Proceedings of the 2018 Health IT Workshop on

Developments in ICT & Healthcare: Legal, Ethical & Social Aspects

8th & 9th March 2018
Middlesex University, London, UK

Proceedings of the 2018 Health IT Workshop on

Developments in ICT & Healthcare: Legal, Ethical & Social Aspects

8th & 9th March 2018
Middlesex University, London

Editors:
Carlisle GEORGE (*Middlesex University, UK*),
Diane WHITEHOUSE (*The Castlegate Consultancy, UK*),
Kenneth GOODMAN(*University of Miami, USA*),
Penny DUQUENOY (*Middlesex University, UK*).

ISBN 978-1-64713-306-1

Contents

Welcome from the Vice-Chancellor **1**

In Memoriam - Dr Samantha Adams **2**

Workshop Introduction **3**

Programme **4**

IT, Health, Ethical use of Public Health Data in the context of Universal Health Coverage
Dr Joana Namorado, Scientific Officer, European Commission, Brussels **6**

ICT and Healthcare: The Challenge for Social Theory
Dr Malcolm J Fisk, Senior Research Fellow, CCSR, De Montfort University **7**

Understanding Blockchain Technology and Applications in the Healthcare Domain
Ms Sukhvinder Hara, Senior Lecturer, Middlesex University **9**

The General Data Protection Directive: Some Implications for the Healthcare Sector
Dr Carlisle George, Associate Professor & Barrister, Middlesex University **11**

Cross-Border Exchange of eHealth Data in the EU
Dr Ioannis Komnios, Project Coordinator, The KONFIDO Project **13**

Own it. Personal Data Trading as an Alternative Model
Ms Mitzi László, Neuroscientist and Social Entrepreneur, OWN **15**

Enhancing the SCIROCCO maturity model: Scaling-up integrated care in Europe
Ms Diane Whitehouse, Dr Tamara Alhambra-Borrás & Ms Cristina Alexandru **17**

Big (Health) Data, Artificial Intelligence and Black Box Algorithms: Time for Global Standards
Prof Kenneth Goodman, Director, Institute for Bioethics and Health Policy, University of Miami, USA **19**

Error is more complex than Ethics
Prof Harold Thimbleby, Professor of Computer Science, Swansea University **20**

How Can We Assure the Trustworthiness of Federated Big Health Data Ecosystems?
Prof Dipak Kalra, President, The European Institute for Innovation for Health Data **22**

CrowdHEALTH: Aggregating and Analysing Big Health Data for Policy Making
Dr Usman Wajid, Senior Researcher, Information Catalyst **24**

Promoting Health Apps or Assessing Their Quality? A Reflection on Current Attempts to Govern mHealth
Dr Federica Lucivero, Senior Researcher in Ethics and Data, The Ethox Centre, University of Oxford **26**

The Certification of Apps in An Era of Innovation
Dr Mayoni Ranasinghe & Dr Celia Boyer (Executive Director), Health on the Net (HON) Foundation **28**

Update on Progress with the National Summary Care Records Programme in England
Dr Emyr Wyn Jones, Summary Care Record - Clinical Lead, NHS Digital, England **30**

mHealth and the Management of Chronic Diseases: The Rationale for Developing a Suitable Framework
Mr Farad Jusob, Dr Carlisle George & Dr Glenford Mapp, Middlesex University **31**

Proposing a Novel Comprehensive Information Security Framework for mHealth
Ms Nattaruedee Vithanwattana, Dr Glenford Mapp & Dr Carlisle George, Middlesex University **33**

Building Advanced Medical Platforms: Benefits and Possible Threats for Data Storage Management
Dr Glenford Mapp, Associate Professor, Middlesex University **35**

Author Index **36**

List of Participants **37**

Welcome from the Vice-Chancellor

Ethical practice is intrinsic to healthcare. Complex challenges arise when considering the huge value that information and communication technology can bring to achieving better healthcare in both developed and developing countries. There are many issues that need expert understanding but bring solutions that are acceptable to the public, and often involve trade-offs rather than having clear solutions. These include: privacy in an age of constant cybersecurity threats; patients' rights and abilities to manage and control data about themselves in an age of clever algorithms and cloud computing; 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 ICT.

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 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 the two days.

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.

Professor Tim Blackman
Vice-Chancellor, Middlesex University

In Memoriam - Dr Samantha Adams

Dr Samantha Adams died on 13 December 2017, aged 41. Sam was an Associate Professor at the Tilburg Institute for Law, Technology, and Society (TILT) responsible for the e-health research team at TILT.

She was very supportive of our activities in Health IT at Middlesex and attended our previous workshops in 2016 and 2014, at which she was an active participant. She had also volunteered to be a member of the organising team for this 2018 workshop, but soon after became ill.

On the first day of the workshop, we will have a session dedicated to Samantha's memory. Several of the attendees who knew Sam well will pay tribute to her life, and remember the valuable contribution that she made to the fields of ethics and regulation in health IT.

Workshop Introduction

As we continue to explore new technologies and regulatory frameworks to enable healthcare, we must also seek to identify and address the concerns and challenges associated with these new technologies.

This workshop focuses on the legal, ethical and social aspects of new and emerging technologies in healthcare as well as developments regarding regulatory and ethical frameworks that affect health and care.

The topics covered during the two days include:

- The importance of societal, social and ethical issues in the provision of universal health coverage, and health and care, and services for older adults.
- Use of new technologies in healthcare (e.g. blockchain, cloud storage).
- The new General Data Protection Regulation or other regulatory developments and the implications for the use of ICT in healthcare or other regulatory developments.
- Wider access to (personal) health data (e.g., in terms of personalised health; population health).
- Mobile Health (mHealth) Apps – the development of guidelines and regulatory frameworks.
- Intelligent environments to assist in the provision of healthcare services.
- Trustworthiness and trust development in the fields of health and care.
- Threats to healthcare IT infrastructure (e.g., cyber security, network security).
- Cross-border collaboration in eHealth, mHealth, telemedicine, telecare and telehealth, and social care.

Workshop Organisers

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

Workshop Sponsors

- **Faculty of Science and Technology,** Middlesex University, London. 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. http://www.thecastlegateconsultancy.com

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

Programme

Day 1 – Thursday, 8th March 2018

TIME	ITEM	PAGE Reference
12:00-13.00	Registration, mix-and-mingle (Light refreshments available).	*
13.00-13.05	***Welcome*** **Prof Richard Comley,** Director of Research, Middlesex University.	*
13.05-13.10	***Workshop Introduction*** **Dr Carlisle George/ Dr Penny Duquenoy**, Middlesex University.	03
13.10 -13.40	***IT, Health, Ethical use of Public Health Data in the context of Universal Health Coverage.*** **Dr Joana Namorado**, Scientific Officer, European Commission**.**	06
13:40 - 14:00	***ICT and Healthcare: The Challenge for Social Theory.*** **Dr Malcolm Fisk**, Senior Research Fellow, CCSR, De Montfort University.	07
14:00 - 14:20	***Understanding Blockchain Technology & Applications in the Healthcare Domain.*** **Ms Sukhvinder Hara**, Senior Lecturer, Middlesex University.	09
14:20 -14:40	***The General Data Protection Directive – Some Implications for the Healthcare Sector.*** **Dr Carlisle George**, Associate Professor & Barrister, Middlesex University.	11
14:40- 15:00	***Special Session: Tribute in Memory of Dr Samantha Adams (Tilburg University)***	* (02)
15.00-15.20	Afternoon coffee/tea break (20 mins)	*
15.20-15:40	***Cross-Border Exchange of eHealth Data in the EU.*** **Dr Ioannis Komnios**, Project Coordinator for the KONFIDO Project.	13
15.40-16:00	***Own it. Personal Data Trading as an Alternative Model*** **Ms Mitzi László**, Neuroscientist and Social Entrepreneur, OWN.	15
16:00- 16:20	***SCIROCCO: Directions in Integrating Care – 12 Dimensions for Scaling-up*** **Ms Diane Whitehouse**, eHealth Consultant, The Castlegate Consultancy.	17
16.20-17:00	**Discussion/Panel Session and Roundup (40 mins)** ***New Developments in Health IT - Opportunities & Challenges Ahead*** **Chair: Prof Kenneth Goodman**	*
17.00-19.00	An opportunity to relax or have drinks.	*
19.00	Dinner - Sheridan Suite, Hendon Hall Hotel.	*

Day 2 – Friday, 9th March 2018

TIME	ITEM	PAGE Reference
09.00-09.05	Welcome and introduction to the day, **Dr Carlisle George/ Dr Penny Duquenoy**	*
09:05 - 09:35	***Big (Health) Data, Artificial Intelligence and Black Box Algorithms: Time for Global Standards.*** **Prof Kenneth Goodman**, Professor of Medicine, University of Miami, USA	19
09:35 – 10:05	***Error is more complex than Ethics.*** **Prof Harold Thimbleby**, Professor of Computer Science at Swansea University, Wales (UK)	20
10:05 – 10:25	***How Can We Assure the Trustworthiness of Federated Big Health Data Ecosystems?*** **Prof Dipak Kalra**, Professor of Health Informatics, University College London. President - The European Institute for Innovation for Health Data.	22
10:25 - 10:45	***CrowdHEALTH: Aggregating and Analysing Big Health Data for Policy Making.*** **Dr Usman Wajid**, Senior Researcher, Information Catalyst	24
10:45 –11:00	Coffee Break (15 mins break)	
11:00 – 11:20	***Promoting Health Apps or Assessing Their Quality? A Reflection on Current Attempts to Govern mHealth.*** **Dr Federica Lucivero,** Senior Researcher in Ethics and Data, The Ethox Centre, University of Oxford.	26
11:20 – 11:40	***The Certification of Apps and other Connected Objects.*** **Dr Celia Boyer**, Executive Director, Health on the Net (HON) Foundation	28
11:40 – 12:00	***Update on Progress with the National Summary Care Records Programme in England.*** **Dr Emyr Wyn Jones**, Summary Care Record - Clinical Lead - NHS Digital	30
12:00 – 12:40	*Discussion/Panel Session (40 mins)* ***Trust development as a basis for ethical data sharing – the EU experience.*** **Chair: Dr Joana Namorado**	*
12:40 – 13:40	Lunch	
13:40 – 14:00	***mHealth and the Management of Chronic Diseases*: *The Rationale for Developing a Suitable Framework.*** **Mr Farad Jusob**, PhD Student, Middlesex University, London	31
14:00 – 14:20	**Ms Nattaruedee Vitanwattana**, PhD Student, Middlesex University. ***Proposing a Novel Comprehensive Information Security Framework for mHealth***	33
14:20 – 14:40	***Building Advanced Medical Platforms: Benefits and Possible Threats for Data Storage Management.*** **Dr Glenford Mapp**, Associate Professor, Middlesex University.	35
14:40 – 15:20	***Discussion/Panel Session (40 mins) The future and promise of mHealth.*** **Chair: Dr Carlisle George**	*
15:20 – 15:30	Coffee Break (10 mins break)	*
15:30 - 15:55	**Overview of the workshop and next steps.** **Ms Diane Whitehouse**	*
16:55 – 16:00	Thanks and farewell (workshop organisers)	*

IT, Health, Ethical use of Public Health Data in the context of Universal Health Coverage

Dr Joana Namorado,
Scientific Officer, European Commission, Brussels
(joana.namorado@ec.europa.eu)

Ethics is very important in information technology (IT), particularly when used in the provision of health services and the management of healthcare records. In the context of the new European Union (EU) General Data Protection Regulation (GDPR), ethics is central to the exploration and use of public health records. For this reason, the EU is developing an ethics strategy for Health System Research, particularly in the context of the Health Research and Innovation Cloud - where the strictest ethical standards are required – and, as a trust builder, essential for pooling health-relevant data across member states and for international studies using comparable methodologies. The strategy also establishes the conditions of research under which innovative solutions from one context can be implemented elsewhere – for networking between health and research authorities, ministries, and regulatory environments.

