digital enlightenment forum

EU 2016

Ministry of Health, Welfare and Sport

PHILIPS

Trusted Data Management in Health Care

Philips Centre, Amstelplein 2, Amsterdam, NL

7 June 2016

Conference Report

Contents

1. Introduction

Data management in healthcare has become a hot issue. More and more data is being collected of and by patients and stored for specific uses. Data on medical treatment is stored in databases by various medical organisations or professionals for use during the lifetime of the patient and even beyond to improve family medical care. Patients more and more play an active role in their own health monitoring and preventive care, and store their data at service providers. Life sciences research collects (normally anonymised) patient data for research towards improving people's health. The pharmaceutical industry collects data to develop its products. Governments stimulate the data collection to improve quality but also reduce costs of medical and social care for citizens.

All these developments are very welcome and needed, but they raise many questions and worries about the actual implementation. Who stores the data and controls their use and how does this relate to the individual patient's privacy and security? How secure is the storage and how transparent are the processes involved? Who can be held responsible if data is lost, data integrity is violated, or systems hacked? How can the data quality and accessibility be guaranteed over time, to the benefit of lifetime individual healthcare?

The Conference on Trusted Data Management in Healthcare was organised by the Digital Enlightenment Forum (DEF) in cooperation with the European Commission (DG CNECT) and with the Dutch Ministry of Health (VWS), and supported and hosted by Philips. Around one hundred people attended in Amsterdam.

The meeting brought together policy makers, technology experts and industry representatives in view of making concrete recommendations on how to meet specific challenges inherent in emerging policy, technology and application issues. They discussed the state of play, the main obstacles and proposed policies and technology solutions to ensure trust in a privacy-respecting data environment for patients, professionals and other actors in a transparent and auditable healthcare environment.

Presentations from the meeting are available from the Digital Enlightenment Forum website.[1]

2. Welcoming Addresses

Opening the conference, **Prof. George Metakides, President of the Digital Enlightenment Forum**, said it would help to start with a "bit of history". The legal basis for the protection of personal data in general was set by two US judges, Louis Brandeis and Samuel Warren, in a seminal article published in the *Harvard Law Review* in 1890. In their article, entitled simply "*The Right to Privacy"* Brandeis and Warren asserted that: "The protection of the private realm is the very foundation of freedom in the modern age". In this "private realm" health data has historically received special attention and protection, Prof. Metakides added.

Rewinding further, we find the principles of privacy embodied in the oath of Hippocrates of Kos, formulated in the late fifth century B.C. A key sentence in the Hippocratic Oath was that: "What I see or hear in the course of a treatment or even outside the treatment, I will keep to myself". Similar sentiments have been echoed in common law, medical codes of ethics and oaths many times over the years. For example, the constitution of the World Medical Association in Geneva in 1948 included a commitment that: "I will respect the secrets the patient has confided in me even after the patient's death." Hence, we see that health data has always held a privileged place within the "private realm".

This leads us to two fundamental ethical principles that are present in all codes of medical ethics. Firstly, there is the principle of human dignity, which needs no elaboration. Secondly, there is the principle of beneficence: that trust is required to enable those seeking medical care to communicate personal information to their care givers fully and accurately in order to receive appropriate treatment.

[1] See https://digitalenlightenment.org/event/trusted-data-management-health-care

Turning to the current situation, Prof. Metakides observed the growing diversity of health data creators, owners, managers, users and other ‘interested parties’. Hospitals, health science researchers, pharmaceutical companies, health insurers, governments (including smart cities), and increasingly individuals are all involved in generating and using health-related data. In addition, major internet companies – such as Google, Amazon, Facebook, Apple and Microsoft – are now showing serious interest in health data management. Thus, health data is increasingly widespread and new data analytic tools and algorithms are being developed to exploit them.

So how trusted is data management in healthcare today? It is a patchy record. Everyday there are instances of unauthorised access and breaches of security in hospitals and other facilities. Health data is also widely used by employers, insurance companies, political bodies and others with various motivations. Yet surveys show that people are largely ambivalent about the issue. They recognise the potential for beneficial advances from health data management (better quality, lower costs) but are also concerned about discriminatory use and express fear of unknown implications.

Having painted the health data landscape in these “broad brushstrokes”, Prof. Metakides concluded, the challenge for the conference was to address trusted data management in healthcare in a way that respects our ethical concerns and values.

Welcoming the audience on behalf of the hosts, **Walter van Kuijen, Senior Vice President Global Governance and Public Affairs, Philips** noted that trust is a prerequisite in healthcare in general and e-health in particular. Costs of healthcare are spiralling across the developed world, putting the sustainability of healthcare systems at risk. There is an urgent need for reform, moving towards value-based, outcome-based care. This will both benefit patients and offer more sustainable approaches for our societies.

One only has to look around to appreciate that healthcare has been slow to reap the benefits of the digital revolution. In some respects this caution is well deserved, as much is at stake. But technologies such as the Internet of Things (IoT) and big data offer many opportunities for health service providers and for individuals, as both patients and citizens. As users, we don’t yet expect – or are provided with – the same standards of service and convenience in healthcare as we are in banking, for example. We have to change this so as to deliver a more efficient, more effective, more sustainable healthcare system for everyone.

