, different parts of a medical record might arguably be owned by different individuals and/or entities, and different jurisdictions may have different laws on the subject: for example, the ownership of Patient-Generated Health Data may be viewed differently from notes a provider entered directly into a medical record. [4] More pertinent questions might be: Who or what entity(ies) control(s) the Patient-Generated Health Data? Are the data considered to be de-identified or pseudonymized, and if so, what are the prospects for their re-identification? What type of consent(s) have been provided by the individual who generated the data?

Further inquiries as to whether a person or entity might be considered a healthcare information fiduciary might include: What benefits might the holder of the data derive from the data, particularly from a pecuniary perspective? What other benefits might inure from that data, e.g. for the public good? Is the company benefiting from the use of the data commercial in nature? What is the value of the data economically, socially, and/or to society?

Assuming the holder and/or user of the data should be treated as a healthcare information fiduciary, should the traditional fiduciary standards apply? Should the standards be adapted to the healthcare context? Should policy-makers, regulators and legislators seek to develop laws and/or guidance that codifies these fiduciary standards and provide for enforcement mechanisms, if such standards are violated? How should such standards be developed and enforced? How do legislators account for the

global commercial environment and cross-border transactions? Should there be private rights of action? If so, what?

Conclusion

The use of Patient-Generated Health Data for commercial purposes by entities which hold such data is becoming increasingly commonplace. Efforts at re-identifying de-identified or pseudonymized data are increasingly successful. Patient consents often appear meaningless.

As a result, it may be time to start treating entities which hold Patient-Generated Health Data or control such data, such as vendors, online service providers, cloud companies, medical device and tracking device manufacturers, app hosting entities and smart phone manufacturers as healthcare information fiduciaries. These healthcare information fiduciaries might provide the attendant protections to the individuals whose data is being used.

Endnotes

[1] Patient Generated Health Data. The Office of the National Coordinator for Health Information Technology (ONC) [Internet]. Available at: https://www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data. Accessed: 12 Sept 2019.

[2] Shapiro M, Johnston D, Wald J, Mon D. Patient-Generated Health Data. White Paper. Office of Policy and Planning Office of the National Coordinator for Health Information Technology. RTI International. 2012 Apr.

[3] DeMuro PR, Petersen C. Managing Privacy and Data Sharing Through the Use of Health Care Information Fiduciaries. Stud Health Technol Inform. 2019 Aug 9;265:157-162. doi: 10.3233/SHTI190156.

[4] Sharma R. Who Really Owns Your Health Data? Forbes Technology Council. 2018 Apr 23.

[5] Singh R. Ownership of Healthcare Data in the IOT Era, Part 2. Compliance Today, 2019 Jul.

[6] Leetaru K. How Data Brokers and Pharmacies Commercialize Our Medical Data. A1 and Big Data. Forbes. 2 Apr 2018.

[7] Hill S. Should Big Tech Own Our Personal Data? Opinion. WIRED. 2019 Feb 13.

[8] Ruotsalainen P, Blobel B. Trust Model for Protection of Personal Health Data in a Global Environment. MedInfo 2017. EdInfo 2017: Precision Healthcare Through Informatics. International Medical Informatics Association (IMIA) and IOS Press. 2017.

[9] Kostkova P, Brewer H, de Lusignan S, Fottrell E, Goldacre B, Hart G, Koczan P, Knight P, Marsolier C, McKendry RA, Ross E, Sasse A, Sullivan R, Chaytor S, Stevenson O, Velho R, Tooke J. Who Owns the Data? Open Data for Healthcare. Frontiers in Public Health. Perspective. 2016;4(Art.7).

[10] Brous E. Legal Considerations in Telehealth and Telemedicine. American Journal of Nursing. 2016;116(No.9).

[11] Regulations:
Regulation (EU) 2016/679 of the European Parliament and of the Council. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Repealing Directive 95/46/EC (General Data Protection Regulation). 2016 Apr 27.

[12] Flaumenhaft Y, Ben-Assuli Ofir. Personal health records, global policy and regulation review. Elsevier, B.V. Health Policy. 2018 May 7.

[13] Rule:
Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. U.S. Department of Health and Human Services. 2012 Nov 26.

[14] Na L, Yang C, Lo C, Zhao F, Fukuoka Y, Aswani A. Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets from which Protected Health Information has been Removed with Use of Machine Learning. JAMA Network/OPEN/Health Policy. 2018;1(8):e186040. Doi:10.1001/ jamanetworkopen.2018.6040.

[15] Sweeney L. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

[16] Rocher L, Hendrickx JM, and de Montjoye Y-A. Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications. 2019;10(1):3069. Available at: https://doi.org/10.1038/s41467-019-10933-3
[17] McCoy Jr. TH, Hughes MC. Preserving Patient Confidentiality as Data Grow Implication of the Ability to Reidentify Physical Activity Data. JAMA Network OPEN. 2018; 1(8):e186040. Doi:10.1001/ jamanetworkopen.2018.6040.
[18] Sweeney L, von Loewenfeldt M, Perry M. Saying It's Anonymous Doesn't Make it So: Re-identifications of "Anonymized" Law School Data. JOTS Technology Science. 2018 Nov 13.
[19] Sanchez D, Viejo A. Personalized Privacy in Open Data Sharing Scenarios. Abstract. Universitat Rovira I Virgili, Department of Computer Engineering and Mathematics, UNESCO Chair in Data Privacy. ISSN:1468-4527. 2017 Jun 12.
[20] Young SD. Social Media as a New Vital Sign: Commentary. J Med Internet Res. 2018 Apr 30;20(4):e161.
[21] Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc. 2015 Apr;22(e1):e28-33.
[22] Sharp M, O'Sullivan D. Mobile Medical Apps and mHealth Devices: A Framework to Build Medical Apps and mHealth Devices in an Ethical Manner to Promote Safer Use – A Literature Review. 2017 European Federal for Medical Informatics (EFMI) and IOS Press. 2017.
[23] Schairer CE, Kseniya Rubanovich C, Bloss CS. How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent in the Age of Mobile Health? AMA J Ethics. 2018;20(9):E864-872. doi:10.1001/amajethics.2018.864.
[24] Dobkin A. Information Fiduciaries in Practice: Data Privacy and User Expectations. *Berkeley Technology Law Journal*. Vol.33:1:2018. Available at: https://doi.org/10.15779/Z38G44HQ81.
[25] Balkin JM. Information Fiduciaries and the First Amendment. UC Davis Law Review. Vol. 49, No. 4. 2016 Apr.

Privacy-respecting Approach to Data Analytics for Health Care Purposes

Mr Marc van Lieshout[a] and Dr André Boorsma[b]

[a]Senior Researcher/Advisor - Molecular and Systems Biology,
Netherlands Organisation for Applied Scientific Research (TNO), The Netherlands
(Marc.vanlieshout@tno.nl)

[b]Senior Researcher/Consultant - Strategy and Policy
Netherlands Organisation for Applied Scientific Research (TNO), The Netherlands
(andre.boorsma@tno.nl)

Background

People tend to collect ever more health related data on their smart phones. A 2018 survey indicates that seven out of ten smart phone users have at least one health app installed (Lieshout et al., 2018) (p. 19). This can be an app that keeps track of the person's daily number of steps, nutritional intake during a day, or glucose levels – thus enabling granular dosing of insulin. These examples can be multiplied by some 250,000 other examples of available health related apps.

The data from these apps can be combined with health data collected by care givers or in electronic patient records. Making these data available through personal healthcare environments enables individuals to keep track of their data. One of the issues of relevance to people that bring all their health and lifestyle data together in such a personal healthcare environment is in what way, and to what degree, data subjects should be able to exercise some kind of control over the processing of these data.[1]

The five Ps

Within TNO, research is oriented towards making these data available for research purposes. Given the changing role of individuals in the healthcare process, the availability of large data sets, the on-going personalisation of health care, the power of predictive analytics, and the ability to not only focus on cure but especially to promote healthy lifestyles in order to prevent diseases, TNO is focusing on promoting **five Ps**: how to promote **P**ersonalised health care, that enacts **P**articipation by individuals, changing the perspective from cure to **P**revention, using available technology to **P**redict health outcomes and doing this all in a **P**rivacy-respecting manner.

Focusing on the five Ps is not an easy endeavour. A large set of problems need to overcome. TNO has taken up the challenge to help developing a data sharing ecosystem that fulfils the requirements posed by these Ps.

First, TNO sees large potential in having individuals contribute actively to handling their health data. This is **Participation** in **Personalised health care**. Health data cooperatives, such as Patients like me (Tempini and Teira, 2019) may present one of the ways to move forward in combining the five Ps that we embrace. Data cooperatives may offer inroads into a number of stubborn challenges that are visible in the long-standing tradition of clinical trials and medical-scientific research. We are focusing on seeking the engagement of the data subjects in combination with data analytics to promote the personalisation of health, including a healthy lifestyle. This would then become a means to support an efficient use of resources in health care settings.

Second, we focus on **prevention** rather than on cure. Healthy lifestyles prolong healthy life circumstances, and – in particular situations – can even help to reduce the symptoms of specific diseases, such as diabetes.[2] This implies that a larger set of data needs to be aggregated and analysed, with all the potential privacy issues that may arise from this.

[1] The General Data Protection Regulation uses the concept 'data subject' to identify the person whose personal data are processed.

[2] https://www.aafp.org/news/health-of-the-public/20131024diabetesintervene.html, accessed 2-10-2019.

That is our third point: health data belong to the special categories of data identified in the General Data Protection Regulation (GDPR) (2018).[3] Processing of these data is prohibited unless a special ground for exemption can be invoked. Healthcare research and scientific research both offer exceptions to the prohibition to process health data.

TNO has made an in-depth analysis of the requirements that the GDPR poses in this respect. We use the outcomes of this analysis to develop an approach in which legal, technical, organisational and societal implications of processing personal data are brought together and build up a trust framework that guides the approach. This trust framework is labelled RESPECT4U[4] (Lieshout and Emmert, 2018).

RESPECT4U framework

RESPECT4U is a generic framework developed by TNO. It offers an encompassing approach to the responsible processing of personal data.

Seven guiding principles form the cornerstones of the RESPECT4U framework: they underpin the acronym of the framework itself – **R**esponsible processing of data, while **E**mpowering data subjects in ways that are compatible with their rights, offering a **S**ecure data processing environment, adopting a **P**ro-active attitude in which privacy by default and design are systematically unpacked, being aware of the **E**thical issues that come with new data analytics, having an eye for **C**osts and benefits that come along with new data processing practices, and opting for an approach that promotes **T**ransparency on the side of the organisation responsible for the processing of the data.

Each of the guiding principle enables a specific set of measures that can be adopted to develop a privacy-respecting data processing ecosystem. The ecosystem builds on state-of-the-art technological solutions that become available for the secure processing of health data. It is in line with the GDPR, since it takes into account the various obligations that the GDPR imposes on data controllers.

Overview of the presentation

In our contribution, we will present an outline of the approach we are elaborating today for organising **research activities which make use of Real World Data**, i.e. data that are collected by means of commercially available tools and applications, combined with data from electronic health records where possible. We engage data subjects in a meaningful manner. For parts of the processing activities, patient consent is not needed and even not advised. We have come up with an alternative solution that avoids resorting to informed consent (when this should not be invoked) while still guaranteeing data subjects' participation and engagement. In order to prevent the circulation of data that are collected in different places, we are looking for ways to implement the Personal Health Train (Soest et al., 2018), a new conceptual approach. The train enables federated learning that is inherently secure and helps to organise privacy principles.

References

Lieshout, M. v., Chen, M., Karanikoloava, K., Timan, T., Bolchi, M., Costenco, P., . . . Alberti, S. (2018). *Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems - Final Study Report regarding Safety of health, lifestyle and wellbeing apps* (TNO 2019 R10103). Brussels: European Commission

Lieshout, M. v., and Emmert, S. (2018). *Privacy as Innovation Opportunity*. Paper presented at the Annual Privacy Forum, Barcelona.

Soest, J. v., Sun, C., Mussmann, O., Puts, M., Berg, B. v. d., Malic, A., ... (2018). Using the Personal Health Train for Automated and Privacy-Preserving Analytics on Vertically Partitioned Data. *European Federation for Medical Informatics (EFMI) and IOS Press*, 5. doi:10.3233/978-1-61499-852-5-581

Tempini, N., and Teira, D. (2019). Is the genie out of the bottle? Digital platforms and the future of clinical trials. *Economy and Society, 48*(1), 77-106. doi:10.1080/03085147.2018.1547496

[3] See GDPR, art 9, that addresses the general prohibition to process special categories of personal data unless specific exemptions can be invoked.

[4] See https://pilab.nl/what%20the%20pi.lab%20can%20do%20for%20you/respect4u.html

Data Governance in International Neuroscience Research[1]

Mr George Ogoh[a], Prof Bernd Stahl[a], Dr Damian Okaibedi Eke[a],
Dr Simisola Akintoye[b], Dr William Knight[a] and Dr Inga Ulnicane[a]

[a]Centre for Computing and Social Responsibility, De Montfort University, UK
(george.ogoh@dmu.ac.uk; bstahl@dmu.ac.uk; damian.eke@dmu.ac.uk;
william.knight@dmu.ac.uk; inga.ulicane@dmu.ac.uk)

[b]Leicester De Montfort Law School, De Montfort University, UK
(simi.akimtoye@dmu.ac.uk)

Introduction

Medical research is governed by a number of universal principles like those laid out in the 1964 Declaration of Helsinki[1] which stipulates them as 'ethical principles for medical research involving human subjects, including research on identifiable human material and data'[2]. However, the details of its implementation vary from country to country. One reason for this is differences in legislation and agency policy which have an impact on the conduct of research and level of protection accorded research subjects. For example, since 2008 the U.S. Food and Drug Administration (FDA)[3] only abides by the 1989 version of the Declaration rather than the more recent 2013 version and some have suggested this allows U.S companies to cut ethical corners when working abroad[4,5]. In the arena of international collaboration in medical research, such differences raise issues for data governance because they affect how data is shared and used, what data is shared, and with whom data can be shared.