The GDPR, in the context of digital health infrastructures, can be instrumental in setting the scene for an open dialogue and possible cooperation with and among the health research and innovation stakeholders, and the digital health community/users. However, a robust ethics component has to be developed for the technological, governance, management and ethical requirements of health research data, as well as for the development of public trust and support for this field.

ICT and Healthcare: The Challenge for Social Theory

Dr Malcolm J Fisk,
Senior Research Fellow, CCSR, De Montfort University
(malcolm.fisk@dmu.ac.uk)

In 2008, the European Commission received the preliminary findings of a report on 'ICT and Ageing' [1]. The context was one where the European Commission was reported as wanting 'better leveraging of the potential generally provided by ICT for independent living in an ageing society'. This was seen as 'both a social necessity and an economic opportunity'. The focus was, perhaps, unsurprisingly around what was seen as a demographic challenge - a key aspect of which was answering the question as to how 'independent living' could be promoted for a growing number of people many of whom were seen as having health and support needs. The context was one, however, where 'wider mainstreaming of ICT-enabled solutions within real world service settings has to a large extent yet to occur' and where certain barriers to adoption were noted. These included shortcomings in the communications infrastructure, the capacity (and knowledge) of service provider organisations and 'medico-legal uncertainties'. More importantly from the point of view of this appraisal the report signalled some ethical and regulatory concerns that related to the monitoring capacity of some of the technologies concerned (this focusing, in the main, on social alarms and home telehealth).

2008 provides us, therefore, with a benchmark. There was clearly the desire to seek ICT based 'solutions' (this term, of course, betraying a view of the ageing population as a 'problem') but there was a nascence of concern around their ethical implications. However, no reference was made in the report to social theories that might have been corralled to support an ethically-based approach whereby ICT could be harnessed in the area of healthcare in ethically appropriate ways.

Now, a decade later, there has been considerable development in the world of ICT and healthcare. This has been, in part, facilitated through the development of better communications infrastructures that is evident in all EU countries. As part of its work to promote the 'digital economy', the European Commission has recently undertaken consultation on 'Health and Care in the Digital Single Market' (outcomes are awaited). The Digital Economy and Society Index (DESI), meanwhile, bears testimony to steady, year on year, increases in the use of the Internet, the integration of digital technology (in business and commerce) and the range of digital public services [2].

Some 'market' opportunities around ICT are, therefore, being developed. For many of these the ethical issues are focused around good governance and the 'dimensions' associated with 'responsible research and innovation' (RRI) (itself a European Commission initiative) [3]. A cross-over that includes consideration of the needs of product and service users (patients) can be noted, however, with a recent RRI oriented project (Responsible Industry) specifically having examined products 'for an ageing society' that relate to the 'delivery' (sic) 'of health and social care to an ageing society'. Much of the focus for the latter was on the use of sensors to gather personal data – for which a number of ethical concerns were identified. The report in question affirmed that the application of new ICT-based systems 'while reinforcing the person's autonomy at home, may also lead to more control being taken by family relatives over the private life of the older person' [4]. General principles that should be considered for ICT products for older people in need of care (deemed 'vulnerable consumers') were listed in the report as follows: individual rights and liberties; personal safety and health; autonomy, authenticity and identity; quality of life; social isolation; integrity and dignity; bodily integrity; social safety; distributive justice, equality and 'dual use' of developed technologies.

Here lies the beginning of an ethical framework that may have its place in relation to ICT and healthcare. This is complemented by initial work of the European Commission funded PROGRESSIVE project that (in a preliminary report) identifies nine 'ethical tenets' as follows [5]: accessibility and usability; affordability; autonomy and empowerment; beneficence and non-maleficence; care, protection and support; equality, equity and justice; inclusion, non-discrimination and social impact; interoperability; and privacy, safety and security.

Armed with this range of principles and ethical issues, it becomes possible to examine whether, and the extent to which, these resonate with the work of a small range of social theorists. Expectations in relation to this are low insofar as many of the social theories around ageing and health relate to a

context where ICTs were poorly developed. Indeed, the 'lead' in terms of ideas and innovation around ICT and health has been taken by technologists and others who have been quick to consider the commercial opportunities that could arise within what they might recognise as the 'Silver Economy' - noted by the European Commission (in relation to a definition from Oxford Economics) as 'the sum of all economic activity serving the needs of those aged 50 and over including both the products and services they purchase directly and the further economic activity this spending generates' [6].

The perspective explored in this paper, however, has less to do with markets and more to do with rights. Reference points for the ethical dimensions relate, in the main, to the Responsible Industry and the PROGRESSIVE projects.

These are then linked with the work of five social theorists (or, rather, four social theories) and *their* ethical touchstones. The theorists are Tom Beauchamp and James Childress; George Agich, Joan Tronto and Peter-Paul Verbeek [7, 8, 9, 10]. The respective merits of their approaches are considered, most notably around the issues of autonomy, agency, observation and responsibility. Importantly aspects of their work, particularly those espoused by Tronto and Verbeek, carry resonance with the ethical issues and some related tensions that relate to ICT and healthcare and may help in the re-examination of social theories in this rapidly developing digital context.

References

[1] Kubitschke L, Gareis K, Műllller S, Cullen K, Delaney S, Taylor LQ, Wynne R and Rauhala M (2008) 'ICT and Ageing: European study on Users, Markets and Technologies' empirica (Bonn) / Work Research Centre (Dublin).
[2] See https://digital-agenda-data.eu/charts
[3] Wilford S, Fisk M and Stahl B (2016) 'Guidelines for Responsible Research and Innovation', Centre for Social Research and Innovation, De Montfort University, Leicester.
[4] Porcari A, Borsella E and Mantovani E (2015) 'Responsible Industry: A Framework for Implementing Responsible Research and Innovation in ICT for an Ageing Society' Italian Association for Industrial Research, Rome.
[5] See www.progressivestandards.org for a project description.
[6] European Commission (2015) 'Growing the European Silver Economy' Background Paper.
[7] Beauchamp T and Childress J (1985) 'Principles of Biomedical Ethics' Oxford University Press;
[8] Tonto JC (1993) 'Moral Boundaries: A Political Argument for an Ethic of Care', Routledge, Oxford;
[9] Agich GJ (2003) 'Dependence and Autonomy in Old Age: An Ethical Framework for Long-Term Care' Cambridge University Press (updated from original in 1947);
[10] Verbeek PP (2005) '*What Things Do: Philosophical Reflections on Technology, Agency and Design*' Pennsylvania State University Press.

Understanding Blockchain Technology and Applications in the Healthcare Domain

Ms Sukhvinder Hara,
Senior Lecturer, Middlesex University
(s.hara@mdx.ac.uk)

The blockchain protocol was first described by Satoshi Nakamoto in 2008 (Nakamoto 2008) in the context of payment systems, most notably "Bitcoin". At its core, the Bitcoin network maintains a ledger called the blockchain. Within this public ledger are the records of all transactions (and grouping of transactions into blocks) that have been committed upon satisfaction of the protocol requirements and network consensus (Bonneau et al. 2015). These transaction records are placed into the blockchain by a validation process called mining, which has two main objectives: to commit valid transactions and to generate new Bitcoins. This process is incentivised by providing miners with a financial reward for each mined block. Any node in the Bitcoin network may participate in this process by committing their resources needed to mine (computer power and energy). To improve their chance of success, miners often join mining pools thereby combining their resources to solve the proof of work algorithm problem (Teutsch et al. 2017). Once transactions are committed into the blockchain they cannot be modified i.e. blockchains are immutable.

Blockchains once traditionally affiliated with payments systems, have piqued the interest of many domains. One specific context in which blockchain technologies have been applied are in healthcare applications. This is because any healthcare treatment involves a number of transactions, and the present method of processing transactions potentially leads to transactional inefficiencies (e.g. needing thirds parties to verify transactions). Use of the blockchain removes many of these transactional inefficiencies and allows transactions to be processed efficiently. The distributed nature of the blockchain makes data sharing within the healthcare domain more efficient. Unlike the Bitcoin network, healthcare blockchains can be closed and permission based with "controlled ownership of mining" between stakeholders (Yuan et al. 2016), thus providing security and confidentiality. Use of blockchains in healthcare provides numerous benefits especially over the current outdated legacy systems which are often incompatible between healthcare providing stakeholders. Recognising this potential, a number of initiatives and proof-of-concepts have been presented. Blockchain technology has been used in many healthcare applications for example: managing electronic health records (Yuan et al. 2016), managing the treatment of patients between different stakeholders (Ekblaw et al. 2016), and dispensing of prescriptions to reduce "overprescribing and prescription fraud" (Blockmedx 2017) .

Despite all the benefits, concerns have been raised about distributed ledger technology in terms of scalability issues, cost of systems, and whether return on investment at a larger scale is realistic or achievable (Angraal et al. 2017). Furthermore, the General Data Protection Regulation 2018 (GDPR) has introduced the right of erasure (right to be forgotten) that will oblige data controller to erase personal data where certain grounds given in Article 17 apply. These grounds include that the data are no longer necessary in relation to the purposes for which they were collected/processed or that there are no overriding legitimate grounds for processing. The immutable nature of the bitcoin may pose a conflict with the GDPR, however, in most healthcare applications, the grounds for exercising the right of erasure may not apply.

References

Angraal, S., Krumholz, H.M. & Schulz, W.L., 2017. Blockchain technology: Applications in health care. Circulation: Cardiovascular Quality and Outcomes, 10(9), pp.1–4.

Blockmedx, 2017. Combating Prescription Drug Abuse with a Secure Decentralized Application Built on Ethereum. Available at: https://www.blockmedx.com/doc/BlockMedxWhitepaper.pdf.

Bonneau, J. et al., 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies Joseph.

Ekblaw, A. et al., 2016. (MedRec) A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. Proceedings of IEEE Open & Big Data Conference. Available at: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf.

Mukhopadhyay, U. et al., 2016. A brief survey of Cryptocurrency systems. 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp.745–752. Available at: http://ieeexplore.ieee.org/document/7906988/.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, pp.1–9. Available at: http://s.kwma.kr/pdf/Bitcoin/bitcoin.pdf.

Teutsch, J., Jain, S. & Saxena, P., 2017. When cryptocurrencies mine their own business. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 499–514.

Yuan, B., Lin, W. & Mcdonnell, C., 2016. Blockchains and electronic health records. Massachusetts Institute of Technology website, pp.1–23. Available at: http://mcdonnell.mit.edu/blockchain_ehr.pdf.