Philips was proud to be participating in E-Health Week which provided the opportunity to showcase its many achievements in the field and to contribute to the debate. Philips has introduced the privacy-by-design philosophy into all of its healthcare products and aims to embed privacy and data protection controls throughout the product and service lifecycle.

Finally, Mr van Kuijen turned to the role of stakeholders, which he saw as crucial to success. The EU and governments have a key role to play, for example in strengthening the Digital Single Market (DSM), incentivising performance and outcome-based approaches; and harmonising legal frameworks across borders. And all of the stakeholders – private sector, governments, end users – need to come together to create the partnerships and solutions necessary to secure the sustainability of our healthcare systems.

3. Trusted Healthcare in Europe

The Dutch Perspective

Edith Schippers, Minister of Health, Welfare and Sports of The Netherlands opted to be interviewed by Mr van Kuijen rather than to deliver a set speech. Their discussion covered a wide range of issues regarding health data management in the Netherlands and in Europe.

Mr van Kuijen began by asking the Minister what were her takeaways from the World Health Assembly, which she had recently attended in Geneva. Minister Schippers replied that cooperation is key in all areas. Societies around the world are looking to make their healthcare systems more sustainable and affordable. New technologies offer major opportunities, but we need standards – a common technical language – so that the various solutions are compatible. Pharmaceutical registries, for example, are seeking common approaches in the fight against antibiotic resistance. In Geneva, multi-stakeholder engagement was much more evident than was the case a few years ago. The WHO is looking for a new Director-General and the EU sees the ability to open the doors for stakeholders and to facilitate collaborations as key qualifications.

Asked about the situation in Europe, Ms Schippers said that national systems look more alike than they did 20-30 years ago. Member States face similar challenges – an ageing population, rapid advances in technology, rising costs of care – and need to seek common solutions. It was evident from her visits to healthcare institutions that many exciting innovations are available but that they are not being scaled. Good ideas are being held back by barriers such as lack of interoperability and the attitudes of professionals, civil servants and insurers. Ms Schippers urged companies to listen to users and ensure they developed their ideas with patients and the care professions fully alongside. If clinicians perceive that a solution will bring more bureaucracy then they will not be supportive; similarly, users want systems that are attractive and well designed. In Europe, there is still some reluctance towards cooperation on healthcare but we need to join forces at European level if we are to tackle the issues for the future.

The Netherlands is a good example of where we failed to fully engage all stakeholders regarding the introduction of electronic health records (EHRs). In the end we were unable to win the support of patients and medical professionals. The government didn't put forward a good enough business case. "Stakeholders are crucial and we forgot to take doctors and patients with us", Ms. Schippers observed. "A problem needs a problem owner; we should be all owners and part of the solution."

Turning to the potential contribution of DEF, the Minister echoed her and others' earlier points regarding the value of cooperation. The conference, as well as the many other events taking place during E-Health Week, was a valuable opportunity to network and bring people together. The Netherlands has also setup a network for startups and entrepreneurs to interface with healthcare providers.

Summing up the discussion, Mr van Kuijen encapsulated the Minister's message as: "Don't be afraid to disrupt and challenge, and create clarity around the pain points because that is the only way to advance."

The European Perspective

Paul Timmers, Director Digital Society, Trust and Security, European Commission spoke on Health Data Management: Viewpoint of the Regulator.

From the regulatory point of view, health data impacts on five domains: privacy, access, security, usage and storage. In terms of privacy and access, the EU's Data Protection Directive (now updated through the General Data Protection Regulation (GDPR)) safeguards the right to personal data protection and guarantees the free flow of personal data between Member States. These measures capture EU values and streamline international transfers while ensuring the rules are strongly enforced. A code of conduct on data privacy in m-Health apps is being introduced and further work is underway to identify other specific guidelines where necessary.

On cybersecurity, the Network and Information Security Directive represents significant progress in creating a more robust legal framework. Threats from ransomware, etc, are spreading and hospitals and other service providers will need to protect themselves by making their systems more resilient.

Storage and usage is being reinforced through exchanges on interoperability, such as the refined Health Interoperability Framework, and on standardisation of health data. The European Commission is preparing a new initiative on the 'free flow of data' under the DSM strategy. Important details remain to be worked out and are the subject of a Commission consultation: When is free flow of data appropriate? Who should have access and what should they be allowed to do? How to trade off public, private and users' interests? Striking the correct balance will be a key challenge and the approach may need to be different in healthcare than in other fields. New initiatives in understanding causes of health and disease through the European Science Cloud and improving high performance computing capability in relation to healthcare will also contribute.

Asked whether privacy and security measures promoted by politicians blocked innovation, Mr Timmers said we needed to be conscious of the EU's limited mandate in the health sector. Digital health sits at the intersection between the DSM and health which have different perspectives and levels of cooperation. Politicians may have only a short term in office and we need to ensure that decision-making on health reflects also Single Market and economic dimensions. We should also ensure existing laws are enforced as well as making new ones. Even if there is strong legislation, enforcement has to follow: healthcare providers have to comply with privacy laws, otherwise they are at risk of a fine which can be as high as 5% of their revenue. The GDPR is not prescriptive in every detail, so we need guidance and smart regulators.

4. Key Issues in Trusted Healthcare

In the first of a series of keynotes, **Ernst Hafen of IMSB, ETH Zürich** (Switzerland) described MIDATA.coop, an initiative to put citizens in control of their own health data.