With an ever-growing appetite for collaborative research, one of the areas where issues relating to data governance can easily arise is in the field of neuroscience. Neuroscientists have come to realise that the complexity of the human brain and nervous system mean that, only by working collaboratively together, they can in good time hope to successfully unravel the mysteries of the brain for the benefit of humankind. However, it is not yet clear what rules will govern neuroscientific research collaborations particularly when it spans across national borders and what level of protection will be in place for research subjects when their data is shared across multiple geographic regions. In this era of big neuroscience data[6] and large brain projects[7–13], this type of collaboration raises serious concerns as the principles governing data collection, sharing, and use vary from country to country. This position paper therefore highlights how growing collaborations in neuroscience projects may raise important questions for data governance that needs to be addressed.

The evolving landscape of neuroscientific collaboration

In the last decade, the call for neuroscientific collaborations has become more urgent due to growing alarm at societies' inability to deal with neurological and psychiatric disorders and the increasing costs of these conditions[14–16]. For example, Ivinson[17] pointed out that more collaboration between basic, translational and clinical neuroscience will improve effectiveness, productivity, and efficiency. Similarly, Belin and Rolls[18] maintained that multi-disciplinary and multi-systems collaborations offer unique opportunities for knowledge expansion and open up new ways of thinking. As researchers in this scientific environment come to the realisation that much benefit can be derived from collaboration between the different branches of neuroscience, while closely working with other relevant disciplines, an overwhelming volume of data[19] is being generated and shared.

[1] This project/research has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under the Specific Grant Agreement No. 785907 (Human Brain Project SGA2).

A marked increase in collaborations between institutions, both at the national and international levels, with a view to sharing data and resources is also being witnessed. Two examples that are particularly relevant are:

- The European Union-led Human Brain Project (HBP), which seeks to 'create ICT based scientific research infrastructure for brain research, cognitive neuroscience, and brain-inspired computing'[20], is made up of over 100 partner institutions in 19 countries[21]. As well as being international, it is also interdisciplinary as it includes such disciplines as cognitive neuroscience, neuro-informatics, medical informatics, brain simulation and neurorobotics; and transdisciplinary covering computing, informatics, mathematics, as well as philosophy [22].
- The International Brain Initiative (IBI), an international brain research collaborative project that is still at the proposal stage[23]. It is a consortium of seven large brain[24] research initiatives that includes the already international (European) Human Brain Project. The six other brain projects that make up the IBI are the Australian Brain Initiative, the Canadian Brain Research Strategy, the China Brain Project, the Korean Brain Initiative, Japan's Brain/MINDS, and the U.S. Brain Initiative.

The vision of the IBI to 'catalyse and advance ethical neuroscience'[23] indicates that like the HBP[25], ethics is at the core of the project. Yet, differences in ethical principles and legislation (in terms of data protection, generation, sharing, use, and maintenance) that each of these large brain projects conform to, may have ramifications on their ability to collaborate effectively. These differences are not well known and the significance for 'ethical neuroscience' within the IBI remains a relatively unexplored arena. It is important therefore, to understand the consequences of such collaboration from an ethical perspective and to anticipate the potential for unintended consequences.

Methodology

For this paper, a narrative review[26–28] has been done to provide a synthesis of collaboration in neuroscience research and how data governance issues might arise. The paper has provided a background understanding of the nature of collaborations in this area and how it raises interesting questions for data governance in the international arena. One important issue that has been pointed out here pertains to differences in legislation and policies governing scientific research and data protection in the various jurisdictions where the largest brain initiatives[24] are based and how this might have consequences for data governance in neuroscientific collaboration.

This outcome will form the basis for a more systematic review that will include doctrinal analysis of legal literature and scoping review of peer-reviewed literature. Hutchinson[29] describes doctrinal analysis as a 'critical conceptual analysis of all relevant legislation and case law to reveal a statement of the law relevant to the matter under investigation. It will be centred on legislation on scientific research and data governance policies relevant to the seven brain research projects that make up the IBI. This will be done to highlight important pieces of legislation and policy that have an impact on international research collaboration. The scoping review on the other hand, will focus on two popular academic databases i.e. Scopus[30] and PubMed[31]. These are widely available databases that index a variety of subject areas and research themes. The objective will be to highlight current practices in terms of scientific research and data governance and the problems arising from such practices.

Conclusion

The complexities of neuroscientific research mean that, at different levels, international collaborations are bound to grow. Even so, the prospect for collaborations between big brain initiatives raise interesting questions and dilemmas for data governance (which need to be addressed because of differences in national legislations and agency regulations). This assessment will help to limit the potential for negative output of such large international projects as the IBI and for their outputs to have unintended societal implications. It will also propose a set of policy recommendations for data governance to enable 'ethical' international neuroscience collaborations. At the heart of such data governance will be clear ethical principles that will enable the maximisation of the societal benefits of big brain projects. This output will help resolve potential ambiguities and address procedural concerns about international data transfers within the proposed initiative.

References

1. World Medical Association. World Medical Association Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects. *JAMA*. 2013;310(20):2191. doi:10.1001/jama.2013.281053
2. Largent EA. Recently proposed changes to legal and ethical guidelines governing human subjects research. *J Law Biosci*. 2016;3(1):206-216. doi:10.1093/jlb/lsw001
3. Food and Drug Administration. Acceptance of Foreign Clinical Studies. U.S. Food and Drug Administration. http://www.fda.gov/regulatory-information/search-fda-guidance-documents/acceptance-foreign-clinical-studies. Published April 20, 2019. Accessed September 30, 2019.
4. Normile D. Clinical Trials Guidelines at Odds with U.S. Policy. *Science*. 2008;322(5901):516-516. doi:10.1126/science.322.5901.516
5. Goodyear MDE, Lemmens T, Sprumont D, Tangwa G. Does the FDA have the authority to trump the Declaration of Helsinki? *BMJ*. 2009;338(apr21 1):b1559-b1559. doi:10.1136/bmj.b1559
6. Fothergill T, Knight, Stahl B, Ulnicane I. Responsible Data Governance of Neuroscience Big Data. *Front Neuroinform*. https://www.frontiersin.org/articles/10.3389/fninf.2019.00028/full.
7. Amunts K, Knoll AC, Lippert T, et al. The Human Brain Project—Synergy between neuroscience, computing, informatics, and brain-inspired technologies. *PLOS Biol*. 2019;17(7):e3000344. doi:10.1371/journal.pbio.3000344
8. Jeong S-J, Lee H, Hur E-M, et al. Korea Brain Initiative: Integration and Control of Brain Functions. *Neuron*. 2016;92(3):607-611. doi:10.1016/j.neuron.2016.10.055
9. Richards LR, Michie PT, Badcock DR, et al. Australian Brain Alliance. *Neuron*. 2016;92(3):597-600. doi:10.1016/j.neuron.2016.10.038
10. Okano H, Mitra P. Brain-mapping projects using the common marmoset. *Neurosci Res*. 2015;93:3-7. doi:10.1016/j.neures.2014.08.014
11. Poo M, Du J, Ip N Y, Xiong Z-Q, Zu B, Tan T. China Brain Project: Basic Neuroscience, Brain disease and Brain-Inspired computing. *Neuronview*. 2016;92(3):591-596.
12. Martin CL, Chun M. The BRAIN Initiative: Building, Strengthening, and Sustaining. *Neuron*. 2016;92(3):570-573. doi:10.1016/j.neuron.2016.10.039
13. Illes J, Weiss S, Bains J, et al. A Neuroethics Backbone for the Evolving Canadian Brain Research Strategy. *Neuron*. 2019;101(3):370-374. doi:10.1016/j.neuron.2018.12.021
14. Fineberg NA, Haddad PM, Carpenter L, et al. The size, burden and cost of disorders of the brain in the UK. *J Psychopharmacol Oxf Engl*. 2013;27(9):761-770. doi:10.1177/0269881113495118
15. Thakur KT, Albanese E, Giannakopoulos P, et al. Neurological Disorders. In: Patel V, Chisholm D, Dua T, Laxminarayan R, Medina-Mora ME, eds. *Mental, Neurological, and Substance Use Disorders: Disease Control Priorities, Third Edition (Volume 4)*. Washington (DC): The International Bank for Reconstruction and Development / The World Bank; 2016. http://www.ncbi.nlm.nih.gov/books/NBK361950/. Accessed October 1, 2019.
16. World Health Organization, ed. *Neurological Disorders: Public Health Challenges*. Geneva: World Health Organization; 2006. https://www.who.int/mental_health/neurology/neurological_disorders_report_web.pdf.
17. Ivinson AJ. Collaboration in Translational Neuroscience: A Call to Arms. *Neuron*. 2014;84(3):521-525. doi:10.1016/j.neuron.2014.10.036
18. Belin D, Rolls A. Collaboration in neuroscience: the young PI perspective. European Journal of Neuroscience. 2016;43(9):1123-1127. doi:10.1111/ejn.13226
19. Ferguson AR, Nielson JL, Cragin MH, Bandrowski AE, Martone ME. Big data from small data: data-sharing in the 'long tail' of neuroscience. *Nat Neurosci*. 2014;17(11):1442-1447. doi:10.1038/nn.3838
20. Aicardi C, Reinsborough M, Rose N. The integrated ethics and society programme of the Human Brain Project: reflecting on an ongoing experience. *J Responsible Innov*. 2018;5(1):13-37. doi:10.1080/23299460.2017.1331101
21. Amunts K, Ebell C, Muller J, Telefont M, Knoll A, Lippert T. The Human Brain Project: Creating a European Research Infrastructure to Decode the Human Brain. *Neuron*. 2016;92(3):574-581. doi:10.1016/j.neuron.2016.10.046

22. Amunts K, Knoll AC, Lippert T, et al. The Human Brain Project—Synergy between neuroscience, computing, informatics, and brain-inspired technologies. *PLOS Biol*. 2019;17(7):e3000344. doi:10.1371/journal.pbio.3000344
23. International Brain Initiative. About us. https://www.internationalbraininitiative.org/about-us. Published 2019. Accessed August 8, 2019.
24. Rommelfanger KS, Jeong S-J, Ema A, et al. Neuroethics Questions to Guide Ethical Research in the International Brain Initiatives. *Neuron*. 2018;100(1):19-36. doi:10.1016/j.neuron.2018.09.021
25. Human Brain Project. Ethics and Society. Social Ethical Reflective. https://www.humanbrainproject.eu/en/social-ethical-reflective/. Published 2019.
26. Noble H, Smith J. Reviewing the literature: choosing a review design. *Evid Based Nurs*. 2018;21(2):39-41. doi:10.1136/eb-2018-102895
27. Cronin P, Ryan F, Coughlan M. Step-By-Step Approach. *Br J Nurs*. 2008;17:38-43. doi:10.4135/9781446213971.n6
28. Mitchison D, Mond J. Epidemiology of eating disorders, eating disordered behaviour, and body image disturbance in males: a narrative review. *J Eat Disord*. 2015;3(1):20. doi:10.1186/s40337-015-0058-y
29. Hutchinson T. The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law. Taekema S, ed. *Erasmus Law Rev*. 2016;3. doi:10.5553/ELR.000055
30. Scopus. Scopus - Document search. https://www2.scopus.com/search/form.uri?display=basic. Published 2019. Accessed October 2, 2019.
31. PubMed. US National Library of Medicine National Institutes of Health. https://www.ncbi.nlm.nih.gov/pubmed/. Published 2019. Accessed October 2, 2019.

Data Protection, Privacy and Data Sharing for Health: Ethics and Legal Framework

Dr Joana Namorado

Medical Doctor and Consultant - Fraunhofer Institute for Biomedical Engineering, Germany
(joananamorado1@gmail.com)

Introduction

There is no denying that the public trusts companies and social media with personal data. We share data we don't even know we are sharing. We believe that the data we provide is as "consumers". Preference of one brand of a sweet drink over another isn't a big deal. We don't mind being "bombarded" by advertisements in exchange for a service; what we don't realize is that we ARE the service or the product.

In a way, we "trust" companies because we see them as frivolous. Common perception, possibly limited to some cultures, tends to show we distrust administrations. Perhaps our attitude towards public administrations is a measure of the respect and importance we confer on them. So, we hesitate to share as citizens. After all, the public administrations actually can force their will on us, track, and enforce behaviours. Imprison and in well known cases, intern, persecute and kill.

An example of this is the data collected by health services of all types. Some people take it for granted that the health information gathered on them is shared. In some cases, even, we are outraged if we learn that it isn't. There are countries where people assume that, for example, biopsies are taken and are publicly owned. Or rather, that the information garnered from these biopsies is for the common benefit. Other countries refuse to participate in the social effort. This conflict, though, only becomes acute when there are different attitudes prevalent in one and the same jurisdiction. The case in point is the ownership of HeLa[1], the woman versus the sombre history of her cells. But what is clear is that both clinical medicine and population health sciences:

1. Have always been information-intensive (observe-compare).
2. Assumed consent of its users.
3. Are utilitarian in nature – Presumed to be for the general benefit.

Privacy or science?

Privacy and confidentiality have never been seen as barriers to sharing and analysis. Biomedical research relies on the work of trusted entities, be they persons or institutions – to collect very personal information. So why has it become an issue now?

How do we find a solution? Perhaps we can start with a transparent responsible attitude on the part of the researchers and collectors of this information?

This means that the purpose of the collection must be clearly stated, and a declaration and explanation of the purpose, and how the data are protected. In other words – an inbuilt ethics code of conduct, intrinsic to the system of collection and use of data, and the defence of the original owners against intrusion. That is the responsibility of the collector and of the researcher.