The General Data Protection Directive: Some Implications for the Healthcare Sector

Dr Carlisle George,
Associate Professor & Barrister, Middlesex University
(c.george@mdx.ac.uk)

In May 2018, Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), is scheduled to come into effect in the European Union (EU) updating and replacing the EU Data Protection Directive 95/46/EC (aimed at protecting the privacy of individuals and the use of personal data). The GDPR places specific obligations on data controllers and data processors in organisations (that process personal data) either within the EU or outside the EU but offering goods/services in the EU. The latter gives the GDPR extra territorial effect, which implies that non-EU based organisations in the healthcare sector (e.g. organisations carrying out research or clinical trials) will be subject to the GDPR. While the key principles and concepts of the current Data Protection Directive 95/46/EC remain, the GDPR aims to strengthen existing individual rights, creates new rights (e.g. the right to erasure of personal data) and places greater accountability on organisations. Data controllers must put appropriate technical and organisational measures in place to ensure that all processing complies with requirements under the regulation. Data processors must be able to demonstrate compliance by maintaining records of their processing activities. The Regulation has a stronger focus on data privacy and security, mandating data protection by design and default, including the use of privacy enhancing technologies such as pseudonymisation and encryption. Further pseudonymised data (often used in the healthcare sector when conducting clinical trials) is now classed as personal data if it can be used to re-identify individuals. Organisations are now mandated to carry out data protection impact assessments in some circumstances. In relation to the healthcare sector these circumstances will include when processing large amounts of health-related data (such as in clinical trials) or when processing data using new technologies. In the event of any data breach, organisations are now obliged to notify the appropriate supervisory authority within 72 hours and to notify affected individuals without undue delay (if the breach will pose a high risk to the rights and freedoms of these individuals).

With regard to data relating to health, the Regulation introduces three new definitions namely: “data concerning health”, “genetic data” and “biometric data”. These three forms of data are included in the category of “sensitive personal data” hence requiring a higher standard of protection than ordinary personal data. Specifically the processing of sensitive personal data is prohibited subject to some exemptions including health-specific conditions. Any processing in the healthcare sector must therefore be aware of how these exemptions apply. The Regulation also enables Member States to impose further conditions on the processing of genetic, biometric or health data. A related issue is that the GDPR has strengthened the definition of consent and the recording of consent for the processing of sensitive personal data. Consent has to be freely given, specific, informed, an unambiguous indication of the data subject’s agreement and must be capable of being withdrawn without detriment.

Scientific research is automatically deemed to be a lawful compatible purpose, meaning that personal data initially collected for any purpose can be processed for scientific research purposes. Where personal data is processed for scientific research purposes, the GDPR provides exemptions to various subjects’ rights if organisations implement appropriate safeguards (e.g. “technical and organisational measures to ensure data minimization”).

The GDPR imposes harsh fines for non-compliance/infringements, i.e. up to 4% of an organisation’s annual turnover, an important development in light of the relatively high number of security incidents reported in the UK healthcare sector compared to other sectors (Raywood, 2017).

This paper discusses some important implications of the GDPR for the healthcare sector. The previous discussions suggest that organisations in the healthcare sector must review their present operations and procedures to be in compliance with the GDPR, especially ensuring that: the legal basis exists for the processing of data relating to health; any further restrictions on the processing of data relating to health in a particular Member State is complied with; data controllers and data processors understand their responsibilities; the forms and wording requirements for obtaining/recording consent are updated; a data protection by design and default approach is taken, including implementing appropriate technical and organisational measures for processing activities (e.g. pseudonymisation, and

encryption); pseudonymised data that can lead to the identification of an individual complies with the GDPR requirements; data protection impact assessments are carried out when the circumstances apply; and subjects' rights and when they apply are understood and complied with.

References

EU GDPR (2018), GDPR Portal Site Overview, https://www.eugdpr.org/

Raywood, D (2017). UK Healthcare Accounts for 43% of all Breaches. InfoSecurity Magazine, https://www.infosecurity-magazine.com/news/uk-healthcare-43-breaches/

Cross-Border Exchange of eHealth Data in the EU

Dr Ioannis Komnios,
Project Coordinator, The KONFIDO Project
(i.komnios@exus.co.uk)

Abstract: In order to facilitate cross-border exchange of eHealth data in the EU, the OpenNCP community has designed and developed a set of open source components that can be adopted by participating nations. The KONFIDO project addresses the challenges of secure storage and exchange of eHealth data, as well as protection and control over personal data at a systemic level, through the implementation of six innovative technology pillars, including homomorphic encryption and blockchain.

Keywords: Cross-border exchange; eHealth data; Security; OpenNCP.

The epSOS project [1] aimed to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. In the first phase, epSOS targeted the exchange of two types of information:

- *Patient Summary* that provides an overview of the most important medical data for patient treatment and;
- *ePrescription* for cross-border use of electronic prescription.

The technical outcome of epSOS has been the OpenNCP open source project [2] (currently supported by eHDSI [3]) that aims to design and develop a set of open source components that can be adopted by participating nations to build their own implementation of the National Contact Point (NCP). In this way, NCP-B (i.e. the NCP in the country of treatment) can communicate and exchange eHealth data with NCP-A (i.e. the NCP in the patient's country of affiliation). As far as security is concerned, OpenNCP has defined the measures that must be put in place to grant the confidentiality, integrity, authenticity and availability of cross-border communication of eHealth data [4].

To further enhance security, the European Commission (EC) has funded the KONFIDO project [5] to advance the state-of-the-art of eHealth technology with respect to the four key dimensions of digital security: *data preservation*, *data access and modification*, *data exchange* and *interoperability and compliance*. In particular, KONFIDO takes on a holistic approach by targeting all architectural layers of an IT infrastructure, such as storage, dissemination, processing and presentation, extending the results of a series of successful previous projects, such as epSOS, STORK [6], DECIPHER [7], EXPAND [8] and ANTILOPE [9]. KONFIDO's implementation approach is based upon six technology pillars:

- The new security extensions, such as Software Guard eXtension (SGX) [10], provided by the main CPU vendors;
- Physical Unclonable Function (PUF)-based security solutions based on photonic technologies;
- Homomorphic encryption mechanisms;
- Customized extensions of Security Information and Event Management (SIEM) solutions;
- A set of disruptive logging and auditing mechanisms based on blockchain;
- A customized eIDAS-compliant eID implementation.

KONFIDO is working on an integrated prototype based on the aforementioned technologies to be tested in three Member States, namely Denmark, Italy and Spain. In parallel to the technical validation, the developed solution is also assessed in ethical and legal terms.

From the legal point of view, providing cross-border health services needs to adhere to the relevant directives and agreements. Directive 2011/24/EU [11] clarifies the legal rights of patients in cross-border healthcare. The Directive covers both public and private healthcare providers, and requires Member States to provide information to patients and the public on their rights and options. As part of the same Directive, the eHealth Network has been created, providing "Guidelines on a minimum/non-exhaustive patient summary dataset for electronic exchange" [12] in 2013 and the "Agreement for the exchange of health data" [13] in 2017. Cross-border exchange of health data is further submitted to the application of European and national legal rules regarding the protection of personal data, including the General Data Protection Regulation (GDPR) [14].

The efforts that started a decade ago prove that providing secure cross-border exchange of eHealth data is a complex process. By 2020, the eHDSI Operations Community and the KONFIDO project will have made a significant step towards the wide implementation and adoption of cross-border eHealth services in the EU.

Notes

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727528 (KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services). This paper reflects only the authors' views and the Commission is not liable for any use that may be made of the information contained therein.

References

1. epSOS project (2008-2014), http://www.epsos.eu/home/about-epsos.html
2. OpenNCP Community, https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Introduction
3. eHealth Digital Service Infrastructure (eHDSI), https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home
4. Security services of the eHealth DSI, https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Section+II+-+Security+Services
5. KONFIDO project (2016-2019), http://www.konfido-project.eu/konfido/content/what-konfido-project-about
6. STORK I and II projects (2008-2015), (https://www.eid-stork2.eu
7. DECIPHER project (2013-2017), http://www.decipherpcp.eu
8. EXPAND project (2014-2015), https://ec.europa.eu/digital-single-market/en/news/expand-deploying-sustainable-cross-border-ehealth-services-eu
9. Antilope project (2013-2015), https://www.antilope-project.eu/front/index.html
10. Intel® Software Guard Extensions (Intel® SGX), https://software.intel.com/en-us/sgx
11. Directive 2011/24/EU, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF
12. Guidelines on a minimum/non-exhaustive patient summary dataset for electronic exchange, https://ec.europa.eu/health/sites/health/files/ehealth/docs/guidelines_patient_summary_en.pdf
13. Agreement for the exchange of health data, http://jasehn.eu/wordpress/wp-content/uploads/2017/10/D6.2.B_RECOMMENDATION_for_the_Governance_and_Implementation_of_the_Agree.._.pdf
14. General Data Protection Regulation (GDPR), https://www.eugdpr.org

Own it. Personal Data Trading as an Alternative Model

Ms Mitzi László,
Neuroscientist and Social Entrepreneur, OWN
(mitzilaszlo@gmail.com)

The Data Trading Industry

Data is the new oil. In 2011, three of the five top companies by stock market capitalization were oil companies, only five years later all top five were America data companies (Bloomberg). OPEC has been replaced by GAFAM: Google, Amazon, Facebook, Apple, and Microsoft.

While the tech services, such as search engines, communication channels, and maps, are provided for free, the new currency that has been uncovered in the process is personal data. The Attention Economy is an approach to information management that treats human attention as a scarce commodity. GAFAM use techniques explained in the book Hooked by Nir Eyal to ensure that users maximise screen time. Apple stated that users unlock their iPhones 80 times per day on average. On average, Americans spend more time in front of a screen that they do asleep (Common Media Sense, 2017). This attention is then sold to those wishing to advertise. These advertisements are targeted using data so as to be more efficient at converting the attention into a desired outcome, for example, spending money or voting in a particular way.

How much is the data of one individual worth? According to Statista, in 2016 Google had a revenue of 89.5 billion dollars and 1 billion Gmail users meaning that, each person per year generates roughly 90 dollars in 'data added value'. There are many holes to be picked in this rudimentary calculation: the financial figures of tax evading companies are unreliable, would revenue or profit be more appropriate, how do you define an active user, you need a large number of individuals for the data to be valuable, would there be a tiered price for different people in different countries, not all Google revenue is from Gmail, etc. Although these calculations are undeniably crude, the exercise serves to make the monetary value of data more tangible. The examples given only cover one case, but if we extend profits from data sales to other areas such as healthcare the monthly profit per individual would increase.

The Chinese government is widely using facial recognition technology in public spaces to match physical identity with online behaviour. Individuals are given a social index score based on their behaviour which determines the extent of their access to public services.

Ultimately the personal data trading industry is possible because individuals give consent by clicking 'accept' on the terms and conditions. However, a negligible number of individuals actually read the terms and conditions which are constantly changing and have estimated to take a month of every year to read.

Why we need a rethink

While ethical checks are extensive for research, they are close to non-existent in the data trading industry, making it difficult for public research to keep up. It has become increasingly difficult for users to reject the terms and conditions and still remain an active participant of society. The right to privacy attempts to provide some resistance to corporate surveillance, however the business model behind the data trading industry means there is a large incentive to identify individuals and profile them. Ibarra et al (2018) propose that GAFAM should pay their users for collecting their data, which has also been proposed in the form of a universal basic income from GAFAM. However, this does not answer the question of voice: a select wealthy few would still be deciding on behalf of their users how their data is used.

Like it or not, the human digital identity is a consumable product and other people are currently deciding on behalf of others what to use their personal data for. From this standpoint an alternative model has been designed.

An Alternative Model: Personal Data Trading

The ultimate goals are:

- More equitable global resource distribution
- A more balanced say in allocation of global resources

Personal Data Trading (PDT) is a framework that gives individuals the ability to own their digital identity and create granular data sharing agreements via the Internet. Rather than the current model which tolerates companies selling personal data for profit, in PDT, individuals would consciously sell their personal data to known parties of their choice and keep the profit.