Starting with an analogy from the world of personal finance, Mr Hafen noted that today we all have bank accounts and are used to the fact that we are able to invest our funds in different ways. Of course, this has not always been the case. Bank accounts have only become commonplace in the last half century and in the Middle Ages the populace had few financial assets of any kind. We are in a similar situation now with health data: we have the power to combine and use our own data the way we want, including by 'investing' it with providers offering dedicated services.

In most European countries health data is still kept in silos. The exceptions are Denmark and Estonia where national regulations allow service providers and regulators to exchange data more freely. In the future we need to put the individual (as a citizen rather than as a patient) at the centre by creating a framework that allows people to combine and trade their health data in the same way that banks do for financial assets. When it comes to genome data, we are all billionaires, Mr Hafen explained, wherever we live. We need to be able to share the benefits and avoid a winner takes all situation.

In healthcare, big data offers the opportunity to integrate diverse data sets from millions of people. Geographical information systems allow data to be analysed at a spatial level, while human information systems allow data to be analysed at a personal level. There is significant potential to generate new value from copies of data sets that are not available to health care organisations at the moment. The active participation of citizens with the data that is collected in social networks and other clouds is essential. We must avoid a situation – already seen in other areas – where digital oligarchs harvest and monopolise health data for their own ends without control of individuals. Citizens recognise that, despite data protection laws, they have little influence over what personal data is collected and by whom or how their data is used. Consequently, transparency and optimal use of the totality of available data is missing and people's trust in data companies is dwindling.

Experience shows that people want to contribute: one only has to look at Wikipedia – which took 100 million hours to create – to see the power of collective efforts. In surveys 60% of people said they would be willing to share the results of a genome analysis in order to find out about diseases and medical traits.

Citizens need to be empowered to take control of their own data. Every individual should have a constitutional right to a digital copy of all their personal data – medical and non-medical. They should be able to deposit this data in a safe and secure 'bank account' in which they are able to store, manage and actively share their data on transparent terms. These personal data banks should be not-for-profit cooperative organisational structures owned by the citizens. Revenues from citizen-controlled secondary use of data would be invested in projects and services that benefit members and society at large.

MIDATA.coop is building such a citizen-centred data storage system. It is owned by citizens as a cooperative; is not-for-profit, built on open source code; has transparent governance; and operates to the highest security standards (based on data encryption). It is foreseen as a federation of national personal data cooperatives providing a common IT structure and data exchange platform, similar to the way SWIFT operates for financial exchanges.

The project is progressing well. The platform prototype is now completed and three independent security audits have been performed. The MIDATA.coop organisation has been founded and a legal and ethical framework for MIDATA.coop cooperatives is under development. Financial support is being provided nationally (ETH and BFH) and there is strong international interest as well. The first pilot projects started in Switzerland in May 2016 and will follow the 'flipped trial' concept, where patients recruit their doctors to the trial.

Michiel Sprenger, Senior Advisor, Nictiz[2] and Mentor Clinical Informatics, Eindhoven Technical University (the Netherlands) focused on the potential for content standardisation in improving the quality of care.

There are three challenges in healthcare in which eHealth is crucial. Firstly, advances in technology as well as changing social attitudes mean that patients are no longer to be passive recipients of care. They want to be the manager of their own health, be informed, and be in control. This requires solutions for patients and interoperability between the systems used by patients and health professionals on various levels.

The second challenge is continuity of care. We have to make sure that organisational barriers in care delivery do not block continuity of care. This requires integration of health and social care, as well as interoperability to be assured on various scales (regional, countrywide, etc.).

The third challenge is to close the quality loop. We have to think of healthcare as a learning system where we measure outcomes and quality, provide feedback into the care practise, and measure the health of the general population. This requires high quality and consistent documentation in the clinical process, together with content standardisation for semantic consistency.

The Netherlands is a medium-sized country (population 17 million). Healthcare is executed by private enterprises and is financed partly by the state with increasing market mechanisms. Delivery is fragmented across numerous institutions. There is no regional political structure in healthcare, although institutions cooperate in a pragmatic way. Consequently, much of the steering is 'bottom-up' and relies on consensus models. Although quality is recognised to be very good (e.g. rated No.1 in the European Health Consumer Index for many years), the system is expensive, with expenditure among the highest in Europe as a percentage of GDP. Interoperability is also a severe problem.

[2] National Competence Centre eHealth in the Netherlands

All three of the challenges identified above can be addressed through content standardisation. We need to pay more attention to what we collect and how the data is structured, rather than just the compatibility between systems. Mixed structuring will lead to ever greater chaos.

In the long term, the ideal would be to have as much data as possible as close to the patient as possible. Data should be registered once, unambiguously, in (or close to) the primary treatment process. It should then be selected, aggregated and processed in a variety of ways for multiple uses, from patient care and patient transfer, to research, management information, quality assessment, finance/reimbursement, etc. The information would be based on clinical building blocks (CBBs), the definitions of which should be driven by professionals and be used case neutral (i.e. usable in any context). The CBBs are the connection between the professional world (clinical concepts) and the technology world (unambiguously implementable definitions), and are the basis for higher level information content and applications (patient summary, quality summary, ePrescription, discharge letter, etc).