Ethics in recording and banking of information must be intrinsic and systemic. Security, de-identification, anonymization, and pseudonymization are not always possible. For example, smart collection of electricity usage data can be usable for tracking of people, their habits, or demographics. That means also that the collectors of data should be trusted gatekeepers to access it. Is there a "tech reply" to this conundrum? Sharing data (and more than any other, health data) is a citizenship obligation, what can we offer as security, so as to build trust.

Consent, privacy, confidentiality, stigma, etc. are not abstract concerns. Quite the opposite, they have practical and real results. Data in Health Systems, properly handled, helps humanity to face real

[1] Skloot, Rebecca (2010), The Immortal Life of Henrietta Lacks*, New York City:* Random House*, p. 2,* ISBN 978-1-4000-5217-2

challenges. The only barrier is perception and trust. Exception made for cases of extreme unsocial behaviour, or misunderstanding of what is their role as social apes, most people will willingly share data. But in return, researchers and data collectors need to acknowledge that:

1. Demonstrating compliance is an important factor for trust. So, comply with common legislation-local sanctions through local authorities.
2. Compliance sets the stage for data ethics in science, which means one should be: Proactive, preventive, thoughtful.

About personal data?

Personal data is any information relating to an identified or identifiable natural person ("data subject"). Art. 4(1) GDPR)[2] – But can technology provide an answer? Can we find a lock and key mechanism, or a safe deposit for our secrets, can we mirror the "Room of Requirements" with technological magic?

Another issue is that we use very imprecise nomenclature. What do we mean when we say what it is that we do? We look for images and metaphors to explain what we do. And then the metaphor becomes the reality. We are poorly served by imprecise terminology.

1. "Cloud" is not always water vapour.
2. "Data" is used variously; is it "information" or "knowledge" or "classification" or more?
3. Meta-data and merged databases make identification simple or irrelevant.
4. Algorithms diagnose patterns and open the door to manipulation.
5. "Share" what? Name and date of birth or abstract signs, symptoms, lab parameters, genes?
6. "Big Data" is imprecise and is over-used as a term.

Let's be precise

We can introduce precision and meticulous attention to responsible research. We can define terms and what our responsibilities are. This can affect one's research; so how and who takes care of it? A talented amateur or a seasoned professional?

What is the role of ethics? It illuminates the force, the scope and limitations of rights. And it identifies and balances conflicting duties and corresponding rights; it identifies and justifies duties to the other and to one's surroundings. Privacy is not an absolute right, but it must be balanced against other rights and the rights of others (including a "right to benefit from science"). Rights can be erroneously invoked by individuals, who will be quick to invoke the opposite when it suits them.

To balance health and privacy, some premises must be taken care of. The population must trust smart laws and policies, and there has to be recognition of social duty. It must become clear that learning healthcare systems are a public health analogue of "duty to treat".

Trust is generated by management and governance, by people and systems taking care to balance quality of data, consent, privacy, and an ex ante review of the ethics of projects and of entities. Within the research community, we have to build the consultation capacity for risk communication, decisions under uncertainty. And we have to be conscious and open about patients' duties to share, and be open to consider concepts of "tacit" and "non-explicit" consent. Also, to be quite explicit that all people – not just investigators – have duties to share.

The counter-balance is to continuously improve the security of one's own data collections.

To earn trust is a continuous task. Health of all "e" types are indeed – challenge and opportunity. But an ethics oversight for data in research also constitutes a challenge. Because processing data is complex and new, anonymization techniques are complex, sometimes unavailable and poorly understood.

Technical innovation is fraught with promise, but includes pitfalls and dangers. That is why it is exciting. That is why we have a duty to defend it. Ethics is a great tool to do this. Ethics isn't grinding teeth and

[2] The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA

hand-waving. It is a systematic smart attention to detail and balance. But the return is huge, as ethics protects good research and supports researchers. Provides traceability, ownership.

Ethics, from the start, will permit a confident use of new mining algorithms, ensure ownership, safeguard principles, standards and regulations, and create conditions, or even, a new context, opportunities for science and new products to share.

Science requires imaginative solutions to facilitate use of data for healthcare. Transforming ethics into an honest broker. Unromantic? Perhaps, but essential.

Digital Health Europe: Collaborating with People and Patients Through Platforms and Spaces[1]

Ms Diane Whitehouse

[a]Director - The Castlegate Consultancy, UK.
[b]Principal eHealth Policy Consultant – EHTEL, Belgium
([a]diane.whitehouse[@]thecastlegateconsultancy.com, [b]diane.whitehouse[@]ehtel.eu)

Introduction

In just a few weeks from today, a new European Commission is due to start its work: it contains a number of high-profile areas of activity relating to the ***Digital Age***, ***Health***, and the ***Internal Market***. A key activity in the field of digital health will be the creation of a ***European Health Data Space***. Its role will be "*to promote health-data exchange and support research on new preventive strategies, as well as on treatments, medicines, medical devices and outcomes. As part of this,* [...] *citizens* [should] *have control over their own personal data*" [1].

By ***sharing data and exchanging data***, improved research could take place in a wide variety of health-related and care-related fields. Purely as examples, one could envisage improvement in knowledge – which might serve policy-makers and health decision-makers – about how health and care systems function together with how they face growing public health challenges such as chronic conditions, infectious diseases, or the effects of ageing throughout the life-course. Associated with this data-sharing are implications with regard to good personal control of individual ***citizens***' own health data [2].

Clearly, the future focus is to be on data exchange for the purposes of prevention, cure, and care. Yet, if this is to be one of tomorrow's future scenarios, it implies at the same time ***a greater responsibility, awareness, and ultimately*** **control** on the part of European citizens with regard to the uses to be made of their health and care data.

This Middlesex University eHealth workshop includes, at its core, questions about ***building responsibility, awareness, and control***. Several colleagues' presentations concentrate on the control of **data**. More pertinent to this presentation are the challenges implicit in wide ranges of ***people, including patients, collaborating together to better understand European health, care, and technology policy directions***, contribute to them, and generally become more involved in their own, and others', decisions about ***data-sharing and data-exchange*** in the fields of health and care.

The digitisation of health and care and DigitalHealthEurope

The digitisation of health and care – as well as of many other services, both public and private – is taking off throughout the European Union. Fundamentally, it is about encouraging digital health and care innovation in the Digital Single Market.

The ***Communication on digital transformation in health and care*** [3], was issued by the European Commission in April 2018. It focuses on the digital transformation of health and care in the Digital Single Market, empowering citizens, and building a healthier society.

The Communication is especially influential in drawing attention to three important future priorities in health and care:

[1] The Digital Health Europe project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826353.

- ***Citizens' secure access*** to and sharing of health data across borders.
- ***Better data*** to advance research, disease prevention and personalised health and care.
- ***Digital tools*** for citizen empowerment and person-centred care.

In January 2019, the ***DigitalHealthEurope*** coordination and support action [4] was launched to provide coordination and support for the future priorities identified in the Communication. Among other activities it focuses on getting more people informed about and involved in these priorities. It has formed three ***multi-stakeholder communities*** in order to support digital innovation and transformation in health and care. Each community focuses on one of the ***three priorities*** of the Communication.

Three multi-stakeholder communities, tools, and coverage including twinning

These three communities act as ***fora for discussion****:* they generate the creation of even larger communities. They are based on an electronic platform [5]. However, they also use a wide range of other ***instruments*** in order to spread the news about the progress of digital health and care in Europe. These include activities and events at workshops and conferences, and others such as focus groups, electronic meetings and conference calls, surveys, and the sharing of documents for the purposes of commenting. Their activities often follow a World Café style approach [6].

The ***tools and techniques*** that the communities use in their gatherings are varied. They cover activities that are intended to obtain the highest possible impact for the digital transformation of health and care in Europe. Example tools include the SCIROCCO (digital) maturity tool on scaling-up integrated care [7]; the MOMENTUM tool for telemedicine [8]; personas [9] and user scenarios [9]; and co-production techniques [10].

The way in which ***digital technologies can support health and care concerns*** ranges widely across, for example, community support, civic participation, healthy homes and buildings, healthy outdoor spaces and built environments, social inclusion, transportation, and work – expressed in the so-called "WHO flower" [11] and similar sector-spanning work covering the social determinants of health by Dahlgren and Whitehead [12]. Of key importance is the ***policy directions*** to be taken in any of these domains, and the ***involvement*** and ***engagement*** of European citizens in these discussions.

All three of the communities are supporting efforts towards:

- The creation of ***partnerships for large-scale deployment of digital*** **solutions** for person-centred integrated care.
- The analysis of ***high-impact scenarios*** for the digital transformation of health and care.
- ***Twinning to promote successful large scale innovations*** that can act as essential foundations ("building blocks") for scaling-up digital initiatives in health and care.

The last of these three efforts – twinning schemes – is among one of the most currently emphasised initiatives in the European Union at the present time. Twinning with other sites and organisations is seen as a collaborative, yet concrete, way of ***improving the expansion of the use of digital technologies in health and care organisations*** around Europe [13]. In this sense, patients, citizens, and both health and care systems and organisations can all benefit.

Towards a summary and conclusions

Fifteen years after the concept was first developed, today it feels as if the ***European e-Health area*** is coming to fruition [14]. It is doing so in a manner that brings together people, patients, and also health and care organisations in a pro-active and collaborative spirit. The discussion spaces and collaboration platforms being created are not only digital and electronic, as befits the end of the second decade of the 21st century. They also seek to maintain the humanity and social interaction given special importance when speaking of ***fora for discussion*** *and* ***discussion spaces****.* In overview, an even wider variety of tools and techniques for communicating and collaborating is foreseen. In this way, humaneness, care and sensitivity are all likely to be maintained, at the same time as people and patients around the globe benefit from ever more widespread digital technologies and communities.

References and useful links

[1] Mission letter to Stella Kyriakides, Commissioner-designate for Health: https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-stella-kyriakides_en.pdf, Brussels, 10 September 2019.
[2] This text draws on a 13 September 2019 news item published by EHTEL: https://www.ehtel.eu/media-room/latest-news/62-forging-ahead-on-the-digital-age-in-europe-the-importance-of-digital-health-data-health-and-care.html
[3] COM(2018) 233 final. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society.* 2018. https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering Brussels. (25.04.2018)
[4] DigitalHealthEurope coordination and support action: https://digitalhealtheurope.eu
[5] DigitalHealthEurope multi-stakeholder communities: https://digitalhealtheurope.eu/communities.html
[6] Brown J., Isaacs, D. and the World Café Community. 2005. *The World Café: Shaping our Future through Conversations that Matter*.
[7] SCIROCCO/the SCIROCCO tool: www.scirocco-project.eu and https://www.scirocco-project.eu/scirocco-tool/
[8] MOMENTUM/the MOMENTUM tool, including 18 critical success factors: http://www.telemedicine-momentum.eu/wp-content/uploads/2015/07/MomentumLeaflet2015-BlueprintInANutshell.pdf
[9] Blueprint personas and user scenarios: https://ec.europa.eu/eip/ageing/blueprint_en
[10] Guidelines for user co-production in standards. https://progressivestandards.org/wp-content/uploads/2019/01/Guidelines-for-user-co-production-in-standardisation-PROGRESSIVE-D9.1_20181210.pdf
[11] World Health Organization (WHO). 2007. *Global Age-friendly Cities: A Guide*. WHO: Geneva http://www.who.int/ageing/age_friendly_cities_guide/en/
[12] Dahlgren G, Whitehead M. 1991. *Policies and Strategies to Promote Social Equity in Health*. Stockholm, Sweden: Institute for Futures Studies.
[13] Fourteen current twinning schemes ranging from full to partial adoption of digital health and care solutions can be seen at: https://digitalhealtheurope.eu/twinnings.html
[14] COM(2004)356 final (2004) *e-Health – making healthcare better for European citizens: An action plan for a European e-Health area*. Luxembourg: European Commission (30.4.2004)

Digitalisation in Maternity: Improving the patient experience

Dr Jasmine Leonce[a] and Ms Janet Harris[b]

[a] Consultant Obstetrician, Clinical Director Obstetrics - East and North Herts NHS Trust (jasmine.leonce@nhs.net)

[b]Audit Midwife - East and North Herts NHS Trust

The National Maternity Review, Better Births, (NHS England, 2016) emphasised the importance of coordinated care across the whole system delivering maternity care. Introduction of Local Maternity Systems (LMSs) as part of Better Births (NHS England, 2019a) initiated local maternity providers to work together to share ideas and best practice as well as formulate a LMS digital strategy that would enable seamless access to data. As a consequence, women have a choice in what care they access and where, across the local maternity system in which they live. The data detailing their maternity care should be accessible without the need for the woman to repeat her pregnancy history or require duplication of data entry. Better Births advocates empowering women by allowing them access to electronic health records tailored to their own needs (Carter, 2018). The NHS Long Term Plan asserts that "by 2023/24 all women will be able to access their maternity notes and information through their smart phones or handheld devices" (NHS, 2019b).

There is a vast amount of pregnancy-related information available digitally, but women are unsure whether the information is accurate or if it reflects UK maternity health care. This lack of certainty impacts safety and experience (NHS England, 2016). Evidence suggests that maternity services have invested in 'work arounds' as the market has failed to meet their digital information needs (Health Technology Newspaper, 2019). Also, it has been suggested anecdotally that maternity services are starting to move away from apps in search of other more innovative digital solutions such as websites, text messaging, online group support, social media, and telehealth.