How would PDT work from the perspective of the individual? The individual would download an app, login, initiate personal data collections through sending data access requests, and then reject or accept data sales proposals presented via the app.

At the core is an effort to re-decentralise the Internet. Importantly, this is more about data ownership rather than data transactions. Considering we do not yet know the exchange rate of data and therefore would not be able to define a unit, or token, blockchain is not a silver bullet solution to enabling personal data trading.

There are approximately thirty personal data trading initiatives globally. Notable, the inventor of the World Wide Web, Sir Tim Berners-Lee is leading one of these initiatives. Own (www.ownyourdata.xyz) was founded in 2014 by Mitzi László in Amsterdam and is one of the first personal data trading initiatives.

The governing principle of PDT is that individuals own their own personal data. The collective of one individual's personal data forms a digital identity (or perhaps digital alter ego is more fitting). A digital identity encompasses all of our personal data shadowing, representing and connected to our physical and ideological self. In Europe, data access requests mean that individuals can simply ask for their data and organisations are obliged to provide it. However, the customer service and bureaucracy involved in auctioning these data access requests mean that a tool is needed to automate the process and ideally create an application programming interface under a standardised certificate of data handling norms.

Data is sold in aggregate form describing a group. For example, 20% of Amsterdam eats Muesli for breakfast, NOT, Anna eats muesli for breakfast. The algorithms generating these metrics need ethical checks similar to those applied to public research standards. The algorithm, time frame, data input, data receiver, recurrence of sale, and price, need to be presented to the individuals who is ultimately the one to decide to give informed consent or not. In the Internet era, perhaps it makes sense to have an international agency to make these ethical checks to ensure personal data trading has a positive impact on society.

Enhancing the SCIROCCO maturity model: Scaling-up integrated care in Europe[1]

Ms Diane Whitehouse[1], Dr Tamara Alhambra-Borrás[2] & Ms Cristina Alexandru[3]

[1]EHTEL (Belgium)
[2]Polibienestar Research Institute-University of Valencia (Spain)
[3] University of Edinburgh (Scotland)

(diane.whitehouse@thecastlegateconsultancy.com)

Keywords: SCIROCCO, focus group(s), qualitative, quantitative, tool.

1) Introduction

Integrated care is of considerable importance in Europe, joining together different parts of the different Member States' health and care systems. Europeans want increasingly to be able to scale up these activities and make sure that they are planned well.

Developed as part of the SCIROCCO project [1], the SCIROCCO tool incorporates the Maturity Model for the adoption of Integrated Care [2] developed by the European Innovation Partnership on Active and Healthy Ageing's action group B3 on integrated care. The SCIROCCO tool can be used to scale up integrated care, across different health and care sectors, in a range of communities, and at different levels within health systems or care systems.

This short paper explores the development of and evaluation processes for the SCIROCCO tool, as well as how end-users' view it – through a collection of their opinions, experiences and perspectives. Ultimately, the aim is to make the SCIROCCO tool much more broadly usable, not only in the field of integrated care but also potentially in a variety of fields and sectors. **The workshop presentation itself will give workshop attendees an overview of how the tool works and focus on a series of use cases**.

2) Theory/Methods and Preliminary Findings

Since the project launch in April 2016, the SCIROCCO tool has undergone two iterations, each followed by an evaluation of its usability through use of an on-line questionnaire. After the second iteration, the end-users of the tool have been interviewed in focus groups. This paper focuses on the outcomes of the focus groups in three European regions (Scotland; the Basque Country, Spain; and Norrbotten, Sweden).

Usability of the tool

Results from the first iteration of the tool were mostly positive, but indicated the need for a clearer way of editing the questionnaires, and a more effective handling of the SCIROCCO dimension scoring rankings. Both of these comments were addressed in the second, and current, iteration of the tool.

End-users' perspectives

With regard to the experience of using the SCIROCCO tool, all stakeholders involved in the self-assessment reported **positive experiences** when using the tool. Most of them highlighted that the tool provided them with a **faithful representation** of their health/care system. In general, they agreed that the value of the tool is in the discussion or **consensus-building** process. Regarding the enhancement of the tool, focus group participants pointed out the need for the tool to be available in the region's **local language**. Moreover, some participants stated that there should be **more distinction between criteria** on some of the 12 SCIROCCO dimensions. The dimension entitled "breadth of ambition" particularly seems to need refinement. There were mixed views offered on whether the justifications offered for any answers given need to be automated (or not). **Further options for uses of the SCIROCCO tool have also been discussed, including undertaking regular assessments, and deciding on initiatives, programmes, and projects in which to get involved**.

[1] The SCIROCCO project was co-funded by the Health Programme of the European Union under Grant Agreement No.: 710033 (CHAFEA).

3) Discussions

The methods used to enhance the tool are sound and appropriate. The tool itself is good for facilitating insight into the (local) regional integrated care system. It provides materials that could then lead to the formulation of a (local – even regional or national) strategy or plan.

Usability questionnaires allow the quick gathering of both quantitative and qualitative data on usability. However, they are heavily dependent on participants filling them in completely and thoroughly, both in general and given issues such as questionnaire fatigue and the demands on their time from the project. In general, a better coordinated joint plan for the different types of evaluation of the tool is important for its next iteration.

The focus group mechanism enables further discussion and reflection on any quantitative findings emerging from use of the SCIROCCO tool. The focus groups permit wide-ranging thinking about future alternative uses of the tool. **For the future, in order to collect more data on usability, this topic is planned to also be thoroughly discussed as part of focus groups**.

4) Conclusions

The SCIROCCO tool is judged to be easy-to-use. It facilitates consensus-building among the people (including experts) who conduct the self-assessment process. Moreover, the tool provides useful feedback to the local region on its healthcare system and integrated care maturity. It is particularly helpful in enabling local stakeholders to reflect on the current state-of-play of the system and future its directions, indicating that it can be very useful in terms of policy decision-making. **The next stage of work on the part of the SCIROCCO consortium will be to develop policy-related messages about the SCIROCCO tool.**

5) Lessons learned about the approach

In terms of process, the SCIROCCO project is an initiative in which there is good teamwork; different work packages work together well and can exchange information well. On the one hand, it is useful to have researchers evaluating the usability of the tool and, on the other hand, its usefulness and impact: this collaboration and sharing of findings has proved useful. In terms of triangulation, the results so far show considerable synergy – explained by the fact that the usability of an interface also influences whether it will be as useful and achieve its potential for its users.

6) Limitations of the approach

These results are limited to three regional sites in the case of the focus groups, and to one region in the case of the iteration of the tool; however, five European regions in total are involved in the SCIROCCO project. The current state of analysis of the study findings mean that these initial observations will be further refined by the end of the project in autumn 2018.

7) Suggestions for future research

Future replies to questionnaires from other users and regions and holding of focus groups will help confirm, and add, more issues and suggestions, both to the tool itself and to the numerous uses to which it can be put. Widening the range of regions/countries that can use the SCIROCCO tool will make its validation more effective. Finally, it would be interesting to research in what other fields/domains – besides integrated care – the SCIROCCO tool could be used.

8) References

[1] http://www.scirocco-project.eu/
[2] https://ec.europa.eu/eip/ageing/sites/eipaha

Big (Health) Data, Artificial Intelligence and Black Box Algorithms: Time for Global Standards

Prof Kenneth Goodman,
Director, Institute for Bioethics and Health Policy, University of Miami, USA
(kgoodman@med.miami.edu)

The health information technology multiverse has received guidance and critical analysis from the ethics and legal communities for more than three decades. Some of this support was requested, and some has even been accepted. In the process, ethical issues were identified and analyzed, best practices mooted and recommended, education and curriculum development celebrated. The issues, practices and curricula have correctly emphasized privacy and confidentiality, appropriate uses and users, decision support, clinical standards and the ancient relationship between clinicians and patients. There has however been an omission, a major and important omission, an omission underpinning all other ethical, legal and social issues.

Hidden – buried? obscured? concealed? – whether by design or not, are billions of lines of computer code, the very digital foundation of all electronic health records, research registries and data bases, data mining algorithms, programs that emulate or replicate human intelligence, user interfaces, mHealth apps, data sharing protocols and, well, so on.

If we are to realize the full potential of Big Data and Artificial Intelligence, we absolutely must attend to some familiar and several new questions shaping the field of software engineering. Some such questions: How, by whom and under what values was this code written? Was it shared, and by whom? Will it be shared; if not, why not? Did those who wrote or crafted the code have any responsibility to attend to its future uses? If so, how?

Answers to these questions, some of which are empirical and some conceptual, should shape a new generation of guidance, governance and education in the world of health information technology.

The global health informatics community needs to revisit and refine a number of ethical issues, some already recognized, underpinning the crafting of computer code:

- Annotation and documentation
- Fitness for purpose; safety
- Testing and analysis; quality control
- Version control
- Data sharing and transparency
- Provenance and intellectual property

By informing and guiding a new generation of code writers, thus helping to professionalize their craft, attention to ethics can at the outset make a plenary and legitimate claim to improving health, respecting rights and fostering reproducibility in research. Because software production is already internationalized, an international initiative is required. Standards, let alone global standards, are difficult to develop, but in all other endeavors that matter – that affect the lives of billions of people, that weigh heavily on collective safety, public trust and community purses – we have come to accept and even rely on evidence-based and ethically optimized standards. Big Data and AI require this. Global standards can help achieve it.

Error is more complex than Ethics

Prof Harold Thimbleby,
Professor of Computer Science, Swansea University
(harold@thimbleby.net)

Abstract: In Western healthcare, *preventable error* is recognised as the third biggest killer (on a par with cancer and cardiovascular diseases). Computers are involved in every aspect of healthcare, from booking appointments through to magnetic resonance imaging (MRI) scans. Although there is no useful data, it is likely that computer-related error is significant. When errors occur, the clinicians at the "sharp end" are blamed rather than any underlying problems; this raises legal, ethical and social issues. If we are to learn how to improve systems and avoid future errors, we need more deliberative ethical thinking than "justice by scapegoating."

Introduction

Clearly, computers can transform healthcare. On the one hand, the recognition of computer-inspired transformation closely matches market forces with political and consumer desires. On the other hand, enthusiastic market demands lead to acquiescence over low quality.

Computer error falls into a large, under-recognised area that induces healthcare errors and patient harm. It is largely preventable. Here are some stark comparisons about training and skills:

- It still takes an anaesthetist, if good enough to be accepted on a course, 8 years to qualify to give a patient anaesthetics.
- Somebody who wants to program a drug delivery system can start now with no training or qualifications.
- A bad anaesthetist might kill one person at a time; bad programmers can kill as many patients as there are infusion devices made to their design.
- There is no plausible way any clinician could sustain a level of harmful effects comparable to bad programming without triggering investigation and action.
- If something goes wrong, programmers protected by the European Medical Device Directive (and other harmonised laws in the USA and elsewhere); they have probably required the anaesthetist to indemnify them.

Error as a dual of ethics

Let us define error as a *failure to do good*. Hence, for every ethical stance, there is a dual error stance; for example, deontology defines good through rules, so error may equally be defined by deviance from rules. Situational ethics has a dual in error root cause analysis (i.e., to explore what situation caused the error). Virtue ethics has a dual in error-prone people: errors are committed by people who, clearly, are not virtuous. (This perspective slides into *blame culture*: a previously virtuous person involved in an error has betrayed our trust. No longer virtuous, they deserve punishment. The logic of this argument is very seductive, not least because it is simple and cheap.)