The Netherlands is experimenting with such an approach as a means of standardising what is in systems rather than just standardising between systems. The project, led by Nictiz and involving university medical centres and general hospitals, has developed 88 CBBs describing healthcare processes. The system is being trialled at institutions across the country and is planned to be applicable for all sectors of care. Even so, more regulation and greater consensus on how to standardise content is needed at European level.

Jacob Hofdijk, Founding Partner of Casemix, CQT Health and Care Group (the Netherlands) spoke on the key principles for the design and delivery of person-centred, integrated care systems.

At present the patient is lost in silos between primary, secondary and after care. We have to think in terms of a paradigm shift from supply to demand. The focus should be on the patient's health or health problem. The concept of person-centred health records according to SOAP[3] principles was introduced in 1965 and is still valid.

Taking one example, a national care standard for diabetes was introduced in the Netherlands in 2003, focused on prevention and avoiding complications. It aims to deliver appropriate care for the individual patient within the health network. It has the active involvement of the patient, who is encouraged to self-manage his/her condition, and is based on guidelines and protocols.

The Blue Line approach links the patient with the care group and other providers through an individual care plan. Such a person-centred approach has five pillars: technological interoperability; semantic interoperability; social interoperability; society incentive framework; and balancing health and life goals.

This approach is now being applied in perinatal care. The project, called Geboortehart, has developed a dictionary to facilitate the semantic exchanges between care providers, together with an appropriate IT infrastructure (IHE – XDS). Proof of concept is being shown at facilities in Zorgring (West Friesland and Amsterdam). The system will cover the full care path for the woman and her baby, from confirmation of pregnancy through to post-natal care. The outcome will be a good start for mother and child, each continuing their journey with their own personal health record (PHR).

5. Trusted Healthcare in Action

The first session of the afternoon comprised a series of presentations on best practice projects for trusted data management within the healthcare field.

Jos Dumortier of Time.Lex (Belgium) described AEGLE, a reference big data architecture for the healthcare sector.

[3] Subjective, Objective, Evaluation, Planning

AEGLE is a Horizon 2020 Innovation Action, that started in March 2015, with partners from eight European countries. It addresses a variety of technical, business and user challenges relating to big-data applications in healthcare. In particular, the project aims to understand how to exploit, manage and analyse big *bioclinical* data across a diverse range of real-life healthcare scenarios. Data will be collected from three use cases covering distinctive elements of the health spectrum: an intensive care unit; treatment of chronic lymphocytic leukemia (CLL); and type 2 diabetes (T2DM).

A first release of the AEGLE system architecture has been issued based on a user-centred design approach. The first validation phase is now underway to illustrate proof-of-concept and engage users. Initial steps in relation to the business landscape for big bioclinical data and assessment of legal and ethical issues have also begun. In the short term, all AEGLE's activities across all areas of the data value chain will need to comply with the requirements of the 1995 Data Protection Directive. Since every Member State has specific procedures for this, compliance is time consuming and complex. In the longer term, the legal framework will be set by the GDPR, allowing a more stable environment for AEGLE and for other European big data initiatives in the health sector.

In response to a question, Mr Dumortier confirmed that the project informed patients involved in the trial that their data would be used for clinical and research purposes.

Xander Heemskerk, Director Product Security, Philips (The Netherlands) described his company's strategy for building trustworthy healthcare applications based on an holistic approach to address security in products and services.

Reiterating trends identified by other speakers, Mr Heemskerk noted that healthcare is experiencing foundational changes. Consumers are increasingly engaged in their health. The shift to value-based healthcare will reduce waste, increase access and improve outcomes. Care is shifting to lower cost settings and to the home, calling for new tools for caregivers and patients. Underlying all this, connectivity and digital are shifting value from devices to software and services.

Connectivity in healthcare has increased rapidly over the past few years. In today's hyper-connected era, doctors use tablets to examine patient information, offsite physicians are able to undertake remote diagnoses and more and more equipment is becoming connected. Under its open data management approach, known as Connected Care, Philips has achieved many industry "firsts". These include HeartStart MRx, a monitor/defibrillator capable of connecting via LAN or wifi with the hospital's patient monitoring network, streaming real-time data to a nursing station for remote alarming and surveillance.

For its next generation solutions, Philips unites medical devices, apps and data in the cloud. Its HeartSuite IoT architecture, based on Amazon AWS, combines data sources, connected devices and sensor data to help put the patient/customer in control. With more and more medical devices being put online, security is a major concern. Press reports have shown thousands of critical medical systems – including Magnetic Resonance Imaging machines and nuclear medicine devices – to be vulnerable to attack.[4]

Product security risk assessments, security and privacy by design, as well as vulnerability and penetration testing are at the heart of Philip's holistic approach throughout the lifecycle of the product and service. The responsible disclosure policy and processes provides a feedback loop from external Security Investigators has shown its purpose in the past.