The Health Systems Support Framework (NHS England, 2019b) gives access to accredited suppliers of information technology at the leading edge of health and care system reform; however the focus is on Enterprise-wide Electronic Patient Record (EPR) Systems which do not meet the needs of some specialist areas such as maternity care. The Wachter report (2016) highlighted the important role that clinicians must play in making new digital initiatives a success. Challenges within digital working in maternity include: workforce readiness, resources, infrastructure, equipment, interoperability, technology, and enabling mobile working.

In 2018, NHS Digital conducted a Maternity Digital Maturity Assessment (DMA) which indicated a wide variation across England in terms of how well maternity services are using digital technology (NHS Digital, 2018). The focus of any maternity digital strategy must consider the 'perspective of the end users' and any recommendations must support solutions which are co-produced by service users and clinicians. Digital solutions must provide a joined-up experience for women and families, where they only have to tell their story once and feel confident that up-to-date information is flowing safely between care settings and chronological stages of development or pathways of care.

Whilst digital innovation is recommended by Better Births, the human factors elements, lack of connectivity, and lack of dedicated budgets continue to pose a challenge to UK-wide implementation. Digital innovation is by no means the solitary tool to improving women's experience of pregnancy and childbirth. The future, however, remains bright as the appetite for digital advancement is ever present among medical and midwifery staff, and women.

References

Carter, R. (2018). Electronic Maternity Care Records - what women want?
https://digital.nhs.uk/blog/transformation-blog/2018/electronic-maternity-care-records

Health Tech Newspaper (HTN) (2019), Basildon Hospital launches maternity app
https://www.thehtn.co.uk/2019/08/08/basildon-hospital-launches-maternity-app/

NHS Digital (2018) Maternity DMA Report – Digital Maturity Assessment of Maternity Services in England (2018)
https://www.england.nhs.uk/publication/maternity-dma-report-digital-maturity-assessment-of-maternity-services-in-england-2018/

NHS England Better Births: Improving outcomes of maternity services in England- A Five Year Forward View of maternity care (2016)

NHS England (2019a), Implementing Better Births.
https://www.england.nhs.uk/mat-transformation/implementing-better-births/

NHS England (2019b), Health Systems Support Framework
https://www.england.nhs.uk/hssf/

NHS (2019), NHS Long Term Plan, Chapter 3: Further progress on care quality and outcomes.
https://www.longtermplan.nhs.uk/online-version/chapter-3-further-progress-on-care-quality-and-outcomes/a-strong-start-in-life-for-children-and-young-people/maternity-and-neonatal-services/

Wachter, R. (2016) Making IT work: harnessing the power of health information technology to improve care in England.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf

Exploring The Societal Impacts of Emerging eHealth Technologies with High-School Students

Mr Richard Taylor[a] and Ms Sandra Stark[b]

[a]Subject Manager - International Baccalaureate Organisation, UK.
(richard.taylor@ibo.org)

[b]Chief Examiner (ITGS) - International Baccalaureate Organisation, UK.

The constant evolution of digital technologies poses many societal challenges. The International Baccalaureate (IB) is attempting to provide learners with the skills to flourish in this constantly changing world. Its mission statement, which provides a framework for developing these skills states " … These [IB] programmes encourage students across the world to become active, compassionate and lifelong learners ……." [1] The mission statement is exemplified by the Learner Profile that aims to develop learners who have the following attributes; inquirers, knowledgeable, thinkers, communicators, principled, open-minded, caring, risk-takers, balanced and reflective [2].

The IB Diploma Programme (DP) is aimed at pre-university students and offers around 25 subjects. A number of subjects offer case studies but only those in Computer Science, in the Experimental Sciences group, and Information Technology in a Global Society (ITGS), in the Individuals and Societies group, give students the opportunity to research a specified scenario for one year.

Authoring case studies for a diverse global cohort of teachers and students is challenging. Each year the authoring team must select a scenario that allows the underpinning digital technologies to be presented at an appropriate depth as well as sufficient opportunities for independent and sustained research. Each case study has a standardized format and is linked to an externally assessed examination.

The 2017 Case Study, *Wearable technology - Kita Health Tech (KHT)* was released on the 31st May 2016. This case study was based on a fictitious scenario where four Indonesian students created a company (KHT) with a mission statement to ".. improve the lives of people using wearable technology in as many ways as possible". The scenario originated from a conversation about one of the author's smart watches. Was he walking the 'required' 10,000 steps each day? What else did companies, such as Google and Amazon, know about him?

As soon as the case study was released, collaborative spaces were set up by teachers. Two examples of collaborative spaces were the ITGS Facebook group [3] managed by Barbara Stefanics and the Taipei European School site [4] managed by James Greenwood. The ITGS Facebook group creates a space for both teachers and students to discuss the case study. However, it is predominantly teachers who use this resource and create their own in-house collaborative spaces for their students, such as the one created by James Greenwood.

James Greenwood is the Head of Computing and Media at Taipei European School. He explains "... When teaching the case study in ITGS, I provide my students with a number of curated starting points as a beginning for inquiry into the topic. This is intended to prevent the students going off-course at the start of their exploration". He continues "… We have an in-class discussion about what makes a good source, comparing the curated examples with others from less reliable sources. [This allows] ... the students to collect their own resources, using social bookmarking tools or collaborative working tools such as Padlet or Google Docs." James sets up a website that acts as a focal point for the research, arranges (if possible) for guest speakers on the topic, and devises activities for students to carry out primary research (for example, testing out the accuracy of the sports watches that many students wear).

Case studies are critically important for ensuring the timeliness of IB courses, i.e., that they do not become too quickly outdated. In the subject areas such as ITGS that discuss digital technologies, change is constant, and it is almost impossible to predict what technologies may exist towards the end of the lifetime of a seven-year long course. However, case studies provide more than just the acquisition of subject specific knowledge, they also offer a framework that helps develop the skills of students in preparing them for lifelong learning.

In the future, digital technologies will continue to evolve. In response, individuals, organizations and governments, such as Japan with its Society 5.0 initiative [5], will need to make informed decisions about how these evolving technologies might be best utilized.

References

[1] IBO. (2005 - 2019). Mission. Retrieved October 16, 2019, from https://www.ibo.org/about-the-ib/mission/.
[2] IBO. (2005 - 2019). Mission. Retrieved October 16, 2019, from https://www.ibo.org/about-the-ib/mission/.
[3] Stefanics, B. (2016, May 31). Case Study 2017: Wearable Technology – Kita Health Tech (KHT). Retrieved October 16, 2019, from https://www.facebook.com/groups/940292289416791/.
[4] Greenwood, J. (2017, May 31). ITGS Paper 3 2018. Retrieved October 16, 2019, from http://itgs.org/wp-login.php?redirect_to=/course-info/getting-started/paper-3-2018/.
[5] UNESCO. (2019). Latest news on japan-pushing-ahead-society-50-overcome. Retrieved October 16, 2019, from https://en.unesco.org/news/japan-pushing-ahead-society-50-overcome-chronic-social-challenges.

Digital Healthcare and the Ethical Principle of Dual Effect Applied to Digital Healthcare

Prof Harold Thimbleby

See Change Fellow in Digital Health – Swansea University, UK.
(harold@thimbleby.net)

Introduction

It is well known that drugs have side-effects: curing one health problem often causes or exacerbates other problems. Aspirin, for instance, helps reduce the risk of stroke, but it also unavoidably increases the risk of bleeding, a problematic side-effect for people with stomach ulcers. I myself am on rituximab, which manages my neuropathy: it has numerous unwanted side-effects (NICE, 2019) with different probabilities, including some that are fatal. The only side-effects I have had so far are unwanted infections, but the side-effects will get worse over time. On balance, though, the unwanted side-effects are justified by the benefits.

Fatal side-effects take us into an ethical minefield, although side-effects of any severity raise ethical issues even if they are without such a sharp focus.

A dramatic dilemma with regard to side-effects arises when giving pain killers that are also known to accelerate death. It is uncontentious that giving a pain killer to *cause* death is murder, and is considered unethical; on the other hand, giving a pain killer to manage or reduce pain is good, and is considered to be ethical. Where, then, on the ethical spectrum, is giving so much legitimate pain killer that death is expected to be inevitable? Or, where does it lie on the ethical spectrum when a patient pleads for death as release to insufferable pain? How would using an off-label drug affect the ethical arguments? ("Off-label use" is when a drug is not used for the purposes it was rigorously evaluated and regulated to manage.)

It is tempting to think of drug side-effects as being an impersonal property of drugs; that is, the side effects are a property of the drug. Furthermore, particularly since the Thalidomide scandal, clinical trials are performed so the properties of drugs are well-known and evidence-based. Yet anyone prescribing a drug unavoidably makes an ethical decision: does its benefit for the patient (at this dose; under these circumstances) out-weigh its risks for *this* patient? In other words, the ethical questions are not a property of the drug alone.

It is important to note that ignoring an ethical decision does not simply free a decision from the ethical domain. For instance, in hindsight a doctor may realise they ignored a patient's drug allergy: if there is harm to the patient, then this is professional misconduct, and it properly comes under ethical scrutiny, even though the pressure of work at the time of prescription meant that the ethics were ignored (Johnson and Haskell, 2015).

The Principle of Dual Effect

The ***Principle of Dual Effect*** is an established ethical principle, but in the clinical context it means that giving a drug (or performing any other intervention) with the intention of curing, while managing the risk but not intending it, is ethically acceptable.

The Principle of Dual Effect has been developed rigorously. It has clear criteria: not just that the good effects must out-weigh the bad effects, but there must be diligence taken to minimize potential harms. Specifically (Cavanaugh, 2016):

- the nature of the act is itself good, or at least ethically neutral;
- the agent (e.g., the healthcare professional) intends a good effect;
- the agent identifies all bad effects;
- the agent does not intend the bad effects as a means to some good;

- the agent does not intend the bad effects as an end in themselves;
- the good effects outweigh the bad effects in circumstances sufficiently grave to justify causing the bad effects;
- the agent exercises due diligence to minimize the bad effects;
- ***Where all these conditions are met, the action under consideration is ethically permissible despite a bad result.***

In hindsight, after a bad outcome occurs, it may be very hard to establish that adequate prior ethical assessment was performed with due diligence according to the standards of the Principle. In particular, when an outcome is so bad that it motivates a formal investigation, hindsight bias may motivate simplistic blame, by labelling an act as unethical even when it was not apparently so at the time. ("Hindsight bias" is that after an incident, it is easy to see clear causal chains that were unknown at the time of the event.) Hindsight bias makes it seem that a poor outcome was much more predictable than it was at the time. Here's one way to put it: before the incident, a particular bad effect had an estimated probability sufficiently less than one for the risk to be ignored or considered worthwhile. However, now the bad effect has happened, the probability is — with no analysis required! — exactly one, since it has as a matter of fact actually happened.

A brief but very powerful applied discussion of the Principle of Dual Effect can be found in Rana Awdish's page-turner, *In Shock: How Nearly Dying Made Me a Better Intensive Care Doctor* (Awdish, 2017). Awdish is a doctor and was a patient on the "receiving end" of the Principle.

The Principle of Dual Effect can be traced back to Thomas Aquinas's *Summa Theologica*, written some time over the period 1265–1274AD. The aim of the present paper is now to consider digital healthcare in the light of this practical ethical principle.

Digital healthcare

Digital systems have bugs; computers and apps regularly crash, sometimes losing or corrupting our work. Digital systems used in healthcare are not immune to bugs, and the bugs in digital healthcare systems may precipitate patient harm. Sometimes bugs can directly cause patient harm, as in bugs in radiotherapy machines, medical apps, and pacemakers (Thimbleby, 2020).

With digital healthcare, then, the Principle of Dual Effect looms large, at least in principle if not explicitly. A developer writes a program intended to help staff or patients, but any program may have bugs, which could have counter-productive effects. The Principle of Dual Effect implies that it is ethical to develop digital healthcare *provided* that the risks — e.g., of bugs, cybersecurity challenges, design faults and their effects — are properly managed and that *explicit steps have been taken to minimise those risks*.

Developing healthcare software without considering and mitigating digital risks is unethical.

That claim, I hope, sounds uncontentious.

Yet, on closer analysis, there are critical differences in digital health – when compared to conventional domains (such as prescribing drugs) – that make the application of the Principle in digital healthcare raise novel and urgent issues. These issues include the following (unfortunately this paper is not long enough to consider each in detail): Software is very complex; The business models underpinning software are disruptive; Software has unknown (and therefore unmanaged) side-effects; The software business is reluctant to evaluate software to avoid side-effects; Software can only be proved correct not tested (testing can only find bugs; proof shows bugs are absent); Software is widely promoted as a "side-effect free solution" to healthcare inefficiencies; Software skills and resources in healthcare lag behind the current best practice (e.g., to understand modern software engineering techniques); Digital healthcare is poorly regulated — not least because it is too slow to react to new digital innovations such as artificial intelligence (AI), machine learning (ML), cybersecurity, blockchain, and more. Historically weak regulation is often used to justify the reluctance of industry and healthcare sectors to address the related problems.

Arguably, all digital healthcare is off-label use, because no "label" equivalent to the rigour applied to drugs is available. There is a widespread blame culture that deflects from examining digital trade-offs in detail — software's complexity dissuades informed analysis.

A bug, of course, is not a side-effect as such, but is, potentially, the cause of a side-effect. The problem is that even knowing that there is a bug does not directly help anticipate what its side-effects might be. For example, a bug causing numerical errors in an infusion pump may turn a drug dose from 1 mg to 1.0 mg, which has no clinical impact, but the same bug could change 1 mg to 10 mg, and such an out-by-ten error is likely to have a clinical effect.

For the success of legal negligence claims, it is critical whether an outcome is *foreseeable*. With a drug, normal side-effects are documented (and are available in standard publications, such as *British Pharmacopoeia*), but side-effects of digital systems are not documented — the culture is that digital systems do not have side-effects, and even when bugs are known, their side-effects are generally unknown. What is foreseeable is that a digital system may be wrong, and therefore the clinician should have double-checked any results used. For example, the potential that 1 mg and 10 mg are confused due to a bug means that diligence is required to check accuracy.