Two case studies

Harms to patients are estimated to be in the 100,000s per year in the UK. Computers are involved in all stages of the patient care pathway, and therefore bugs (i.e., errors in design) will contribute to treatment errors. For example, when a nurse enters a number correctly, but it is misinterpreted due to a bug, or enters a number incorrectly that is not spotted by the computer because of a bug, both cases can contribute to patient harm.

Clinical examples are complex, so we have chosen two simple examples to illustrate our points: one refers to the calculation of drug dosage through the use of calculators; the other to address data available on a prescription form.

Drug doses are often calculated on calculators. Sometimes a calculation goes wrong: patients can die from over-doses (or be ineffectively treated with an under-dosage). Sometimes nurses are sacked, or even commit suicide, after adverse incidents. Note that it is hard to spot calculation errors; the point of using calculators is that we, the users, do not know the right answer. We rely on the calculators to calculate correctly.

Calculator users may make an error they notice and therefore wish to correct. The Casio HR150TEC has a delete key to help correct errors. Unfortunately, its delete key ignores the decimal point. Hence trying to correct, say, 2.5 to the intended 25 will likely leave 5, which is out by a factor of five. If the result is involved in a longer calculation, the final error will be very hard to spot and may cause harm.

The HR150TEC can keep a record of what it does. If a user encounters the design error described above, the log records what the calculator did. If used in an investigation, the log would seem to show the user incorrectly entered 5 and did not correct it.

Figure 1. Patient data.
(Note that the doctor's name is not Jon (it is longer), and the address is not Medical Ce.)

Figure 1 shows a simple error. The computer has truncated the doctor's name and address, which will encourage unnecessary errors. This is an avoidable bug: the patient's name was not truncated.

Discussion

These two case studies showed common bugs in relation to medical devices and systems. The following points are critical:

- Manufacturers have years to develop products, to test them and follow best practice. Leaving bugs in systems must be (to put it charitably) driven by commercial realities.
- The example bugs described in the two case studies have been around for years, unfixed. If manufacturers do not notice bugs (which is an approach that seems preferable to noticing but not caring), what hope is there for clinicians to notice and understand bugs or report them correctly?
- Clinicians work under time-critical, high pressure demands. They and their patients rely on systems to work, as they do not have the cognitive capacity to continually check them.
- Standard resilient processes, such as two nurses working together as a team to check each other, cannot provide adequate protection against common mode failure (such as we illustrated above) in the systems they use.

Preventable errors will continue to occur that will be incorrectly investigated, and blame will be misdirected. Unfortunately, blaming the closest front-line staff (often nurses) is the cheapest and most expedient solution; taking a manufacturer to court would be expensive and would imply an expensive hospital refit. Blaming the user is self-perpetuating; few people today think that computers are causing errors when the healthcare profession itself suspends so many clinicians. This is a failure of justice.

Conclusions

The duality of error and ethics is proposed as a place to think more clearly about error, combined with an awareness of the pivotal role of ethical computing (considering pre-planned system design, asymmetry of power, inevitability of error within a capitalist ethic) and ethical investigation of bugs.

How Can We Assure the Trustworthiness of Federated Big Health Data Ecosystems?

Prof Dipak Kalra,
President, The European Institute for Innovation for Health Data
(dipak.kalra@eurorec.org)

This presentation examines how to build trustworthiness in large, federated health data ecosystems. It examines current directions in the field, including various drivers. It explores the dominant research infrastructures, and some of the major and minor challenges they present. Looking to potential solutions, the author investigates the need for an overall portfolio of targeted activities. It covers: the implications of the General Data Protection Regulation (due to be applied in May 2018); the adoption of good practices; and clear communication with the general public.

Many European countries have invested in national eHealth infrastructures, which are progressively communicating more and more electronic health record data to support continuity of care and public health strategies. Countries are now launching research infrastructure programmes to scale up the availability of data for clinical research. European infrastructures are now also coming into existence (most recently Switzerland [1] and Germany [2]), and there are plans to establish a European science cloud to share research data [3,4].

The drivers for these research infrastructures are to accelerate and reduce the cost of academic and pharmaceutical industry clinical trials, and to increase the availability of large population data sets for drug development, biomarker validation, pharmacovigilance, rare disease research and health outcomes optimisation. New opportunities are also emerging to engage patients who are accessing their own data, so as to be able to manage their own health care and prevention more effectively and collect personal health data.

By far the dominant model for these research infrastructures is to enable federated (distributed) research access to multiple data repositories. These repositories might be de-identified electronic health records (e.g. in hospitals), disease and procedure registries, cohort studies and biobanks. Research queries might be performed remotely across multiple data sources and the result sets combined, or focused data set extracts might be linked and merged within an approved safe haven for in-depth analysis.

There are important European initiatives seeking to address a number of challenges related with these research infrastructures [5,6]. The major challenges being tackled when establishing infrastructures relate to privacy protection, promoting good practices in data sharing, and the general acceptability to patient populations of reusing (personal) health data for research, the limited adoption today of interoperability standards which make it difficult to combine heterogeneous data sources, and the variable data quality found in electronic health record systems.

Of paramount importance to establishing a trusted federated research ecosystem is the need for compliance with data protection legislation, at a European level and across all European Member States. The General Data Protection Regulation (GDPR) is currently in the spotlight, with particular concerns about uncertainties in national interpretations on the need for and nature of (specific vs. generic) informed consent for research use of routinely collected health data, opt in and opt out models of consent, the status of pseudonymised data, and implications of the “right to be forgotten” on longitudinal research. There is also uncertainty about how the principle of data minimisation applies to big data being curated for long-term hypothesis generation.

One cornerstone of ensuring regulatory compliance and assuring trustworthiness is the definition and adoption of good practices: e.g., codes of practice, and standard operating rules and procedures. Another is the quality labelling of clinical research platforms and tools to ensure the robustness of their privacy protection measures. Staff training and accreditation is also important, in particular the training of clinical research staff in the appropriate handling of data in safe havens and in the conduct of remote queries.

Society as a whole has varied understandings of how clinical research is conducted, and in particular the importance of health data to enable knowledge discovery i.e., research. It is therefore important to promote the value of health-related research to the public, and how people's data can be both used and yet still protected in this process.

The overall goal of a portfolio of good practice measures is to establish and govern a trustworthy clinical research ecosystem while using big health data. This is vital if we are to win greater societal endorsement of public health and research uses of health data. This endorsement of good practices will bring greater confidence in, and reduce the risks both for those providing data for research use, e.g. hospitals, general practitioners, patients, and for those performing the research, managing the data, or sponsoring the research.

1. Swiss Personalized Health Network (SPHN). Web site https://www.sphn.ch/en.html. [Accessed 11th December 2017]

2. Research in Germany. "Germany launches medical informatics initiative". Web page, 31st August 2017. https://www.research-in-germany.org/en/research-landscape/news/2017/08/2017-08-29-germany-launches-medical-informatics-initiative.html [Accessed 11th December 2017]

3. European Commission. European Open Science Cloud. Web site https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud [Accessed 11th December 2017]

4. European Commission. ESOC Declaration. Available from: https://ec.europa.eu/research/openscience/pdf/eosc_declaration.pdf [Accessed 11th December 2017]

5. Kalra, D., Stroetmann, V., Sundgren, M., Dupont, D., Schlünder, I., Thienpont, G., Coorevits, P., and De Moor, G. (2016) The European Institute for Innovation through Health Data. Learning Health Systems, doi: 10.1002/lrh2.10008

6. The European Medical Informatics Framework project. Web site http://www.emif.eu [Accessed 11th December 2017]

CrowdHEALTH: Aggregating and Analysing Big Health Data for Policy Making

Dr Usman Wajid,
Senior Researcher, Information Catalyst
(usman.wajid@informationcatalyst.com)

Abstract: Today's eHealth environment is characterised by the multitude of data sources providing health related information that has not yet reached its full exploitation potential. The CrowdHEALTH approach introduces the paradigm of Social Holistic Health Records (SHHRs) that aggregate clinical, social and human context to establish a one-stop shop for all health determinants. The CrowdHEALTH approach seamlessly integrates big data technologies across the complete data path to facilitate the creation of SHHRs for population segments, providing of Data as a Service (DaaS) to the policy makers. CrowdHEALTH also provides a big-data analytics toolkit to support cross-domain co-creation and evaluation of policies, causal and risk analysis, and for the predictions.

Keywords. Big data, health analytics, public health, policy making

Extended Abstract

The explosion of ICT services led to several devices and platforms providing health related data (e.g. medical records, lab reports, wearable data, etc.). However, the different types of data, in different standards and frequencies create havoc at integration level in any platform. Thus, it is getting increasingly common for important information or events to be missed while analysing health related information e.g. early indications of spatiotemporal development of diseases. On the other hand, the multitude of data sources highlights a unique opportunity i.e. data to be exploited for effective and targeted policy making, development of personalised medicines, forecasting of epidemics and health promotion in general.

Additional to medical records are the health determinants that should also be considered, as highlighted by the WHO [1], including the physical, social and economic environment, genetics, and relationships with friends and family. Today's health records (EHRs and PHRs) are far from being what the citizens consider as of value to their health. Capturing and linking additional information (e.g. behavioural, social etc.) with the data in EHRs and PHRs would be beneficial to analyse prevention strategies, evaluating diseases prevention mechanisms and efficiency of clinical pathways.

Furthermore, collective community knowledge could play a significant dual goal: (i) collect, fuse and analyse information from different entities to extract valuable information for the provision of actionable insights, (ii) provide the ground for targeted health policy making. The impact is apparent: 46% of the respondents in a survey [2] highlighted that information sharing has changed their overall approach towards healthy life. Another survey [3] shows the need and value for sharing health information with others and communities.

With this background, the EU H2020 funded CrowdHEALTH project aims to deliver an *integrated platform that incorporates big data management mechanisms addressing the complete data path: from acquisition, cleaning, to data integration, modelling, analysis, information extraction and interpretation*. CrowdHEALTH will enable proactive and personalized disease prevention and health promotion, while providing decision support to authorities for policy creation, through the exploitation of collective knowledge and intelligence.

CrowdHEALTH explores mechanisms that can be clustered across three main areas: (i) extended health records, (ii) collective health knowledge (i.e. clustered records), both produced and exploited by (iii) big data analysis techniques. As highlighted by CISCO [4]: "Humans evolve because they communicate, creating knowledge out of data and wisdom based on experience". CrowdHEALTH's hypothesis is that the "extended" health records can be exploited to a greater degree if they can evolve by following the human communication paradigm. This metaphor means enhancing records with technologies to exploit the knowledge and experience derived from other records e.g. from patients in the same medical, social and environmental situations. Thus, CrowdHEALTH proposes the evolution of health records in two stages: (i) towards Holistic Health Records - HHRs providing a complete view of the citizen including all health determinants, (ii) towards HHRs Clusters to extract collective knowledge. As depicted in the

following figure, an HHR contains several components: (a) the personal component containing health, social and lifestyle data (such as nutrition or physical activities) collected by either the citizen, her family, friends, etc., (b) the social component containing social care data collected from social care providers, (c) the medical device component containing health data from medical devices (e.g. home care systems or wearables), (d) the healthcare component containing data (e.g. clinical data, diagnoses, medication, etc) obtained by healthcare providers (e.g. primary care systems) and (e) laboratory medical data.