At a corporate level, Philips has established the Data Governance Review Board as a review and decision-making body for data analytics initiatives. The Board reviews, approves and provides guidance on data analytics (and storage) initiatives ("Data Initiatives"). It is the authorised body tasked with ensuring responsible data stewardship and effective management of ethical and legal risk for Data Initiatives. The company has also adopted the Philips Data Analytics Code of Conduct to promote good practice and deter wrongdoing. This vigilance extends across the supply chain, where the

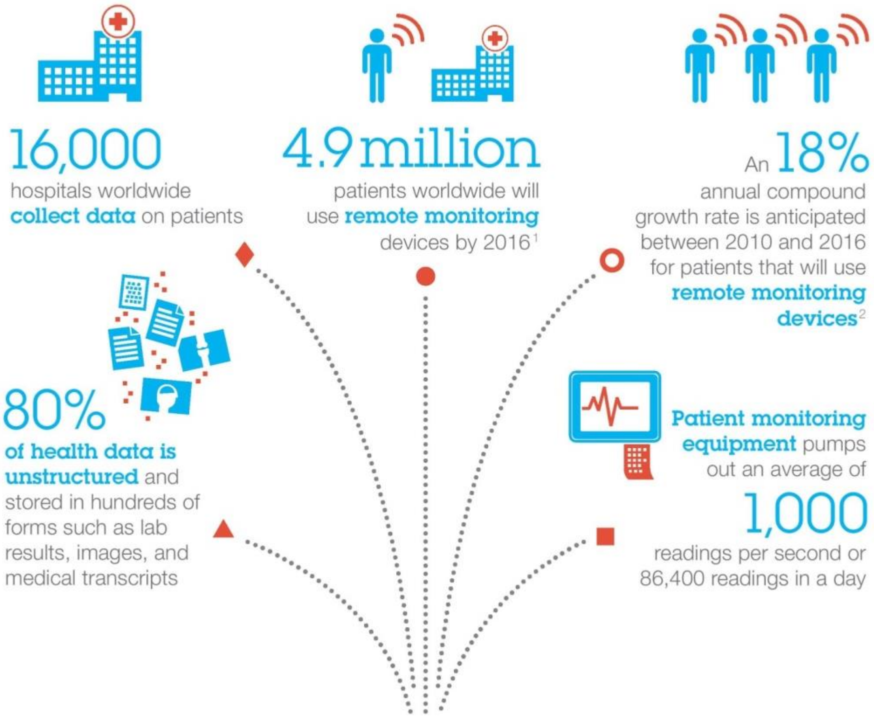
[4] 'Thousands of 'directly hackable' hospital devices exposed online', The Register, 29 Sep 2015, www.theregister.co.uk/

company undertakes due diligence and ensures appropriate governance and liability arrangements are in place.

Wessel Kraaij of TNO and Leiden University (The Netherlands) described a series of projects relating to privacy within the emerging ecosystem for distributed health data.[5]

Big Data has major implications for healthcare, trends that have been captured in an infographic produced by IBM. From a medical perspective, big data facilitates a shift from treatments based on population averages towards personalised treatment based on an individual's own unique characteristics and requirements. This does not mean that we can forget about reference populations. On the contrary: personalised treatments based on interpretation of peer data help improve the reliability of reference data populations – the two are mutually reinforcing.

Currently, privacy and security are given low priority in the development of health apps. A recent UK survey[6] found that 66% of 79 health apps tested – all of which were accredited to the UK NHS accreditation scheme – did not use data encryption. Ninety percent of apps transmitted data to the cloud and 20% of apps did not have a privacy policy. Of those with a privacy policy, 78% did not adequately describe the nature of personal information that was transmitted. Thus, there is a serious risk for unforeseen and unwanted dissemination of data to third party services without clear notification to and consent by the end-user.


16,000
hospitals worldwide collect data on patients
4.9 million
patients worldwide will use remote monitoring devices by 2016[1]
An 18%
annual compound growth rate is anticipated between 2010 and 2016 for patients that will use remote monitoring devices[2]
80%
of health data is unstructured and stored in hundreds of forms such as lab results, images, and medical transcripts
Patient monitoring equipment pumps out an average of
1,000
readings per second or 86,400 readings in a day

Big Data in Healthcare (IBM)[7]

At a time when the development of precision medicine and personalised healthcare is facing serious technical and legal barriers, innovations in data management and governance are needed. So-called FAIR principles is one such approach. This aims to increase the impact of public research by ensuring that data are Findable, Accessible, Interoperable and Reusable.

An alternative approach goes under the acronym RESPECT4U. This advocates a framework based on the following seven principles:

[5] Marc van Lieshout (TNO) had also contributed to the presentation.

[6] BMC, October 2015

[7] www-03.ibm.com/press/us/en/photo/40728.wss

- Responsible: a responsible approach towards handling person related data.
- Empowering: the data subject has full control who can view their data and has instruments to embody their control (e.g. opt in / opt out).
- Secure: safe, accurate, up to data, reliable.
- Pro-active: privacy by design, privacy impact analysis (data processing organisation).
- Ethical: taking into account ethical issues such as fair treatment, non-discrimination, inclusivity.
- Controlled: data processing organisation are under government supervision and can be subjected to claims.
- Transparent: the data controller gives a transparent view on which type of data is collected, how the data is processed, the logic of decision making and the management of data flows.

A series of projects are underway providing experimentation with real patients within healthcare settings and with real patient data. PIME (Personal Information Management Ecosystems) is a European project, funded by EIT Digital, with a focus on patient self-management. PRANA (Privacy Respecting ANAlysis of health data) is a Dutch initiative involving universities and healthcare providers across the Netherlands. Both projects will help address how to perform privacy-respecting analysis on sensitive patient data that is distributed and should not be disclosed to the parties that perform the analysis. Various approaches are being followed, such as: data protection and processing by design; informed consent based on transparency; and privacy respecting analysis of distributed data repositories.