Unfortunately, awareness of digital bugs is very low and, as Thimbleby (2020) shows, bugs may also affect the systems logs (e.g., entering a dose of 1 mg delivers 10 mg to the patient due to a bug *and is logged as* 10 mg), thus corrupting the digital evidence (Mason and Seng, 2017), potentially creating the false impression the error was the clinician's fault.

The deceptive simplicity of blaming healthcare staff, and its apparent success (e.g., in courts after patient harm — see Thimbleby 2018), entrenches the culture of ignoring the ethical complexity of digital healthcare. Unfortunately, blaming staff creates a second victim (the patient is the first victim; the staff member, the second) — the health professional may be harmed as a result of the simplistic blame culture. Indeed, too many doctors and nurses commit suicide as a result of the ethically-shallow perfection culture (such as the "blame game" — see ISMP 2019) widespread in healthcare and society, especially in the mainstream media.

Conclusion

Thoughtfully managing drug side-effects is widely recognised as a professional and as an ethical obligation in healthcare: indeed, so widely that explicit discussions of ethics are rarely needed, at least outside of academia and court rooms. This paper has shown that the Principle of Dual Effect is a precise ethical statement, and one that is very relevant to digital healthcare. The Principle raises – in a clear light – many priorities that help to clearly identify and start to resolve the ethical issues raised by digital healthcare.

References

R. Awdish, 2017. *In Shock: How Nearly Dying Made Me a Better Intensive Care Doctor*, Penguin.

T. A. Cavanaugh, 2016, *Double-Effect Reasoning: Doing Good and Avoiding Evil*, p36, OUP.

ISMP [US Institute of Safe Medication Practices], 2019, Another Round of the Blame Game: A Paralyzing Criminal Indictment that Recklessly "Overrides" Just Culture, https://www.ismp.org/resources/another-round-blame-game-paralyzing-criminal-indictment-recklessly-overrides-just-culture

J. Johnson and H. Haskell, 2015. *Case Studies in Patient Safety*, Jones and Bartlett Learning.

S. Mason and D. Seng, 2017, *Digital Evidence*, 4th ed., School of Advanced Study, University of London.

NICE [UK National Institute for Health and Care Excellence], Rituximab, 2019. https://bnf.nice.org.uk/drug/rituximab.html#sideEffects

H. Thimbleby, 2018. "Misunderstanding IT: Hospital cybersecurity problems in court," *Digital Evidence and Electronic Signature Law Review*, 15:11–32. http://journals.sas.ac.uk/deeslr/article/viewFile/4891/4841

H. Thimbleby, 2020, *Fix IT*, OU.

Big Data, Analytics and AI for Health: Benefits and Risks

Mr John Crawford

Founder and CEO – CrawfordWorks, Digital Health Consulting, UK.
(john.crawford.works@gmail.com)

Introduction

The significance of Big Data and the application of analytics are not new concepts in healthcare. Since the 1850s, doctors, mathematicians and statisticians have been using mortality registers to try to understand the cause and spread of infectious diseases, and the correlation between health risks and observed health outcomes in populations over extended periods. Pioneers including William Farr and John Snow analysed registers and maps in the mid-19th century to identify the origin and spread of cholera in London[1]. A century later, in the 1950s, Austin Bradford Hill and Richard Doll used statistical analysis to connect smoking with lung cancer[2]. There have been many other examples since then, such as the Framingham Heart Study and Nurses' Health Study[3]. These have led to the development of algorithms which can be used to assess the risk of developing a disease, to a greater or lesser extent. The number of ways in which technologies can assist with this analysis has increased dramatically.

Developments in the late 20th century

An early healthcare example in 1972 was the development by Stanford University of MYCIN, an expert system to support antibiotic prescribing[4]. However the expert systems developed in this era did not find mainstream acceptance, and the following two decades have been described as the 'AI winter'. Now, with the growth in capability of AI, some of these advances are finding their way into the practice of medicine and the delivery of healthcare. This is taking place across a broad range of domains, from clinical decision support, medical image interpretation, and diagnostics, to the management of health challenges such as diabetes and heart arrythmias. This progress has been recognised in the broadcasting media, with an explosion of news stories about the potential benefits and possible risks of these developments.

In the 1990s, the rapid growth in processer power led to the possibility of computational algorithms being applied in areas which, up until then, were considered to be the exclusive realm of human beings. This shift started with the famous chess challenge in which IBM's Deep Blue took on, and defeated, Grand Master Garry Kasparov[5]. Since then, there has been an evolution in programmed systems, exemplified by Deep Blue, and a more recent move towards systems that can be trained by human experts, or which can even train themselves, using novel computing models and methods such as Neural Networks and Deep Learning. Topical examples include Google's 'Alpha Go' and 'Alpha Go Zero' projects[6,7].

Recent developments

After several 'false starts' from the 1950s to the 1980s, we now appear to be entering an era of high innovation and fast growth in the adoption of Artificial Intelligence (AI). Today's thrust in AI is now being driven by the huge growth in computer power and storage; availability of digital datasets that can be used to train and validate AI systems; and advances in computer science which have accelerated the capabilities of machine learning.

Gartner, for example, has attempted to position many of these innovations on Gartner's AI Hype Cycle[8]. Many books have been written which explore the driving forces behind this technological revolution, and the impact they will have for all of us[9,10,11]. Questions have been raised around the issues of **privacy**, **efficacy**, **safety**, **transparency**, **liability** and **legal redress**.

AI: benefits and risks

The introduction of AI into the fields of medicine and healthcare in particular needs particularly **careful consideration**, given the many possible benefits combined with the potential for harm.

This presentation explores this evolution in AI, and places AI's benefits and risks – as it is already being deployed in healthcare – in a broader context.

For example, AI has **established a positive reputation** in the area of diagnostics, especially when this involves analysis of medical images such as X-rays, CT scans, retinal images, and dermatological photographs. Well trained systems can be much faster than humans, and can identify features in images which even the best clinicians miss. The system developed by DeepMind, in use at Moorfields Eye Hospital, London, which diagnoses diseases of the eye[12] illustrates the potential. Many other possible applications are being investigated, in areas such as spotting early signs of dementia from brain scans, predicting risks of kidney failure, detecting prostate cancer, and performing robotic surgery.

At the same time, there are clearly **risks** associated with AI systems using Neural Networks and Deep Learning methods, resulting in a 'black box' system (where it can be difficult to determine how a diagnostic result has been reached). There is also the question of transferability, where algorithms have been optimised to perform a specific task ('narrow AI'), but may appear overly confident when presented with examples that they have not seen before. The quality and extent of the training dataset is crucial in avoiding this challenge.

Other applications of AI, such as the use of chatbots or avatars to provide triage services to citizens, such as the GP at Hand service provided by Babylon Health[13], may increase access to healthcare information and advice. However, there are questions about how much trust can be placed in these services compared to a consultation with a human being, and there may be unseen biases in the training data leading to incorrect advice being given. If this bias leads to harm, who can be held accountable? There is also the question about who 'owns' the data provided by the users of such services, and how that data will be used or potentially misused.

A further question is about how to evaluate the quality and safety of these systems against best current practice. Do the systems need to be almost perfect to be accepted, or is it sufficient for them to be at least as good as human beings at performing their work? As is well understood in medicine, human error will occur. What is a 'good enough' error rate or safety record, for AI systems, and how do we measure this?

References and useful links

1 - https://www.ncbi.nlm.nih.gov/pubmed/15313591
2 - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2038856/
3 - https://www.framinghamheartstudy.org
4 - https://en.wikipedia.org/wiki/Mycin
5 - https://www.scientificamerican.com/article/20-years-after-deep-blue-how-ai-has-advanced-since-conquering-chess/
6 - https://ai.googleblog.com/2016/01/alphago-mastering-ancient-game-of-go.html
7 - https://www.nature.com/articles/nature16961
8 - https://www.gartner.com/smarterwithgartner/top-trends-on-the-gartner-hype-cycle-for-artificial-intelligence-2019/
9 - Hello World, Hannah Fry - Transworld Publishers Ltd, ISBN: 9781785175763
10 - Superintelligence, Nick Bostrom – Oxford University Press, ISBN: 9780198739838
11 – Life 3.0, Max Tegmark – Penguin Science/Technology, ISBN: 9780141981802
12 – https://www.moorfields.nhs.uk/content/latest-updates-deepmind-health
13 – https://www.forbes.com/sites/bernardmarr/2019/08/16/the-amazing-ways-babylon-health-is-using-artificial-intelligence-to-make-healthcare-universally-accessible/

Artificial Intelligence for Health and Care in the EU: Developing ethical and legal frameworks

Dr Carlisle George

Associate Professor and Barrister – Middlesex University, UK.
(c.george@mdx.ac.uk)

Introduction

This presentation focuses on the increasing importance of Artificial Intelligence (AI) in the digital transformation of health and care in the European Union (EU), and changes to the regulatory (ethical and legal) environment. The presentation gives a selected historical overview of recent actions by the European Commission on AI and health and care, as well as the progress made in some aspects of ethical and legal frameworks.

Background

Several recent European Commission Communications and reports have referred to the importance of AI for Europe.

In April 2018, the European Commission issued the *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society* [1]. One of three priorities identified, was the need to promote digital tools for person-centred health and care. A key enabling technology identified for digital health was AI. For example, use of AI and data analytics was cited to "help design and test new healthcare products, provide faster diagnosis and better treatments" and, together with computer modelling and simulation, to develop "digital patient" predictive approaches.

Another *Communication on Artificial Intelligence for Europe* [2] in April 2018 stated that AI was one of the most strategic technologies of the 21st century and argued that the EU should lead the way in developing and using AI. The Communication noted that some AI applications may raise new ethical and legal questions (e.g. related to liability or biased decision-making), hence there is a need to develop AI in an appropriate ethical and legal framework. Such a framework must respect EU values and fundamental rights, ethical principles (e.g. accountability, transparency) and must ensure compliance with relevant laws (e.g. data protection). As part of the way forward, the Communication listed many future initiatives on AI. Initiatives related to legal and ethical issues included: implementing the General Data Protection Regulation (GDPR) to enhance personal data protection; drafting AI ethics guidelines; and issuing guidance on existing product liability rules. The drafting of guidelines and guidance were tasked to relevant High-level Expert groups.

In December 2018, the Commission issued a *Communication on a Coordinated Plan on Artificial Intelligence* [3] that outlined EU-level activities to maximise the benefits of AI for all Europeans. Regarding the development of a suitable ethical and legal framework for AI, the activities proposed included: the drafting of guidance on the implementation of a Product Liability directive; the drafting of AI ethics guidelines involving making "ethics by design" a key principle at the start of the design process of AI products and services; providing strong "cybersecurity" to prevent hacking or manipulation of AI algorithms (or the data processed by them) and to ensure customer safety; ensuring the suitability of existing regulations relating to data protection and privacy, consumer protection, competition law by design, and intellectual property; and ensuring fairness, transparency and accountability of decision-making by (AI – machine learning) algorithms.

Some Developments in EU Ethical and Legal Frameworks to address AI

This section explores in greater detail some of the issues that the European Commission has determined are important for the satisfactory development of AI. It starts with ethical guidelines and then discusses some legal issues namely data protection, product liability, intellectual property and cybersecurity.

Ethics Guidelines for AI

On 8 April 2019, the EU's High-Level Expert Group on AI presented its "Ethics Guidelines for a Trustworthy AI" [4]. The guidelines' main aim is to promote "trustworthy AI", which has three components that must be met throughout an AI system's life cycle: (i) It must be *lawful* – there must be compliance with relevant laws and regulations; (ii) it must be *ethical* – adhering to ethical principles and values and (iii) it must be *robust* – both technically and socially (i.e. to prevent unintentional harm). The guidelines set out seven key requirements that must be met by an AI system to be trustworthy, namely: Human agency and oversight; Technical robustness and safety; Privacy and Data governance; Transparency; Diversity, non-discrimination and fairness; Societal and environmental well-being; and Accountability. The new guidelines will be essential to the design, development and use of AI technology in health and care.

Data Protection

In May 2018, the General Data Protection Regulation (GDPR) [5] came into force in the EU to regulate the processing of personal data [6] and protect fundamental rights (e.g. the right to privacy, human autonomy and non-discrimination). Among many provisions, it contains several high-level data protection principles, obligations on data controllers and processers, subject's rights, and enhanced protection for "sensitive data" such as medical data. These provisions impact the development and use of AI in cases where personal data is processed. Some important provisions include: the need for a legal basis for processing (collection and any use of) personal data; being fair and transparent when processing personal data; collecting the least amount of data needed for a specific purpose; keeping data accurate and up-to-date; retaining data only for as long as is necessary for the purpose collected; assessing the impact of processing on data subjects; complying with subjects' rights (including not to be subject to a decision based solely on automated processing, including profiling); and requiring data protection by design and data protection by default.

The nature of AI systems and processes presents many challenges with regard to compliance with many provisions of the GDPR. One example is the nature of machine learning and data analytics means that machine learning algorithms are optimised by the use of extensive amounts of data for training. This is in contrast to the GDPR, which mandates data minimisation – i.e. collecting the least amount of data as possible for a specific purpose. Another example is that the requirement for "transparency" under the GDPR can be impossible to meet in AI technologies, since human beings may not understand (and hence be able to explain to a data subject) how machine learning algorithms work (how they make decisions) both before they are deployed and after they have been optimised by training on data. A third example is that subjects' rights, such as the "right of erasure" of personal data, may be impossible to achieve after personal data has been used in combination with numerous other data to train algorithms.