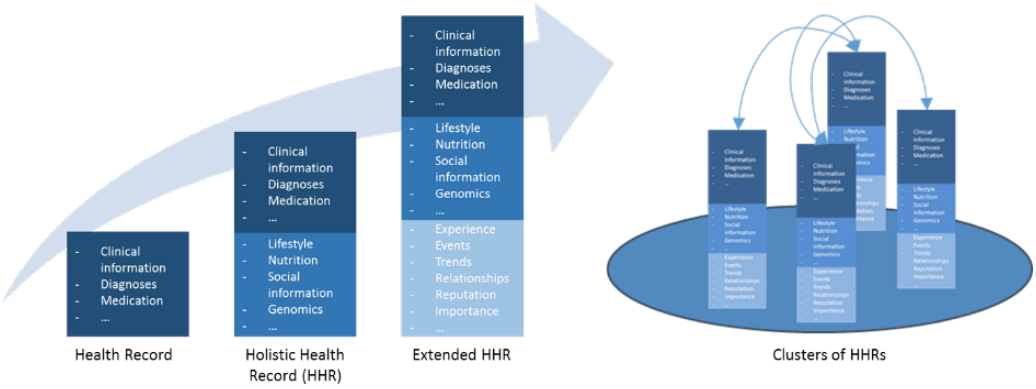

Figure 1. Holistic Health Records and Clusters of Records in CrowdHEALTH.

The HHRs clusters act as living entities, including properties such as experience (i.e. medication experiences of patients), relationship with other HHRs (i.e. relationships with friends and family, and "classification" of relationships as for example patients with the same disease), reputation, events and trends that affect the groups of citizens. This means that HHRs could form networks in an automated way based on a variety of criteria such as lifestyle choices or disease symptoms, and exchange information as experiences.

In the context of the Health Analytic*s*, big data analytics techniques are utilized for carrying out Risk Models & Models Execution, Causal Analysis, Multimodal Forecasting, and Clinical Pathway Mining, upon all the gathered data. The analysis techniques allow the identification of the properties that affect the performance of policies and care plans and help to identify similarities or differences in treatment among groups of patients, indicate major effective factors that affect several treatments. Moreover Multimodal Forecasting techniques estimates the applicability and effectiveness of health policies, their variations and combinations to particular population segments taking into consideration social information and spatiotemporal properties.

In CrowdHEALTH, Policies Creation is facilitated by a policy development toolkit that uses analytic outcomes and a visualisation environment to identify and evaluate indicators that can help in the development of public health policies, which are then evaluated through cost-benefit based analysis techniques. The CrowdHEALTH approach is under evaluation through scenarios with heterogeneous data sources / devices, data to be included in HHRs, target groups (e.g. chronic diseases or youth obesity), and environments (care centers, social networks, public environments, living labs, etc). Exploiting 2 million records and 700.000 streams of everyday activities, while engaging 200.000 users, the platform is expected to exploit the current 7.5 million measurements from 1 million people with additional 200.000 / year being also analysed.

References

[1] World Health Organization, *The determinants of health*, http://www.who.int/hia/evidence/doh/en
[2] Flash Eurobarometer 404, European citizens' digital health literacy, http://ec.europa.eu/public_opinion/flash/fl_404_en.pdf
[3] M.C. Domingo, Managing Healthcare through Social Networks, IEEE Computer, vol. 43, no. 7, 2010
[4] Cisco Internet Business Solutions Group (IBSG), *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*

Promoting Health Apps or Assessing Their Quality? A Reflection on Current Attempts to Govern mHealth

Dr Federica Lucivero,
Senior Researcher in Ethics and Data, The Ethox Centre, University of Oxford
(federica.lucivero@ethox.ox.ac.uk)

Following, the Commission's Green Paper on mobile health (April 2014), early in 2016 the European Commission established a working group with the mission "to develop guidelines for assessing the validity and reliability of the data that health apps collect and process"[1]. Such mission was derived from the results of a public consultation on the Green Paper held in 2015 when respondents identified "safety and transparency of information" as one of the main challenges for mHealth uptake. As this view is explained on the EC website, there a number of ways lack of transparency of information can challenge mHealth uptake: First, the lack of clear evidence on quality and reliability of the increasing amount of lifestyle and wellbeing apps available on the market makes it difficult for consumers to assess their usefulness. Second, quality of data collected and processed by health apps needs to be assessed through a common methodology in order for these tools to be linked to electronic health records and effectively used in clinical practice. Third, if apps are going to be increasingly used by chronic patients and linked to electronic health records, healthcare professionals need to be reassured about the reliability of the apps "in order to be able to recommend apps to their patients and take apps' data into consideration in a treatment/monitoring process."

The working group had therefore been commissioned to "seek to provide common quality criteria and assessment methodologies that could help different stakeholders (users, developers, vendors of electronic health record systems, payers etc.) in assessing the validity and reliability of mobile health applications"[2]. In doing this, the group was encouraged to build on existing initiatives and best practices in Europe.

The working group, established by DG CNECT (Communications Networks, Content and Technology) comprised 20 members - selected based on their expertise and representing civil society, industry and research organisations – and 10 representatives of Member States authorities[3]. They met four times face-to-face in Brussels and four times via conference call. Interim drafts of the guidelines were published on the European Commission website and discussed at two stakeholder consultation events. The final outcome was published in March 2017 and consisted in a report describing the mission and the process of the working group activities. The report lists 13 criteria for assessment[4] discussed by the working group and presents views on such criteria by different stakeholders. The document however is rather inconclusive stating that "by the end of the [last] meeting there was still not a firm agreement between stakeholder representatives, neither on the scope and target groups, nor whether the work should proceed on the basis of assessing both apps and data or only data as foreseen in the original mandate of the Working Group".[5]

Why was it so difficult for this group to provide guidance on this issue? As I was one of the designated experts, in this contribution I offer my reflections on the challenges that this group encountered throughout the process and attempt to draw some more general considerations and lessons to be learnt. In terms of challenges I divide them in two categories: 1) controversies among experts about mHealth; 2) issues of legitimacy of the working group. The first category concerns the conceptual and practical differences in experts' understanding of the guidelines' scope. The controversies that emerged in the discussions reflect the complexity of the field of mHealth and the limitation of current assessment tools. The second category concerns issues that emerged in the negotiations of roles and competences between experts, mediators and the EC officers. These issues boil down to a more general question

1 https://ec.europa.eu/digital-single-market/en/news/new-eu-working-group-aims-draft-guidelines-improve-mhealth-apps-data-quality

2 *ibidem*

3 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3390&NewSearch=1&NewSearch=1

4 Privacy 2. Transparency 3. Safety 4. Reliability 5. Validity 6. Interoperability 7. Technical stability 8. Effectiveness 9. Efficacy 10. Efficiency 11. Accessibility 12. Usability/desirability 13. Scalability

5 p 4 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=34905&no=1

concerning the legitimacy of such a group to draw guidelines and to the democratic role of such working group in European regulation in general and in the mHealth field in particular. Despite being disappointing in its direct output, this exercise can be used to learn some lessons both on the governance of mHealth and the role of EC working groups. Some of these lessons are practical and advocate the need to rethink the design of the process (e.g. selection of expert, role of external consultancy). Other lessons are more normative in nature and require an open discussion and deliberation on the meaning and direction of mHealth policy (e.g. rethinking the distinction between objective vs subjective criteria; defining the legitimate actors who play a role in this context).

The Certification of Apps in An Era of Innovation

Dr Mayoni Ranasinghe & Dr Celia Boyer (Executive Director),
Health on the Net (HON) Foundation
(celia.boyer@healthonnet.org)

Abstract. Can a person without any advanced medical knowledge, tell the trustworthiness and the accuracy of the sources of information she/he accesses on the Internet? The Health on the Net (HON) HONcode certification addresses this issue in websites. However, mobile applications such as health apps are a new dimension of eHealth and present their own unique challenges. This abstract presents this issue and introduces a solution with a drafted Code of Conduct for health apps and connected objects.

Note. In this short paper, we do **not** deal with health apps which are categorized as medical devices, and which have to undergo specific accreditation by the United States Food and Drug Administration.

Introduction

One arena that has greatly changed in healthcare is the way patients see themselves as active participants in their own healthcare. With mobile health apps not only do patients have access to medical information but also to functionalities which can consist of tracking their own heart rate, or blood pressure, medication adherence monitoring, and maintaining a diary with self-filled data such as intake of the day. Health apps offer a personalized response to the user via algorithms using and analyzing tracked and measured data. The Health on the Net (HON) Foundation HONcode, a quality code of conduct for online health information since 1996, has continued to evolve its principles to accommodate the dynamic nature of the internet [1]. After more than 20 years of existence, HON has now become a well-known beacon of trust, so that Web users know they are on safe ground when they see the blue and red logo on a website. But now, there are new challenges to face – developments such as mobile health apps, whether connected or not to objects pose new hurdles to leap.

Health apps usage and challenges

We can estimate that we are only at beginning of the mHealth revolution. Connected objects, linked to m-health apps, are part of daily life of more and more individuals and healthcare professionals. The ubiquity of smart phones, tablets, sensors, wearables, personal trackers and similar wireless smart devices means that huge volumes of data concerning health, fitness, life-style, stress and sleep are being harvested and processed. A report "mHealth App Developer Economics 2016" foresees that the revenues coming from mHealth app-related services will grow by 15% (compound annual growth rate (CAGR)) to reach US$31 billion in 2020. Five hundred and fifty-one million users will by then actively (at least once a month) make use of a mHealth app [2]. The main issue then becomes how to identify the most appropriate, adapted and trustworthy health app out of hundreds of thousands of similar health apps. HON has analyzed what is available on the market in term of guidelines, tools, recommendation and scale to assess the level of trust one can have in a health app. Various organizations have worked on the issue of security, data privacy, and other criteria related to quality in the mobile applications.

In 2014, the United States government hosted multi-stakeholder talks to forge some common ground on mobile app privacy. The result was the Mobile App Privacy Voluntary Code of Conduct, which calls for mobile applications to include a short form privacy notice to disclose their practices related to data storage and usage[3]. However, this service is still not widely used. The American Health Information Management Association has developed a brochure[6] to inform and educate end users about how to select an app, with details on the implication of privacy and personal information. The Mobile Application Rating Scale (MARS) is a scale intended for users of the app with 23 questions, where each item is rated on a 5-point scale from 1 inadequate to 5 excellent [4]. The main sections are Engagement – fun, interesting, customizable, and interactive; Functionality; Aesthetics – graphic design; Information – Contains high quality information; and App subjective quality. Several European organizations or companies have developed their own labels focused on the local market. One example is the French one, which is mhealth-quality.eu by DMD santé (to access the guidelines users are required to register – the evaluation is based on a fee which is not disclosed). As of 5th November 2017, 41 apps were listed on mhealth-quality.eu. In Spain, the Agencia de Calidad Sanitaria de Andalucía has developed a freely available set of guidelines with 31 recommendations distributed across four main groups, such as design and appropriateness, quality and safety of information, provision of services, and confidentiality

[6] http://www.myphr.com/HealthLiteracy/MX7644_myPHRbrochure.final7-3-13.pdf

and privacy [5]. A list of apps, 20 which have been assessed and 70 under evaluation, are available on http://www.calidadappsalud.com/.