Mike Yeh, Assistant General Counsel, Worldwide Public Sector for Microsoft, looked at developments in relation to healthcare and the cloud, focusing on the regulatory environment.

In the US, as elsewhere, healthcare providers are increasingly moving their data to the cloud. Yet many of these applications are being deployed as "Shadow IT" without appropriate security safeguards. A recent investigation by security firm Compaas trawled Google Docs and Dropbox and found thousands of sensitive documents belonging to hospitals, schools, and corporations. "We found a couple of hospitals that had breaches in HIPAA compliance," according to Compaas COO Doron David. "There was patient information, what types of surgeries they had, social security numbers."

The regulatory environment has been slow to adapt. Often only very minor changes are needed. In Belgium, for example, the law has been changed to specify that "each patient must have a patient record kept *by* the hospital" rather than "*in* the hospital". In Germany, some healthcare customers believe that Section 203 of the German Criminal Code, which stipulates that any infringement of personal privacy by the healthcare or associated professions is liable to a fine or imprisonment of up to one year, prohibits the use of cloud services. Multiple layers of regulation often apply. In Germany, for example, data protection is subject to Federal law, as well as State/Regional law, religious exemptions (in church-affiliated hospitals) and other rules in areas such as cybersecurity, medical devices and social security codes.

Although the healthcare system in the United States has its flaws, the Health Insurance Portability and Accountability Act (HIPAA), which sets the standard for protecting sensitive patient data, has enabled healthcare providers to embrace the latest cloud-based solutions. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. Even in 1996, when the law was passed, lawmakers recognised that patient health information would be digital in the near future. The United States also benefits from the lack of legacy and general data protection regulations. Before HIPAA, there was no federal law in the US regulating the privacy or security of health information. The Act assumes consent for uses and disclosures of protected health information for treatment, payment, and healthcare operations. It is backed up by strict enforcement: 8,000 cases were investigated in the first five years and multi-million dollar fines have been issued. In recent years the Act has been extended to cover cloud services. In 2012, for example, Phoenix Cardiac Surgery settled a HIPAA claim based on the improper use of cloud services and was fined US$100k.

Looking forward, Mr Yeh offered a roadmap for healthcare providers for enabling the cloud based on the following five steps:

1) Commit to going digital and testing cloud-driven solutions to improve healthcare outcomes.
2) Develop a data classification system that realistically assesses the costs and benefits of moving certain workloads to the cloud.
3) Define cloud security requirements based on international standards where possible.
4) Include a consent mechanism that strikes the right balance between improved healthcare outcomes and patient privacy.
5) Enforce the law so that patients and providers have confidence in the system and approved cloud providers.

The key to success is in understanding your data. For example, it's unlikely that healthcare data is critical to national security and thus, the same level of protection and security should not be required. Much of it – possibly up to 90% – is routine business or official information that could be stored and processed using commercially available services with industry standard security controls.

Healthcare providers should look to regulators to create a framework for enabling and accrediting cloud-based services. Key questions for healthcare providers to ask of cloud service providers include: What are you doing to protect my data? Who has access to my data? How is my data being used? How can I verify what you're doing?

Dimitris Potoglou of the School of Geography and Planning at Cardiff University (UK) presented results from a pan-European study on the privacy of health records. The study was undertaken by PACT, a three-year research project funded under FP7 that finished in 2014.[8] It looked at health data records and data mining for personal and public healthcare as one of three use cases for privacy data protection in Europe. Over 26,000 interviews were undertaken in 27 EU countries among the general population aged over 18, using a mixture of face-to-face and online data collection.

Overall, respondents recognised the benefits of storing electronic health information, with strong support for their use in relation to improving treatment quality (75.5%), preventing health epidemics (63.9%), and reducing treatment delays (58.9%). However, between 48.9% and 60.6% of respondents also expressed concerns about different levels of access to this data, and only 38.4% agreed that healthcare providers are currently successful in providing effective data security.

Other key findings were:

- Strong variations observed in the levels of health privacy concern across Europe. The highest proportion of respondents answering "Very concerned" was observed in Lithuania, while the least concerned about privacy were observed in Sweden, Slovenia, and Denmark.
- In most EU countries respondents generally preferred a device to store increasingly expansive healthcare data rather than just basic health status, but only up to a point. Devices that store a full lifelong medical history were viewed negatively.
- Younger people were more supportive of a wider range of data being stored than older people.
- Respondents were against professionals other than doctors, nurses and paramedics having access to their data. In particular, they were averse to immediate family, health insurance and pharmaceutical companies, and academic researchers having access to this information.
- In terms of access beyond the country of residence, respondents expressed strong support for access from within the EU but were less supportive of access from the rest of the world.
- Everything else being equal, respondents were willing to pay for privacy protections but not for sharing of data.

The study provides insight across several areas in this ongoing debate; particularly around the sharing of electronic health records for research. Overall, people across the EU27 feel that the benefits of new technology outweigh risks to privacy. However, people are suspicious of data being shared

[8] Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action. www.projectpact.eu

beyond healthcare professionals, such as with private companies, researchers and even with the emergency services. The findings provide some support for the current system of separation and anonymity in the storage of sensitive medical records.