Product liability

Product liability refers to liability (the responsibility of a manufacturer or vendor) for injury or damage to a consumer arising from a defective product. In the EU, the Product Liability Directive 85/374/EEC applies to any product marketed in the European Economic Area[7]. Since the Directive came into force, there have been numerous technological developments. Notwithstanding that the Directive is technology-neutral, new technologies such as AI bring unanticipated consequences. One such issue is the debate on whether AI (i.e., self-learning) technologies that are autonomous and capable of unpredictable and automated decision-making (without the influence of human beings) should be treated as a legal personality (separate from their creators) and therefore be held liable for their actions [8]. In light of some of these issues and other challenges, the European Commission's "Expert Group on liability and new technologies" has been organised into two subgroups to determine how best to further develop the 1985 Product Liability Directive. One subgroup is tasked with drawing up guidance on the Directive (e.g. providing clarity on concepts such as 'product', 'defect', 'damage', and advising on any reforms needed). The other subgroup is tasked with assessing the implications of emerging technologies for liability frameworks at national level and at European level. At the time of writing (November 2019), the Commission has not yet issued its official guidance on the Product Liability Directive (although it was originally due in mid-2019).

Intellectual Property (Copyright) law

A major aspect of AI is the use of Text and Data Mining (TDM) which involves the copying of large amounts of material (texts and data) in order to perform electronic analysis to reveal patterns or relationships. The use of TDM may involve material protected by copyright and, hence, copyright law impacts on TDM. In light of the importance of TDM to AI, and the need of AI to access large datasets to extract knowledge, the Commission included a mandatory exemption for TDM in the 2019 Directive on Copyright in the Single Market [9] (Articles 3 and 4 to be enacted by Member States). This has important implications for enabling information search/retrieval, research, and the development of intelligent applications in the medical sector (including the pharmaceutical industry).

Cybersecurity

As noted previously, the European Commission identified the need for strong cybersecurity to protect AI algorithms, data, and people. In June 2019, the European Cybersecurity Act [10] came into force. It complements the GDPR (requiring security when processing personal data) and the EU Network and Information Security Directive (NIS Directive) [11] which focuses on the protection of critical national infrastructure. Among other provisions, it mandates: (i) new tasks for the EU Agency for Cybersecurity (ENISA) that include increasing cooperation at EU level, handling cyber attacks at the request of EU Member States, and helping with EU-coordination in the event of large-scale attacks or crises; and (ii) the development of an EU-wide cybersecurity certification framework to certify information and communication technology (ICT) products, processes and services for compliance with specified cybersecurity requirements.

Conclusion

The advent of AI to the digital transformation of health and care in the EU has required the transformation of existing regulatory (ethical and legal) frameworks. AI continues to bring challenges, and further changes to ethical and legal frameworks will be needed as we become more aware of the impact of AI. It is not clear, however, whether we will ever become privy to the secrets of AI due to the opacity of self-learning algorithms. This means that regulation may become increasingly difficult as AI systems become more autonomous. We must, therefore, remain vigilant and continue to put adequate regulatory structures in place to guide the development and use of AI in health and care.

Endnotes

[1] https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering
[2]https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe
[3]https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence
[4]https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[5]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[6] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject').
[7]See Andoulsi and Wilson (2013), Understanding Liability in eHealth: Towards Greater Clarity at European Union Level, in Carlisle George, Diane Whitehouse and Penny Duquenoy (eds). eHealth: Legal, Ethical and Governance Challenges, Springer-Verlag.
[8]Atabekov, A and Yastrebov, O (2018), Legal Status of Artificial Intelligence Across Countries: Legislation on the Move. European Studies Journal, Volume XXI, Issue 4, 2018
[9]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593
[10]https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[11] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Standards for the Ethics of AI

Mr Brian Tranter

ANEC representative – IEC , UK.
(btranter@btinternet.com)

Artificial intelligence (AI) is a transformative technology. It is already impacting consumers and will increasingly do so in different ways, many of which are yet to be defined. In the majority of cases the impact will be positive, offering solutions to modern day problems. However, although a system utilising artificial intelligence may be safe, applied inappropriately it has the potential to lead to unethical or socially unacceptable outcomes. For example, collaborative robots have huge potential to supplement the work of human carers and enhance surgical procedures but what are the ethics of doing so. Should the use of these systems be limited in some way, if so under what conditions and who decides? While encouraging the positive uses of AI it is therefore equally important to have a mechanism to ensure that all who use this technology are protected from these potentially negative effects.

Standards are a well-established tool used to supplement regulatory requirements, set specifications and give guidance to designers, installers, users and others connected to a product or service. For example, standards developed over many years have helped to ensure that the products and services used by us all are physically safe. Through the application of these standards risks and hazards are identified, and solutions determined that remove or at least reduce any risks to an acceptable level.

For a system using AI new and innovative standards are therefore needed to address ethical risks such as loss of human dignity, control or capability in the same way that physical risks are addressed. Historically it is not an area that standards have covered and it is a complex problem. There may not be a 'right solution'. The 'best solution' may not always be the same as it will depend not only upon the application but also the precise circumstances in which it is applied. Regional difference will also influence the acceptability of a solution. What is acceptable in Europe may not be acceptable in Asia or America. And ethical norms are also subject to change.

Despite these difficulties work in this area is progressing. New standards will be developed that will not only help to protect users of AI and associated systems but they will also help to protect the reputation of AI and encourage the positive development of this important transformative technology.

Some useful links:
https://www.anec.eu/
https://www.anec.eu/priorities/digital-society
https://blog.iec.ch/2019/04/iec-standardization-evaluation-group-for-autonomous-and-artificial-intelligence-applications-establishes-new-work-programme/
https://www.iec.ch/dyn/www/f?p=103:186:16011968436394::::FSP_ORG_ID:22827

How Data-driven AI can Benefit from Formalized Knowledge to Become More "Explainable": An Experience from Medical Process Mining

Prof Stefania Montani

Professor of Computer Science - University of Piemonte Orientale Alessandria Area, Italy.
(stefania.montani@uniupo.it)

From self-driving cars, to speech-interpreters, and to medical decision support, we are experiencing an explosion of Artificial Intelligence (AI) applications, which are demonstrating themselves to be more and more helpful and accurate. However, they are typically powered by unsupervised machine learning algorithms (***data-driven AI***), which often operate as "black boxes", in the sense that no transparent interpretation is available for the algorithm output.

Explainability, that we can define as the ability to explain or to present the output of an algorithm in a way that is comprehensible and understandable to a human, is therefore a critical issue, which has been considered (at least to some extent) also in the GDPR EU regulation [1]. The ***right to explanation*** (i.e., the right to be given an explanation for an output of the algorithm), in particular, becomes particularly urgent in applications supporting medical decision making, as testified in the literature [2].

Existing strategies to deal with this issue range from the definition of global surrogate models [3], to local ones [4]. On the one hand, global surrogates seek to distil the knowledge captured by a black-box data-driven model into a more interpretable model: this approach is flexible, but the conclusions drawn concern the model, not the data, since the surrogate model does not have access to the actual data, but only to the original model output. As such, the explanations provided on the algorithms tend to be only as good as the original model. Local surrogates, on the other hand, make use of a more interpretable model to explain the behaviour of a black-box algorithm when it is applied to a given sample of the input data. This second family of solutions suffers from a considerable degree of instability in terms of explanations of the algorithms used: if the sampling process is repeated, one might obtain different explanations, jeopardizing the method robustness.

In this presentation, we suggest to follow a different research direction, namely to exploit a ***synergy between data-driven*** and ***knowledge-based AI*** approaches (the latter are intended as methods that model human knowledge in computational terms), to deal with transparency and explainability.

In particular, the presentation will illustrate our experience in the field of **medical process mining**, where we have adopted an ontology and a rule-based system (knowledge-based AI) to abstract medical process *traces* (i.e., the sequences of activities that have been actually executed and logged while caring the patients). This approach has led a process mining algorithm (data-driven AI) to learn more readable and understandable process models, where the key process steps are always clear, and the algorithm output is immediately interpretable by domain experts [5].

We believe that this strategy could be considered in other situations as well. Indeed, powerful and promising data-driven AI can strongly benefit of methods based on knowledge formalization, and their generalization and abstraction capabilities, which can be particularly helpful in providing a really explainable decision support; indeed, as stated by the 2017 Barcelona Declaration for the Proper Development and Usage of Artificial Intelligence in Europe [6], "the full potential of AI will only be realized with a combination of these two approaches".

References

[1] Goodman B, Flaxman S. European Union regulations on algorithmic decision-making and a right to explanation. AI Magazine. 2017 38(3):50–57
[2] Shortliffe EH, Sepulveda MJ. Clinical decision support in the era of artificial intelligence. JAMA. 2018 Dec 4;320(21):2199-200
[3]Che, Z., Purushotham, S., Khemani, R., Liu, Y.: Interpretable deep models for ICU outcome prediction.

In: AMIA Symposium 2016, pp. 371–380 (2016)
[4] Ribeiro, M., Singh, S., Guestrin, C.: "Why should I trust you?": explaining the predictions of any classifier. In: Proceedings of 22nd ACM SIGKDD, pp. 1135–1144, NY, USA (2016)
[5] Montani, S., Leonardi, G., Striani, M., Quaglini, S., Cavallini, A.: Multi-level abstraction for trace comparison and process discovery, Expert Systems with Applications 81 (2017) 398-409
[6] Barcelona Declaration for the Proper Development and Usage of Artificial Intelligence in Europe. 2017 Mar;1-4.

The Language of Automated Medicine

Mr Chris Zielinski

Visiting Fellow – University of Winchester, UK.
(chris@chriszielinski.com)

This presentation focuses on what happens to language in the digital age, and specifically language related to health in the context of artificial intelligence. It will explore what the implications are for the further development of artificial intelligence and algorithms.

The first part of the discussion offers a critical review of automated translation software based on 50 years of personal experience (the author started his career as a professional translator). Broadening the discussion from personal experience to empirical results, the author reviews the use of automated translation for medical diagnoses (citing papers in the British Medical Journal and elsewhere). Despite the many breakthroughs in this field, and despite the billions of dollars poured into it, the results are discouraging. Automated translation software continues to be poor and unreliable. Why?

The second section of the presentation focuses on the use of language, specifically, the way language is being used to personify digital technology – from "bugs" and "pirates" to "neural networks" and machine "learning". It is important to recognize that these are metaphoric uses that do not represent – and often mis-represent – reality, producing a kind of fake news. This part of the presentation on personification and "andropomorphism" in the digital age continues into reflections on the language of artificial intelligence.

A brief overview of artificial intelligence from this standpoint is offered in the third part. This addresses the semantic gap – the questions of intelligence, understanding and consciousness are (very briefly) touched on – and leads on to the definition of two forms of AI. One variety is the explicitly algorithm-based AI (as used in the Big Blue/Kasparov chess match) and the other is the goal-seeking variety, where the software generates its own algorithms in search of an explicit target (as used in the DeepMind/AlphaGo attack on the game of Go).

The final part of the presentation addressed the concept of "artificial ignorance"– where the software produces results that cannot be parsed or checked, where we cannot be sure we have the right answer, or the best answer. Books have been written about the biases and prejudices being accidentally or unconsciously coded into software. Examples of these are given, focusing on artificial ignorance and health. Pragmatic and ethical issues are outlined.

It should be stressed that the objective of this presentation is not to debunk artificial intelligence. Artificial intelligence will certainly continue to bring many positive results and solve issues that have plagued the human race since the dawn of time. It will help secure an equitable existence for many in all walks of society and at all economic levels, and is likely to usher in a new era of ever-improving healthcare.

However, there are certainly danger zones. This author does not fear "the singularity" – the term used by Kurzweil and others to describe the moment when artificial intelligence becomes in some way superior to human intelligence and quickly takes over the world, consigning the human race to slavery or extinction. Despite fears expressed in this direction by a number of notable leaders of technology, this is science fiction, and is not going to happen.

In fact, the real and pressing concern for the human race is not that the technology will become too intelligent, but rather that it will become too ignorant if left to its own devices, leading to consequences that will affect millions of people. Human input is essential and cannot be ignored in the development of self-improving software.

References

Patil S. and Davis P. 2014. Use of Google Translate in medical communication: evaluation of accuracy *BMJ* 2014;349:g7392 doi: 10.1136/bmj.g7392 (Published 15 December 2014) (https://www.bmj.com/content/349/bmj.g7392)

Kurzweil, R. 1990. *The Age of Intelligent Machines*, Cambridge, MA: MIT Press, ISBN 0-262-11121-7

Caughill, P. 2017. Elon Musk: "The Singularity for This Level of the Simulation Is Coming Soon" October 5th 2017 (https://futurism.com/elon-musk-the-singularity-for-this-level-of-the-simulation-is-coming-soon)

Cellan-Jones, R. 2014. Stephen Hawking warns artificial intelligence could end mankind. BBC News 2 December 2014 (https://www.bbc.co.uk/news/technology-30290540)

Bostrom, N. 2014. *Superintelligence: Paths, Dangers, Strategies,* Oxford University Press, Oxford; ISBN-10: 9780198739838

Das S. 2019. It's hysteria, not a heart attack, GP app Babylon tells women October 13 2019, 12:01am, The Sunday Times (https://www.thetimes.co.uk/article/its-hysteria-not-a-heart-attack-gp-app-tells-women-gm2vxbrqk)

Figure 1 – Path to Artificial Ignorance

Quality Audits with Blockchain for Healthcare in the UK

Dr Ian Mitchell[a] and Ms Sukvhinder Hara[b]

[a]Associate Professor - Middlesex University, UK.
(i.mitchell@mdx.ac.uk)

[b]Senior Lecturer – Middlesex University, UK.

Quality Audits

Quality audits are necessary to ensure that affiliated organisations' procedures, practices and processes are aligned to the governing bodies' principles, which ultimately inspects, reports and has the authority to issue a license to operate as a healthcare provider.