The French Health Authority (known as the HAS in French) has published a guideline of 101 rules of good behaviour for health app publishers categorized in five categories: Information to users, health content, security, data usage and technical usage [6]. The HAS is working on producing a simplified version of guidelines especially intended for citizens and their family carers. The European Commission has acknowledged the legal risk in terms of privacy and personal health data and, in July 2016, proposed a Code of Conduct on privacy for mHealth apps [7]. The Code has its origins in the Commission's Green Paper on mHealth (2014) which revealed that 45% of consumers were concerned with unwanted use of their data when using mobile devices for health related activities.[7]

Guidelines and assessment tools of health mobiles apps quality

HON has started to assess the possibilities of adapting the HONcode guidelines to health apps [8]. In collaboration with the French Union for Free Medicine (UFML) and the partners of the Kconnect European project (H2020-ICT-2014-1-644753 kconnect.eu) HON has developed a first draft of quality guidelines for health apps. This first draft is aimed at being available for public consultation in order to receive the views of people from each of the professions involved in the development, creation, assessment, and use of health mobile applications. Thanks to the comments and advice received, HON will be able to create guidelines which will be integrated in its code of conduct, certification, but also in the community-based platform Health Curator[8] developed within the Kconnect European project, funded by the European Commission.

Future steps

In this short paper, we have attempted to provide a brief overview of some of the challenges faced in ensuring the quality of information. However, as developments take place on such a frequent and regular basis, the on-going challenges are very real. Just as the process of information-sharing experiences new developments, so too will quality control in the future. Organizations dedicated to ensuring the trustworthiness of information, such as the HON Foundation, should make innovation in quality control a priority so that quality control can keep up with the ever-changing information technology platform. There is a need to have a global solution that proposes a multilingual approach with an evaluation scheme, that enables users to be trained by experts in the HON approach to health websites, or is combined with a crowdsourcing/community-based solution. Education is a first step to inform users and allow them to make truly informed decisions.

References

[1] https://www.hon.ch/Conduct.html

[2] mHealth App Developer Economics 2016 by research2guidance.com; 6th annual study on mHealth app publishing based on 2,600 respondents October 2016

[3] Multi-Stakeholder Process convened the United States Department of Commerce. Code of Conduct for mobile application ("app") short notices on Application Transparency. 2013. URL:https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf).

[4] Stoyanov SR, Hides L, Kavanagh DJ, Zelenko O, Tjondronegoro D, Mani M Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps JMIR Mhealth Uhealth 2015;3(1):e27 DOI: 10.2196/mhealth.3422

[5] Agencia de Calidad Sanitaria de Andalucía . Complete list of recommendations on design, use and assessment of health apps. . 2017-11-14. URL:http:// http://www.calidadappsalud.com/en/listado-completo-recomendaciones-app-salud/. Accessed: 2017-11-14. (Archived at http://www.webcitation.org/6uxxivo4I)

[6] Haute Autorité de Santé, France, Good Practice Guidelines on Health Apps and Smart Devices (Mobile Health or mHealth) October 2016 https://www.has-sante.fr/portail/jcms/c_2681915/fr/referentiel-de-bonnes-pratiques-sur-les-applications-et-les-objets-connectes-en-sante-mobile-health-ou-mhealth

[7] The European Commission. Draft Code of Conduct on privacy for mobile health applications. 2017-11-14. URL:https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised. Accessed: 2017-11-14.

[8] Draft the first version of quality guidelines for Health Apps by HON Foundation URL: https://www.hon.ch/HONcode/GuidelinesHealthApps.html. Accessed: 2018-02-04.

[7] https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[8] http://www.heatlhcurator.org

Update on Progress with the National Summary Care Records Programme in England

Dr Emyr Wyn Jones,
Summary Care Record - Clinical Lead, NHS Digital, England
(emyrjones@nhs.net)

The Summary Care Record (SCR) is a national record sharing solution, which supports direct patient care by informing the decision making of health and care professionals, thus ensuring safer outcomes for patients. SCRs are electronic extracts sent from patients' GP records and held securely on the infrastructure known as the national Spine. Each SCR contains patient confidential key clinical information.

SCRs were created following local public information programmes (PIPs) involving individual mailings to all people in England aged 15¾ years and over. The SCR is an 'opt-out' consent model: only 1.4% of patients who received PIP mailings chose not to have an SCR. More than 96% of people registered with a GP practice in England (>55 million) now have an SCR containing core details of prescribed medications, recorded allergies and known adverse reactions.

SCRs can only be viewed by staff in organisations with access to the secure HSCN network. All accesses to SCRs are auditable. Privacy Officers in each organisation where SCRs are viewed are trained how to audit accesses to monitor appropriateness. SCRs can be viewed only by health and care professionals providing direct care to patients. Each authorised staff member has to have been issued with a Smartcard with appropriate Role Based Access Controls (RBACs) confirming a legitimate role to allow access to confidential information. Around 120,000 SCRs are viewed each week by health and care professionals providing patient care in settings away from their GP surgery.

As per the NHS Care Records Guarantee, the patient's permission to view should be obtained if the patient is present and is judged to have capacity and the ability to give informed permission. If permission cannot be obtained from the patient (e.g. patient is confused or unconscious) then a clinical decision can be made to view the SCR without the patient's permission, provided this is considered to be in the patient's best interest.

Over 90% of GP practices have improved functionality to populate SCRs with a set of additional information that includes: significant medical history (past and present); anticipatory care information (e.g. information about the management of long term conditions); patient preferences (e.g. communication needs; agreed end of life care packages) and immunisations. Enrichment of the SCR with Additional Information requires the patient's explicit (rather than implied) consent.

A Ministerial Review of the SCR Programme which reported in October 2010 concluded that: *"We should only consider expanding the content of the Summary Care Record when we have built trust in the system and when patients request that we do so. We therefore recommend that new governance be established."* The Review recommended that this governance should *'be driven by patients and citizens in partnership with the professions'*.

The SCR Expert Advisory Committee (EAC) was created to meet this requirement, and ensure that proposals to expand the scope of the SCR are subjected to debate and analysis, and appropriate advice is provided to NHS Digital. The EAC is chaired by a patient representative and its membership includes representatives of professional and patient organisations, the Information Commissioner's Office and the Patient Records Standards Board (PRSB).

The National Data Guardian's office is currently reviewing the Information Governance controls which are in place to secure confidentiality of patient information in the SCR and to ensure compliance with the requirements of the GDPR when they come into force in 2018.

mHealth and the Management of Chronic Diseases: The Rationale for Developing a Suitable Framework

Mr Farad Jusob, Dr Carlisle George & Dr Glenford Mapp,
Middlesex University
(FJ105@live.mdx.ac.uk)

The pervasiveness of chronic illnesses such as diabetes and high blood pressure has resulted in the need to improve efficiency when managing patients with these conditions. One such way that this can be facilitated is through the use of mobile health (mHealth) technologies that can collect real time data from patients and remotely monitor them, drastically reducing the need to visit medical facilities which can in turn reduce healthcare costs. mHealth is "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" (WHO, 2011). It also includes mobile applications (apps) (Martinez et al, 2014; Grindrod et al, 2017) on smartphones that are connected to peripherals such as wearable technologies (e.g. activity trackers or smartwatches) and medical devices (Karim et al, 2014). Body sensors and mobile apps enable the collection of considerable medical, physiological, daily activity and lifestyle data which is used to facilitate personalised treatment for patients as well as enable users to manage their own health by self-assessment (European Commission, 2014)

The use of mHealth to manage chronic diseases brings many privacy concerns. An mHealth system consists of various events from the time that data is first collected from a patient to when data is received and analysed by a medical professional or researcher. Table 1 below describes events that occur when using a mHealth system and associated privacy concerns discovered by various studies referenced in the table.

Table 1: Privacy Threats/Concerns –mHealth and Chronic Diseases

Events	**Privacy Threat/Concern**
Data collection and activity monitoring using wearables or sensors.	- Continuous Monitoring (Avancha et al, 2012) - Volume of Data Collection (Steinhubl et al, 2015) - Invisibility (Brey, 2005)
Transmission of data (e.g. between wearable device and mobile phone, or phone and server)	- Data Security (Steinhubl et al, 2015) - Encryption (Avancha et al, 2012; Steinhubl et al, 2015) - Confidentiality (Harvey & Harvey, 2014)
Location tracking using mobile phones	- Profiling (Avancha et al, 2012) - Surveillance (Shilton, 2009)
Sharing of data with healthcare practitioners and third parties (including researchers, insurance providers)	- Data Use (Unauthorised or Unanticipated) (European Commission, 2011) - Sharing of data (Avancha et al, 2012) - Information misuse/abuse (European Commission, 2011)
Manual data Input	- Data Quality (Avancha et al, 2012)
Use of Mobile Apps	- Encryption (McCarthy, 2013) - Data Control (Arora & Nilse,2014) - Accessibility (Arora & Nilse,2014) - Disclosure risks (Steinhubl et al, 2015)
Doctor to Patient Communication	- Confidentiality (Harvey & Harvey, 2014)

Research by the authors of this paper on privacy frameworks and principles concluded that several important frameworks and principles exist. Some of these frameworks are applicable in the context of healthcare and others are more general in nature. These frameworks include: Health Privacy Project Best Practice Principles; Markle's Common Framework; Office of the National Coordinator for Health Information Technology (ONC) Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information; Generally Accepted Privacy Principles; A Privacy Framework for Mobile Health and Home-Care Systems; Privacy by Design; Organisation for Economic Co-operation and Development Principles; EC Privacy Code of Conduct for Mobile Health Apps; and The General Data Protection Regulation.

Further analysis (by the authors) of the frameworks identified above, concluded that no individual existing privacy framework covers all privacy concerns regarding mHealth and the management of

chronic diseases. Hence current privacy frameworks do not adequately address the privacy concerns regarding the management of chronic diseases when using mHealth solutions.

This paper asserts that the inadequacy of existing privacy frameworks to comprehensively address privacy concerns when using mHealth for the management of chronic diseases, presents a compelling rationale for the design of a suitable privacy framework for the use of mHealth in this context. The design of any new privacy framework for mHealth in this context must address the privacy threats at various events when using an mHealth system. A new privacy framework would also consider other issues aimed at supporting privacy such as: patient education; patient feedback; use of privacy enhancing technologies; use of privacy by design principles; and the continuous evaluation of processes and procedures.

References

Arora S, Yttri J, Nilse W (2014) Privacy and security in mobile health (mHealth) research. Alcohol Res Curr Rev 36:143–151

Avancha S, Baxi A and Kotz D (2012) Privacy in mobile technology for personal healthcare, ACM Computing Surveys (CSUR), 45:1-54.

Brey P (2005) Freedom and privacy in ambient intelligence. Ethics Inf Technol 7:157–166

European Commission (2011) Advice paper on special categories of data ("sensitive data"). http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Accessed 15 Jul 2017

European Commission (2014) Green Paper on mobile Health ("mHealth"). Brussels, 10 April 2014, COM(2014) 219 final.