6. The Future of Data in Healthcare

Chair: Jan Adriaenssens, iMinds(BE)

Panel members: Ernst Hafen (IMSB, ETH Zürich, CH); Steven Posnack (ONC, Dept of Health and Human Services, US); Steven Seyffert (Capgemini Consulting); Luk Vervenne (Synergetics, BE)

Introducing the session, Mr Adriaenssens said the event stood at a crossroads between technology, public policy and ethics, all applied to the complex area of healthcare. Healthcare data takes many forms but in the end it is our data.

The conference had heard a lot about citizen empowerment and putting users at the centre: but what does this mean in practice? In a recent study by iMinds on medical wearables, 75% of people said they would wear such a device if advised to do so by a medical professional. But only 0.5% of respondents had worn one. The reason: because professionals are not sufficiently comfortable or familiar with wearable devices to prescribe them. There seems to be a lack of trust. To quote a Dutch saying: “Between the dream and the act are practical issues”.

Europe versus the United States

To initiate the debate Steven Posnack gave an overview of experiences in the US. Since 2009 the US has had enabling legislation under HIPAA – based on the concept of ‘meaningful use’ – promoting the use of heath data and EHRs. The challenge now is to improve the user experience and to address emerging security concerns. We have to recognise that health is now part of the critical information infrastructure and must be protected from threats that emerge from an electronic perspective, such as medical identity theft and ransomware. The trend now is towards bidirectional information flows, directly involving patients/citizens in generating data that can be monitored or used to create health alerts. In healthcare, as elsewhere, provenance matters and patient-generated data has very high value. The ability to segment data once collected is also important.

Expanding on experience with HIPAA in response to questions, Mr Posnack explained that the Act sets a Federal floor regarding the use of health records; states are able to set higher standards if they wish. The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed in 2009, supports the enforcement of HIPAA requirements by raising the penalties of health organisations that violate HIPAA Privacy and Security Rules. It was part of the post-crash stimulus package and has helped drive adoption of EHRs. Business drivers have also been strong. In the US health records are classified as business data, not personal data. This means there is a motivation for corporations to generate and retain the data, but few incentives to exchange.

To counter this, the Blue Button initiative[9] has been introduced to enable access to health records. It allows every citizen to obtain copies of their data. Education is a big challenge, however, and at present HIPAA rights are much underutilised. People are not sufficiently activated to access their data.

Mr Hafen said Europe was quite envious of what the US has achieved by enforcing EHRs. At the same time, there is the opportunity to learn from this and leapfrog over the US. One of the issues that has arisen is where to put the data. Data repositories are needed, like that advocated in MIDATA. Mr Posnack agreed there was a need for standards. The Department of Health & Human Services runs

[9] See www.healthit.gov/patients-families/your-health-data

certification programmes to regulate health IT standards. Experience shows it is best to seek industry agreement before moving to regulation and to pilot standards before they are rolled out nationwide.

Mr Hafen drew attention to the stark differences in the startup culture between the US and Europe. In the US one fund alone had invested around US$4bn in e-health start-ups only, whereas in Europe no individual fund has that level of investment capability in any sector. Europe has to think more seriously about how it supports startups. Ensuring interoperability of health apps would be a good starting point. Mr Posnack explained that in the US private investment was complemented by incubators that help entrepreneurs to partner with the innovation arms of healthcare clinics and hospitals. Together they are engines for funding startups.

Asked about the role of the general practitioner in the US scenario, Mr Posnack explained that they participated in health information exchanges, intermediaries who help facilitate access to data including under the Blue Button initiative. There has been a good rate of adoption of EHRs amongst family doctors and most would not go back to paper records. However, some doctors have complained that the extra time spent on screen depersonalises the relationship with the patient. EHRs also impose a greater responsibility on professionals to document everything they do, which some see as a burden. Health authorities and others have the capacity to collect data for many new purposes and are keen to use these powers; hence EHRs also change the workflow.

Responding to a question about how to incentivise people to use the platforms, Mr Posnack agreed that access to health data alone was not a big driver. People liked the convenience of online scheduling for appointments, etc, as did healthcare providers as it improved efficiency. Providers are looking at ways they can derive better value, for example by comparing their performance to others within their locality or their specialty. Some of these schemes are coming to maturity.

Prospects for Europe

The second part of the Panel discussion looked at the wider prospects for trusted health data in Europe.

Mr Hafen saw the ability for citizens to receive immediate feedback on their personal circumstances as one of the main drivers. In today's consumer society, where everyone is used to convenient, round the clock access to services, the prospect of rapid response is very attractive. Not every individual or organisation will be ready to adopt these features; it will be a matter of learning by doing. Once momentum is obtained the paradigm shift will come very quickly, especially if the systems are fun and easy to use (possibly even utilising gaming).

Mr Vervenne saw personal data management middleware as being very important. We need to help healthcare communities engage with their patients and the wider community, to overcome the 0.5% statistic quoted by iMinds. The healthcare sector has to leave its ivory tower and engage with users, bringing in the social care sector as well.