Quality is concerned with maintaining principles, whilst allowing practices to change. In many cases in healthcare, quality management produces paperwork that provides evidence on the procedures and practices given to care for an individual. It is difficult to generalise about all quality audits, however, many institutions that do quality audits have a governing body. For example, in the context of healthcare providers operating in the UK, the Care Quality Commission (CQC) inspects its accredited or affiliated healthcare providers, be they dentists, care homes or hospitals. This inspection often leads to successful affiliation with a rating, occasionally the inspections will uncover some major transgressions of practices that can lead to the licence being revoked. So audits are often seeing the organisation in its best light, despite short notice given by the CQC. During these quality audits it is the integrity of the paperwork, records or data that is in question and in particular the detection of retrospective editing. Retrospective editing can be prevented by the introduction of a blockchain technological solution, whereby the CPU effort required to alter and edit records becomes insurmountable. This possibility is explained at the end of this next section on blockchain.

Blockchain

Blockchain is not only Bitcoin [10]. Blockchain is the technology [12] supporting Bitcoin and includes: cryptography, to ensure confidentiality; consensus, establishing and ensuring trust; Peer-2-Peer network, to ensure availability and openness; and append-only immutable distributed ledgers, to ensure validation. Despite Nakamoto's paper [10] being over 10 years old, we are on the cusp of a blockchain revolution [6] that is changing how organisations communicate and operate.

Blockchain has two types: permissionless and permissioned. Permissionless allows anyone to contribute and add new blocks and is often thought of as being public; whereas permissioned blockchain allows only members to contribute and add new blocks and is often thought of as being private. The use of tokens can also characterise blockchains. Originally, blockchain was developed as a cryptocurrency [1] to exchange financial value without the need for an intermediary, e.g. a bank, to confirm the trustworthiness of the individuals involved. These blockchains can either be permissioned or permissionless, and are referred to as cryptocurrency. Over the years blockchain was viewed as a direct solution to many business problems, e.g., in financial auditing [5], integrity verification and rights management [7] and governance [8]. For a fuller description and review on blockchain technology and applications see [4]. Many of these applications do not require the exchange of tokens or coins, but just a simple transaction has taken place and created via consensus on the immutable distributed ledger. We call these types of blockchain: tokenised and tokenless.

A combination of the above types of blockchain technologies can give rise to permissioned tokenless blockchain applications that can support, record and enhance the administration of patient records adhering to the principles laid down under the Caldicott Report [3].

While medical blockchain applications [2, 11] and sharing of patients' data is not new [13], this paper examines whether the use of blockchain for quality audits [9] can improve trust in recorded medical data.

Audits and Blockchain

Blockchain by its nature has an affinity with quality audits that, as of writing, is yet to be exploited in healthcare sectors across the UK. Most medical applications concern themselves with handling and sharing of patient data; however, work by Mitchell and Hara [9] focused on a prototype application of blockchain that investigates its use as an auditing tool.

Briefly, the completion of a Medical Administration Record (MAR) sheet is compulsory for healthcare providers in care sectors. Administering medication to a service user requires that a healthcare professional record this action as an entry in a MAR sheet. The objective of MAR sheets is to safeguard vulnerable adults in administering medication that is, amongst other things, inspected by the CQC in the UK.

Blockchain Medical Administration Record (BMAR) allows secure updates on an MAR sheet. Furthermore, it is a permissioned network governed by an authority, e.g., CQC, and hence all updates can be viewed. All healthcare professionals would complete their MARs entry, which would then be created by consensus and updated on an append-only ledger. Currently, when mistakes are made, it is tempting to destroy the original MAR sheet and replace it. Mistakes can be updated on BMAR; however, the update would also be recorded on the blockchain. This makes BMAR tamper-proof and thus promotes the safeguarding of vulnerable adults.

Conclusion

BMARs [9] provides evidence that quality audits can be implemented via the blockchain. Auditability is indeed conducive to the use of blockchain applications, and therefore it is proposed that information required by audits should be completed via blockchain.

References

[1] Andreas M. Antonopoulos. Mastering Bitcoin. O'Reilly, 2nd edition, 2017.
[2] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In Open and Big Data (OBD), International Conference on, pages 25–30. IEEE, 2016.
[3] F Caldicott. Information: To share or not to share? The information governance review. Dept. of Health, UK, March 2013.
[4] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 2018.
[5] Jun Dai and Miklos A Vasarhelyi. Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3):5–21, 2017.
[6] Evgeniia Filippova, Arno Scharl, and Pavel Filippov. Blockchain: An empirical investigation of its scope for improvement. In International Conference on Blockchain, pages 1–17. Springer, 2019.
[7] Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, Tomokazu Yamada, Akihito Akutsu, and Jay Junichi Kishigami. Bright: A concept for a decentralized rights management system based on blockchain. In 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), pages 345–346. IEEE, 2015.
[8] Heng Hou. The application of blockchain technology in e-government in china. In 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1–4. IEEE, 2017.
[9] Ian Mitchell and Sukhvinder Hara. BMAR-blockchain for medication administration records. In Blockchain and Clinical Trial, pages 231–248. Springer, 2019.

A Novel Privacy Framework for mHealth when Managing Chronic Diseases

Mr Farad Jusob, Dr Carlisle George and Dr Glenford Mapp

ALERT Research Group - Middlesex University, UK.
(FJ105@live.mdx.ac.uk)

Introduction

This presentation describes the development of a novel privacy framework for mHealth. The framework (i) proposes a new methodological approach to addressing privacy and mHealth in the context of managing chronic diseases, and (ii) combines specific mechanisms and technologies to enable the development of a prototype mHealth system.

Background - mHealth and Privacy

The widespread rise in chronic illnesses (e.g., diabetes and hypertension) has resulted in the need to find more efficient ways of managing the treatment of patients with these conditions. One such way is through the use of mobile health (mHealth) technologies that can gather real-time data from patients and monitor the patients from a distance, removing their need to be at a medical facility (Estrin and Sim, 2010). These technologies can be an integral part of intelligent healthcare environments (e.g., smart homes that monitor and assist elderly patients) (Augusto, 2013) which are essential to reducing healthcare costs, improving efficiency, and enhancing the quality of treatment and care given to patients.

The use of mHealth, however, brings various privacy concerns and challenges (European Commission 2014; EDPS, 2015). When using mHealth technologies, patients must trust that their health information is private and secure. If patients lack a sense of trust in the treatment of their health data and feel that the confidentiality and accuracy of their health information is in jeopardy, they may choose to not disclose their personal health information. This can result in a misunderstanding of the patients' overall health status by healthcare professionals and in the provision of sub-optimal treatment. Given the sensitivity of health data, the rapid development of the mHealth sector raises privacy and security concerns regarding the data collected from patients.

The Need for a Novel Privacy Framework

In the context of mHealth, managing privacy is a complex issue and patients should have more control over the collection, recording, dissemination, and access to their mHealth data. The management of privacy can be facilitated through the use of suitable privacy frameworks because they outline core principles, best practices and solutions to protect and manage the privacy of information and people. Having a suitable privacy framework for mHealth in the context of the management of chronic diseases is therefore essential to building patient trust and providing good healthcare. A review of various existing regulatory frameworks for privacy concluded that no single framework completely addresses the privacy concerns regarding the management of chronic diseases when using mHealth solutions (Jusob, 2017). Existing regulatory frameworks were designed to be used for health information and were found to focus mostly on the data aspect of privacy and not to take into consideration bodily privacy and user autonomy (Jusob, 2017).

There is therefore a need to develop a suitable privacy framework for mHealth in this context.

Proposed Framework

The work presented in this paper discusses the development of a privacy framework for mHealth in the context of managing chronic diseases. The methodological approach to developing the framework was based on a modified version of the *Engineering Design Process* methodology (Khandani, 2005). First the problem was defined. Second, information was gathered on the problem, (i.e. an analysis of existing solutions regulatory frameworks for privacy was carried out, followed by research to identify privacy threats and concerns from previous studies when managing chronic diseases with mHealth). Third, solutions were analysed and a solution was generated and selected (i.e. framework requirements were

specified, then the framework was designed and illustrated in a diagrammatic format). The fourth step, involves testing the solution generated and focuses on the development of a software prototype (to implement the framework). Prototype development is currently ongoing using a four-step prototype development process described by Naumann and Jenkins (1982).

The proposed framework is illustrated in the **Figure 1** (below) and consists of five layers.

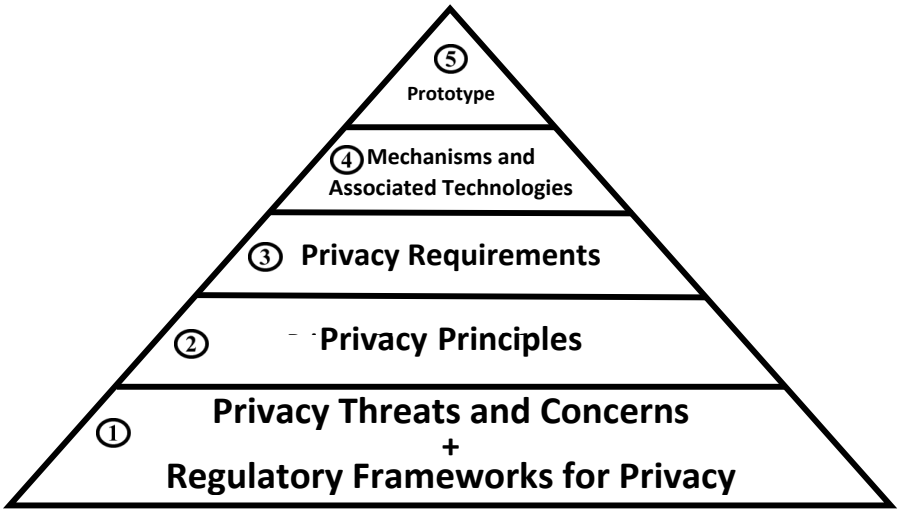

Figure 1 - Proposed Privacy Framework

The proposed privacy framework takes into consideration the data and bodily aspect of privacy as well as incorporates capabilities and mechanisms to facilitate user autonomy. The first layer of the framework focuses on identifying: (i) privacy obligations/guidelines from *regulatory frameworks for privacy* and (ii) *privacy threats and concerns* from existing research studies. The second layer consists of *principles* necessary to address (a) the privacy obligations/guidelines derived from regulatory frameworks and (b) the privacy threats/concerns identified in the first layer. The third layer builds on the second layer and translates the privacy principles into *privacy requirements* that can be implemented into an mHealth system. The fourth layer discusses the *mechanisms and associated technologies* needed to implement the privacy requirements. This includes use of encryption, access control mechanisms, device and storage security, anonymisation and pseudo-anonymisation mechanisms, system programs, and blockchain. The fifth layer defines the *prototype* that incorporates the mechanisms and associated technologies necessary to implement the privacy requirements as well as other technologies needed to develop a privacy-conscious mHealth system.

A comparison made, of the proposed framework with existing privacy frameworks, concluded that the new framework covers a wider array of privacy principles compared with any single previous framework. Currently the prototype proposed is being developed. It will then undergo testing and evaluation.

The presentation will discuss the framework development process and the different layers of the framework in greater detail.

References

Augusto J, Callaghan V, Kameas A, Cook, D, and Satoh I. (2013). Intelligent Environments: a manifesto. Human-Centric Computing and Information Sciences, 3(12), doi: 10.1186/2192-1962-3-12.

European Data Protection Supervisor (EDPS), (2015). Mobile Health: Reconciling technological innovation with data protection. Opinion 1/2015, Brussels. https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf [Last accessed 14/09/2019]

Estrin, D, and Sim, I. (2010). Open mHealth Architecture: An Engine for Health Care Innovation, Science 330:759-760.
European Commission (2014). Green Paper on mobile Health ("mHealth"). Brussels, 10 April 2014, COM (2014) 219 final.
Jusob, F.R., George, C. and Mapp, G. (2017). Exploring the need for a suitable Privacy Framework for mHealth when managing Chronic Diseases. *Journal of Reliable Intelligent Environments,* December 2017, Volume 3, Issue 4, pp 243–256.
Khandani, S. (2005). *Engineering Design Process.* https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/09/ME101-4.1-Engineering-Design-Process.pdf. [Last accessed 14/09/2019].
Nauman, J.D. and Jenkins, M. (1982). Prototyping: The New Paradigm for Systems Development, *MIS Quarterly*, **6**, 3, 29-44.

A Comprehensive Information Security Framework for mHealth and Prototype Development

Ms Nattaruedee Vithanwattana, Dr Glenford Mapp and Dr Carlisle George

ALERT Research Group – Middlesex University, UK.
(NV166@live.mdx.ac.uk)

Introduction

The use of mobile and wireless technologies to support achievements in healthcare systems (mHealth) has an enormous potential to transform healthcare across the globe [1]. mHealth covers "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" [2]. Other solutions include body sensors and wireless infrastructures. These devices are used in collecting clinical health data, and delivering healthcare information (e.g. via Bluetooth) to patients, medical professionals, and researchers. They are also used for real-time monitoring of patients' vital signs, such as heart rate, blood glucose level, blood pressure, body temperature, and brain activities [3]. Healthcare data collected is stored in databases including those on mobile devices and Cloud storage. Healthcare data is classed as "sensitive data" under data protection legislation, and hence requires a high level of security to protect the confidentiality of the data and to prevent unauthorised access. mHealth systems are still vulnerable to numerous security issues relating to weaknesses in their design and data management. Therefore, there is a need to develop a comprehensive information security framework for mHealth.