Grindrod, K., Boersema, J., Waked, K., Smith, V., Yang, J., and Gebotys, C. (2017). Locking it down: The privacy and security of mobile medication apps. *Canadian Pharmacists Journal / Revue Des Pharmaciens Du Canada, 150*(1), 60-66. doi:10.1177/1715163516680226

Harvey MJ, Harvey MG (2014) Privacy and security issues for mobile health platforms. J Assoc Inf Sci Technol 65:1305–1318

Karim (2014) ICT: Wearable Technology – KARIM Foresight Report. INTERREG IV B – 207G, France. (**online**) http://www.karimnetwork.com/wp-content/uploads/2014/11/Wearable-Technology-Final_November2014.pdf Accessed 03 Jul 2017

Martinez-Perez, B., de la Torre-Diez, I., Lopez-Coronado, M., Sainz-de-Abajo, B., Robles, M., and Garcia-Gomez, J. (2014). Mobile clinical decision support systems and applications: A literature and commercial review. *Journal of Medical Systems, 38*(1) doi:10.1007/s10916-013-0004-y

McCarthy M (2013) Experts warn on data security in health and fitness apps. BMJ Br Med J 347(1):f5600. https://doi.org/10.1136/bmj.f5600

Steinhubl SR, Muse ED and Topol EJ (2015) The emerging field of mobile health. Sci Transl Med 7(283):283rv3. https://doi.org/10.1126/scitranslmed.aaa3487

WHO (2011) "mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3" (**online**) www.who.int/goe/publications/goe_**mhealth**_web.pdf. Accessed 15 Jan 2018

Proposing a Novel Comprehensive Information Security Framework for mHealth

Ms Nattaruedee Vithanwattana, Dr Glenford Mapp & Dr Carlisle George,
Middlesex University
(NV166@live.mdx.ac.uk)

The use of mobile and wireless technologies to support achievements in healthcare systems has an enormous potential to transform the face of healthcare across the globe [1]. In the recent years, there has been a huge increase in the number of these technologies to facilitate mobile Health or mHealth. 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]. mHealth is a subset of eHealth, using the benefits from information and communication technologies to support the healthcare service. mHealth solutions include the use of mobile devices, such as mobile phones, body sensors, wireless infrastructures. These devices are used in collecting clinical health data, and delivering healthcare information 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]. mHealth enables users to monitor their own health status and directly facilitates healthcare data sharing with healthcare professionals anytime and anywhere.

mHealth provides a significant potential to tackle the financial challenges of healthcare systems. It delivers more patient-focused healthcare and improves the efficiency of healthcare systems. mHealth provides sustainable healthcare through better planning of patients' treatment which reduces the number of unnecessary consultations. Moreover, mHealth solutions can help patients to take more responsibility for their health through the devices which can detect and report their vital signs, as well as mobile applications that will help them to be more focused on their diet and medication [4].

In mHealth systems, generally sensors which are embedded into mobile devices will collect healthcare data from user using Bluetooth communication. Healthcare data collected will be stored in different databases including the databases of mobile devices and Cloud storage. Healthcare data is classed as "sensitive data" under data protection legislation requiring stricter rules when processing compared to ordinary personal data. Also, it may reveal the state of someone's health which he/she may not want to share with everyone [5]. Databases storing such sensitive data require a high level of security to protect the confidentiality of the data and to prevent unauthorised access.

Generally, mHealth offers smart solutions to tackle challenges in healthcare. However, there are still various issues regarding the development of mHealth systems. One of the most common difficulties in developing mHealth systems is protection the security of healthcare data. mHealth systems are still vulnerable to numerous security issues relating to weaknesses in their design and in data management. Hence, there is a need to develop a comprehensive information security framework for mHealth.

As part of the analysis involved in developing a comprehensive information security for mHealth, this presentation will discuss the most essential security requirements for mHealth systems, assets in mHealth systems that need to be protected, threats which needs to be protect against, and vulnerabilities/weaknesses in mHealth systems. It will also propose possible countermeasures to address threats as part of a proposed new comprehensive information security framework to protect the security of healthcare data in mHealth systems.

References

1. World Health Organisation (2011) *mHealth: New horizons for health through mobile technologies.* [online] Available from: http://www.who.int/goe/publications/goe_mhealth _web.pdf [Accessed: 15 November 2016]
2. European Commission (2014) *GREEN PAPER on mobile Health ("mHealth").* [online] Available from: https://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth [Accessed: 15 November 2016]

3. Germanakos P., Mourlas C., & Samaras G. *"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. European Commission (2014) *Healthcare in your pocket: unlocking the potential of mHealth.* [online] Available from: http://europa.eu/rapid/press-release_IP-14-394_en.htm [Accessed: 15 November 2016]
5. Vithanwattana, N, Mapp, G. & George, C. (2016) "mHealth – Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions" *2016 12th International Conference on Intelligent Environments*, IEEE, London, 14-16 September 2016, p.258-261

Building Advanced Medical Platforms: Benefits and Possible Threats for Data Storage Management

Dr Glenford Mapp,
Associate Professor, Middlesex University
(g.mapp@mdx.ac.uk)

The need to store large volumes of data is powering the deployment of data storage infrastructures based on Cloud Systems. The emergence of Advanced Digital Medical Platforms (ADIMEPs) represents both a benefit and a serious challenge to these storage systems. This is because storage for ADIMEPs must be highly scalable and readily accessible by various parties; yet must also provide a totally secure system because of the sensitivity of patient data. In order to meet these challenges, it is important to realise that no single technique will work but a combination of security and storage mechanisms are required which must be skillfully combined; including the use of capabilities for objects, people and storage blocks; the development of secure Block servers to provide the basis of a scalable storage system and a block-chain system to track transactions in the system. A diagram of the ADIMEP system is shown in Figure 1.

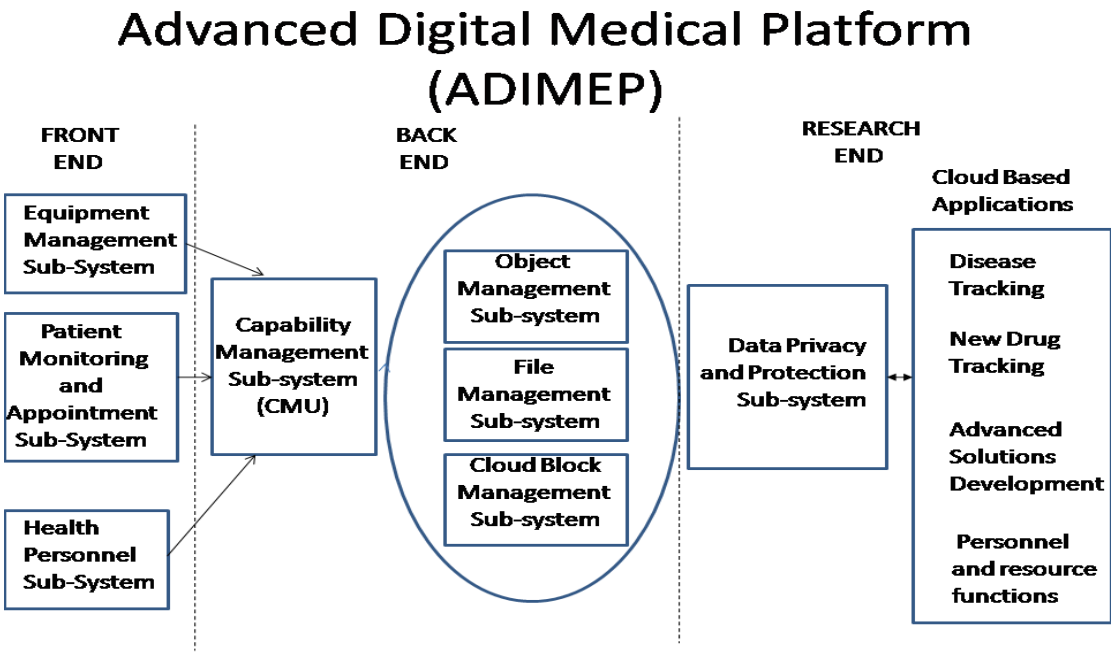

Figure 1: Functional Diagram of the ADIMEP system

This combination of these technologies along with secure communications will enable a very dynamic distributed environment to be built. The resulting synergies of this approach lead to a higher level of efficiency and good-put which can be migrated to other systems. This paper first examines the key characteristics of ADIMEPs highlighting the challenges for data storage in these systems. It then looks at solutions and mechanisms that can be used to address the concerns that are raised. The talk ends with looking at implementation issues and the standardisation of the proposed solutions.

Author Index

BOYER, Celia……28
FISK, Malcolm…… 07
GEORGE, Carlisle……11
GOODMAN, Kenneth…… 19
HARA, Sukhvinder……09
JONES, Emyr Wyn……30
JUSOB, Farad ……31
KALRA, Dipak……22
KOMNIOS, Ioannis……13
LÁSZLÓ, Mitzi……15
LUCIVERO, Federica……26
MAPP, Glenford……35
NAMORADO, Joana……06
THIMBLEBY, Harold……20
VITHANWATTANA, Nattaruedee……33
WAJID, Usman……24
WHITEHOUSE, Diane……17

List of Participants

- **BLACKMAN, Tim**, Middlesex University, London.
- **BOYER, Celia**, Health on the Net (HON) Foundation, Geneva.
- **COCKERTON, Tracey**, Middlesex University, London.
- **COMLEY, Richard**, Middlesex University, London.
- **CORY, Therese**, Beecham Research, London.
- **DUQUENOY, Penny**, Middlesex University, London.
- **FISK, Malcolm**, De Montfort University, Leicester.
- **GEORGE, Carlisle**, Middlesex University, London.
- **GOODMAN, Kenneth**, University of Miami, USA.
- **GOTTERBARN, Don**, East Tennessee State University, USA.
- **HARA, Sukhvinder**, Middlesex University, London.
- **HUBEJ, Tija**, Middlesex University, London.
- **JAJA, Gogo**, Royal Free NHS Trust, London.
- **JONES, Emyr Wyn**, NHS Digital, England.
- **JUSOB, Farad**, Middlesex University, London.
- **KALRA, Dipak**, University College London & The European Institute for Innovation for Health Data, Ghent, Belgium.
- **KIMPPA, Kai**, University of Turku, Turku, Finland.
- **KURT-DICKSON, Aygen**, London School of Economics, London.
- **KOMNIOS, Ioannis**, The KONFIDO Project, London.
- **LÁSZLÓ, Mitzi**, OWN, Amsterdam, Netherlands.
- **LEONCE, Jasmine**, East and North Hertfordshire, NHS Trust.
- **LUCIVERO, Federica**, University of Oxford, Oxford.
- **NAMORADO, Joana**, European Commission, Brussels, Belgium.
- **MAPP, Glenford**, Middlesex University, London.
- **MARZANO, Lisa**, Middlesex University, London.
- **PETRIDIS, Miltos** Middlesex University, London.
- **PLOTKA, Malgorzata**, De Montfort University, Leicester.
- **QAZI, Nadeem**, Middlesex University, London.
- **SHAH, Sarwar**, Guy's and St. Thomas' NHS Foundation Trust, London.
- **SINGH, Dinesh,** University of Delhi, Delhi.
- **SINGLETON, Peter**, Cambridge Health Informatics Limited, Cambridge.
- **TAYLOR, Richard**, International Baccalaureate, Cardiff.
- **THIMBLEBY, Harold**, Swansea University, Swansea.
- **VITHANWATTANA, Nattaruedee**, Middlesex University, London.
- **WAJID, Usman**, Information Catalyst, Manchester.
- **WHITEHOUSE, Diane**, The Castlegate Consultancy, Malton.
- **WOLFF, Tony**, Royal Free NHS Trust, London.
- **ZIELINSKI, Chris**, University of Winchester, Winchester.

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 2018 Health IT Workshop
on
Developments in ICT and Healthcare - Legal, Ethical & Social Aspects
8th & 9th March 2018
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/ehealthwks2018/

ISBN 978-164713306-1