Mr Seyffert saw trust as a central issue. Whatever approach we choose must advocate trust because trust leads to adoption. Citizens must be able to assess both risk and value. Trust will be a major factor in the adoption of next generation systems, with implications for aspects such as data storage. Existing healthcare systems are breached because security is treated as an add-on: building in security from the beginning will offer much better possibilities. The PACT study shows that solutions will be country – and even region – specific, which means we also need to place a high priority on interoperability, including promotion at international level. Mr Hafen agreed and added that interoperability would not come from the technical level alone, it also has to involve the market and the users.

A Japanese delegate asked about the impact on the doctor-patient relationship. Japan has a similar discourse to Europe on EHRs and privacy and will introduce an e-health card for all citizens in 2018. Technology narrows the gap between professionals and patients and there is concern over how to preserve the egalitarian tradition in healthcare. Mr Seyffert commented that doctors had been reluctant to accept the principle of quality assessment and comparative rankings. The medical community has to open up, become part of the ecosystem and play a more active role in transferring new knowledge to patients.

In a major survey in the Netherlands, with 11k responses, one of the main benefits people saw from personal health records was that they could be assured that all professionals had access to the same data. As with banks, there will be a market for many different types of platforms, including ones for rare diseases with little or no healthcare community behind them at present. There is good motivation for users to get involved.

Turning the discussion to health promotion, one delegate asked how access to health data could be used to incentivise people to work on their lifestyle and promote healthy living? Mr Hafen agreed that the sharing of data and use of the tools is one of the big challenges of the next ten years. Not only is health promotion neglected (typically accounting for under 10% of healthcare budgets), very little is known about how healthy people stay healthy (for example, the 80 year old smoker with no lung cancer). Studying these cohorts could add substantially to the reference population. Mr Adriaenssens observed that insurers are looking to use IoT for prevention, so as to reduce their exposure. Mr Vervenne thought that this brought us back to the nub of the problem: everyone wants our data and privacy protections should be in place before we allow access for the purposes of prevention.

7. Conclusions

The Conference explored a wide range of issues relating to the exploitation of and future prospects for trusted data management in healthcare and stimulated much debate, both within the formal sessions and during the networking breaks.

The Conference’s key messages were the following:

1) **Europe is facing foundational changes in healthcare**. Costs of healthcare are spiralling across the developed world, putting the sustainability of healthcare systems at risk. Consumers are increasingly engaged in their health, while care is shifting to lower cost settings and to the home, calling for new tools for caregivers and patients. There is an urgent need for reform towards more value-based, outcome-based care that delivers better results for patients and for society. At the same time, the shift to online systems brings new challenges in terms of security, privacy and trust.
2) **Europeans are generally supportive of electronic health records (EHRs)**, seeing the benefits of the new technology as outweighing the risks to privacy. However, people are suspicious of data being shared beyond healthcare professionals, especially with private companies. And on some issues attitudes vary markedly between countries and between different age groups.
3) **Personal health data promises a revolution in healthcare.** Widespread access to personal health data will change our approach to healthcare, creating many new opportunities from personalised medical treatment through to promoting healthy lifestyles. It is vital that the personal data underlying this health revolution is accessible to and under the control of citizens. On the one hand, we need to ensure that individuals, as both patients and citizens, have access to their data with the same convenience and usability as in other areas of society, such as banking. At the same time, people should recognise that their health data is an asset with a market value, which they have the right to protect and share as they wish. New, trusted solutions and platforms will be required to facilitate this.
4) **Innovation in Europe is being held back by fragmentation and lack of standards**. In most European countries health data is still kept in silos, primarily due to national regulations that prevent the free flow of data. Innovation is being held back by lack of interoperability, as well as by a lack of awareness among health professionals and others. In addition, the investment environment in Europe is not conducive to startups and entrepreneurs.

5) Although the health economy and regulatory environments are very different to Europe, **the United States offers valuable experience in relation to health data management**. The Blue Button initiative enabling access to personal health records, the key role of enforcement, and the record of support for health app startups are all aspects from which Europe can learn.

New approaches are needed for Europe to fully grasp the opportunities of trusted data management in healthcare. An ecosystem for personal health data is emerging: we must ensure that this ecosystem respects European values and is under the control of citizens rather than of large corporations. Empowering citizens to take control of their own data means they must be able to assess both risk and value. Prescriptions suggested by the discussion include the following:

- **Network startups and entrepreneurs with healthcare providers and citizens**, so as to spur innovation and build confidence in personal health data solutions.
- Build **not-for-profit data banks/repositories for personal health data**, along the lines proposed in the MIDATA project.
- Focus on **content standardisation** so as to develop systems that are context-neutral and capable of being deployed across a wide range of applications.
- Promote further **research into privacy-respecting technologies and approaches** based on principles such as FAIR and RESPECT4U.
- Encourage **an holistic approach to trust management within organisations**. The Philips example shows how this should span from privacy-by-design, through product/service verification and assessment, to independent internal review, and due diligence across the supply chain.
- Develop initiatives to **facilitate multi-stakeholder cooperation**, including:
  - **Raise awareness of and support for** personal medical devices among healthcare professionals;
  - **Involve users** (healthcare professionals, citizens and others) in all aspects of system design, development and governance.
- **Empower citizens through regulation**, including the legal right to a digital copy of all personal data.
- Adopt **smart regulation in relation to trusted health data**, for example by removing barriers to innovation in areas such as personal medical devices and free flow of data.