Framework

A major challenge in developing an effective Information Security Framework is to ensure that security encompasses both mHealth devices and Cloud storage in order to secure sensitive mHealth system. This paper discusses a proposed new Information Security Framework, developed by the authors, and a prototype to implement aspects of this framework. As a part of developing the new information security framework for mHealth systems, possible solutions were considered for managing mHealth data using various mechanisms in order to deliver the essential security components of mHealth systems. These include Confidentiality, Integrity, Availability, Non-repudiation, Authentication, Authorisation, Accountability, Auditability, and Reliability. These mechanisms include Encryption as a Service, Capabilities, Storage Management, Digital Filter, Secure Transport Layer, Blockchain, Secure Transactional Layer, and Service Management Platform. Figure 1 below illustrates the proposed new information security framework [4].

APPLICATIONS
APPLICATION DEVELOPMENT LAYER
SERVICE MANAGEMENT PLATFORM
SECURE TRANSACTIONAL LAYER
BLOCKCHAIN SYSTEM
SECURE TRANSPORT LAYER
DIGITAL FILTER SYSTEM
STORAGE MANAGEMENT LAYER
CAPABILITY SYSTEM
OS LAYER

Figure 1 – Proposed Information Security Framework [4]

- The *Application* layer contains mHealth (device) applications and will authenticate and authorise application users.
- The *Application Development Layer* interacts with the cloud server to authenticate the application.
- The *Service Management Platform* will define the requirements to run system services.
- The *Secure Transactional Layer* protects remote procedure calls between stakeholders and cloud servers using strong typing and capabilities.

- The *Blockchain System* is used to record the interaction between any client and servers.
- The Secure Transport Layer secures the transmission of healthcare data between stakeholders and the cloud infrastructure.
- *Digital Filters* delivers additional control by which users will be able to access healthcare data.
- The *Storage Management Layer* is used to secure store healthcare data.
- *Capabilities* manage access rights to stored healthcare data.
- *Encryption as a Service* protects the confidentiality of healthcare data.
- The *Operating System Layer* provides a variety of services including the fundamental operating services such as memory management, file system handling, as well as system and networking services.

Prototype Development

The proposed framework consists of many different layers and each layer is rather complex to implement. As a result, building a viable prototype that clearly embodies all features of the proposed framework will require a significant and lengthy effort. In this context, a prototype was designed consisting of a subset of five layers of the proposed framework (see Figure 2 below). Three of the layers (mHealth Applications, File System and Secure Transport Layer) consist of existing technologies. Two of the layers (Service Management Platform and the Secure Transactional Layer) are being newly developed due to the non-existence of suitable technologies for these layers in the context of ensuring security for mHealth systems.

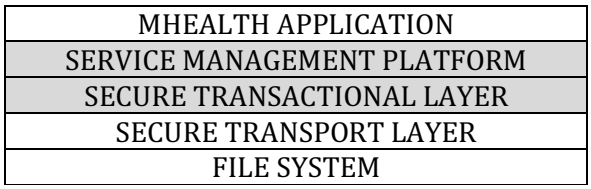

Figure 2: A basic prototype

The five layers of the prototype shown in Figure 2 are described as follows:

- *Application*: An mHealth application, which can create, store, modify, and delete healthcare records.
- *Service Management platform*: Functionality includes service management and security. Services will be tracked and capabilities will be applied to provide access to services. The state of the system will be monitored.
- *Secure Transactional Layer*: A strongly typed Remote Procedure Call will be developed and implemented into this layer to protect the transactions between stakeholders and cloud servers. Capabilities will also be used to check the authentication and authorisation of clients and servers.
- *Secure Transport Layer*: A new protocol called the Simple Lightweight Transport Protocol has been developed and will be used to implement this layer [5].
- *File System*: This layer replaces the need to use a real cloud storage system for purposes of evaluating the prototype. It is used to store and retrieve healthcare data which will be encrypted.

References

[1] World Health Organization (2011). mHealth: New horizons for health through mobile technologies. [online] Available from: https://www.who.int/goe/publications/goe_mhealth_web.pdf [Accessed: 15 October 2019]

[2] European Commission (2014). Green Paper on mobile Health ("mHealth"). Available from: https://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth [Accessed: 15 October 2019]

[3] Germanakos P., Mourlas C., and Samaras G. (2005). A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems. *Proceedings of the Workshop on 'Personalization for*

e-Health' of the 10th International Conference on User Modeling (UM'05). Edinburgh, July 29, 2005, pp. 67–70.

[4] Vithanwattana, N, Mapp, G. and George, C. (2017). Developing a Comprehensive Information Security Framework for mHealth: A Detailed Analysis, in Special Issue on "Application of Software Engineering Techniques to Improve the Reliability of Intelligent Environments", *Journal of Reliable Intelligent Environments*, July 2017, Volume 3, Issue 1, pp 21–39

[5] Mapp, G., Aiash, M., Ondiege, B., and Clarke, M (2014). Exploring a New Security Framework for Cloud Storage Using Capabilities. *In: 2014 IEEE 8th Symposium on Service Oriented System Engineering (SOSE).* Oxford: IEEE, P. 484-489

Securing eHealth and mHealth: Moving from Frameworks to Prototypes

Dr Glenford Mapp, Dr Carlisle George, Ms Sukhvinder Hara,
Ms Nattaruedee Vithanwattana, Mr Farad Jusob and Ms Ann Samuels

Medical Data Research Group – Middlesex University, UK.
(g.mapp@mdx.ac.uk)

Introduction

eHealth and mHealth have been with us for some years. However, the uptake in the use of these systems in developed countries as part of national health programmes has been relatively slow. Though actual devices and physical technologies are now well tested, there still is no national legal, ethical, or more importantly, security framework for eHealth or mHealth. Several frameworks have been examined attempting to address key properties of security for eHealth and mHealth. These include the Firesmith framework [1] that completely specifies the required security properties as well as an operational framework, which has been developed by Nattaruedee Vithanwattana at Middlesex University [2].

Towards an Implementation Framework

By investigating these efforts, we believe that there is now a key set of technologies, which can be brought together to form an Implementation Framework from which practical prototypes may be built. The four technologies are capabilities, secure remote procedure calls (SRPC), blockchain as well as encryption and hashing techniques.

Capabilities

Capabilities are immutable digital tokens or tickets that must be produced by clients in order to get service from servers. Capabilities not only specify the service required but also what functions can be done by the server on behalf of the client. This can be easily shown using a common file system. Owners or creators of files have the right to read, write and delete their files. This is represented by the master capability of the file. However, owners should also be able to share files with others; so we need another capability that would allow a user to read or write to the file and yet another capability that would only allow other users to read the file. These two capabilities can be derived from the master capability.

In the proposed prototype, capabilities are associated with everything in a secure healthcare system including people, devices and digital assets such as files and electronic health records. This allows role-based security to be implemented using capabilities; so doctors, nurses, administrators and patients can function in their normal roles in a hospital context. Hence, capabilities are used for authentication: since every entity must have a capability, and authorization because capabilities also indicate what functions can be exercised on behalf of the holder of a given capability.

The concept of capabilities is not a new idea, it was developed in the 1960s, but fell into disuse as Access Control Lists (ACLs) were used to implement security for digital assets such as electronic records and files. However, recent work [3] at Middlesex University has made the use of capabilities much easier by providing practical solutions to managing capabilities including the safe propagation and revocation of capabilities. In [4], the authors showed how capabilities are used in remote patient monitoring.

Secure RPC

The second major technology is the secure remote procedure call (SRPC). A remote procedure call (RPC) specifies how applications and servers interact with each other. So RPC specifies the function calls and arguments that are used to allow the server to serve clients. However, in normal RPC systems, the interaction between the client and server is predefined and all calls are assumed to follow the predefined format. This has led to large security breaches such as buffer overflows, empty or NULL-call corruption and clients gaining access to sensitive data because servers assume that the clients are safely using the predefined format. Several systems suffer greatly from this malady and thus hospital systems which are not regularly updated has suffered from this as seen in the Ransomware attacks in the UK. In secure RPC, it is possible to pass information about the symbols as well as the value of that symbol or

argument in the remote procedure call. This means that the server can easily check that every call and its arguments obey the predefined format before it attempts to fulfil the call. Security is therefore increased. Performance testing has shown that the added cost of using Secure RPC is only 10% more than native or insecure RPC. Hence, the benefits outweigh the costs.

Blockchain

The third key technology is blockchain. This is a new technology in which transactions between entities can be certified as having taken place without a third entity having to do the certification. Instead a number of distributed algorithms are run on different machines that produce an immutable chain of blocks, which record the transactions. Bitcoin is an example of blockchain technology used to manage financial transactions. The use of blockchain for the management of health records is now being actively explored [5]. A new open source blockchain-based technology called Hyperledger, which can be used to support different types of systems, has been made available to developers. The use of blockchain to record interactions via Secure RPC and capabilities in healthcare systems will enhance the security environment as it adds the important security property of non-repudiation and provides the ability to quickly discover security and privacy violations.

Encryption and Hashing

The fourth and final technology is the use of encryption and hashing algorithms. This can be done at two levels in a practical system. The first is for storage systems. Thus, in the proposed system, all data is stored using strong encryption algorithms such as AES. Encryption and hashing techniques such as IPSec [6] are also used to provide secure communications between entities in the system.

Implementation Framework

The overall system is shown in Figure 1.

CAPABILITIES
SECURE REMOTE PROCEDURE CALLS
BLOCKCHAIN HYPERLEDGER
ENCRYPTION+HASHING IPSec, AES

Figure 1: Components of the Implementation Framework

Conclusions

At Middlesex University we are concentrating on building a functional prototype for eHealth and mHealth based on these technologies.

References

[1] Firesmith D, *"Specifying reusable security requirements," Journal of Object Technology*, vol. 3, no. 1, pp. 61 – 75, 2004.

[2] Vithanwattana N, Mapp G, George C: *Developing a comprehensive information security framework for mHealth: a detailed analysis:* Journal of Reliable Intelligent Environments, 2017.

[3] Mapp G, Aiash M, Ondiege B and Clarke, M.: *Exploring a New Security Framework for Cloud Storage Using Capabilities:* 1st Int'l Workshop on Cyber Security and Cloud Computing, Oxford UK, 7-11 April 2014.

[4] Ondiege B, Clarke, M and Mapp G.E.: *Exploring a New Security Framework for Remote Patient Monitoring Devices*: MDPI Computers Journal: February 2017: doi:10.3390/computers6010011.

[5] Mitchell I and Hara S: (2019) *BMAR – Blockchain for Medication Administration Records.* In: Jahankhani H., Kendzierskyj S., Jamal A., Epiphaniou G., Al-Khateeb H. (eds) Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications. Springer.

[6] Frankel S and Krishnan S: *IP Security (IPSec) and Internet Security Key Exchange (IKE) Document Roadmap* at https://tools.ietf.org/html/rfc6071 last accessed 8th October 2019.

List of Participants

- **BARN, Balbir**, Middlesex University, UK.
- **BOORSMA**, André TNO, The Netherlands.
- **COCKERTON, Tracey**, Middlesex University, UK.
- **CRAWFORD**, John, CrawfordWorks, UK.
- **DeMURO, Paul,** Nelson Mullins, USA.
- **DUQUENOY, Penny**, Middlesex University, UK.
- **GEORGE, Carlisle**, Middlesex University, UK.
- **GALAL-EDEEN, Galal**, Cairo University, Egypt.
- **GOMES DE ALMEIDA**, **Vania**, Middlesex University, UK.
- **HARA, Sukhvinder**, Middlesex University, UK.
- **HAREWOOD, Kelvin,** Middlesex University, UK.
- **JUSOB, Farad**, Middlesex University, London, UK.
- **LEONCE, Jasmine**, East and North Hertfordshire, NHS Trust, UK.
- **MANGIACOTTI, Anthony**, Padua University, Italy.
- **MAPP, Glenford**, Middlesex University, UK.
- **MITCHELL, Ian**, Middlesex University, UK.
- **MONTANI Stefania**, University of Piemonte Orientale Alessandria Area, Italy.
- **NAGARAJAN, Durga Vellore**, Middlesex University, UK.
- **NAMORADO, Joana**, Fraunhofer Institute, Germany.
- **NOVOSELOVA, Tatiana**, Middlesex University, UK.
- **OGOH, George**, De Montfort University, UK.
- **OMISANYA, Joseph Opeoluwa,** Middlesex University, UK.
- **PETRIDIS, Miltos**, Middlesex University, UK.
- **ROSENMÖLLER, Magdalene**, IESE Business School, Spain
- **TAYLOR, Richard**, International Baccalaureate, UK.
- **THIMBLEBY, Harold**, Swansea University, UK.
- **TRANTER, Brian,** ANEC representative, UK.
- **VAN LIESHOUT, Marc,** TNO, The Netherlands.
- **VITHANWATTANA, Nattaruedee**, Middlesex University, UK.
- **WHITEHOUSE, Diane**, The Castlegate Consultancy, UK.
- **WHITNEY, Gill,** Middlesex University, UK.
- **ZIELINSKI, Chris**, University of Winchester, UK.

Thank you to our Workshop Sponsors!!!!

Faculty of Science and Technology
Middlesex University, London, UK
http://www.mdx.ac.uk/about-us/our-faculties/faculty-of-science-and-technology

Institute for Bioethics and Health Policy
Millar School of Medicine
University of Miami, USA
https://bioethics.miami.edu

The Castlegate Consultancy
United Kingdom

The European Centre for the Study of Ethics, Law and Governance in Health Information Technology
Online: http://ecelghit.org

Proceedings of the 2019 Health IT Workshop
on
Emerging Technologies in Healthcare: Legal, Ethical & Social Aspects
7th & 8th November 2019
Middlesex University, London, UK

Faculty of Science and Technology
Aspects of Law and Ethics Related to Technology (ALERT) Research Group
http://www.eis.mdx.ac.uk/research/groups/Alert/ehealthwks2019/

ISBN 978-164713330-6