

# **Health Data: Saving Lives and Protecting Patients' Rights**

*A contribution to the dialogue on how to improve health in Europe while preserving privacy*

- **Regulators and policy makers should be sensitive to differences between “primary” and “secondary” uses of health data.**
- **“Cloud-first” policies should be promoted to improve delivery of care across Europe.**
- **All stakeholders should engage in dialogue and awareness raising that drive a better understanding of the value, safeguards and ethics of “secondary use” of data.**
- **Member States should ensure that their GDPR implementation enables privacy and security and improves health outcomes.**
- **Stakeholders should support research on a new ethical framework for health data and “data donation”.**

**Putting these recommendations into practice will ensure that Europe’s new privacy framework best serves Europe’s citizens – starting with its patients.**

*May 2017*

## *Executive Summary*

**The shared priority of health professionals, health authorities, citizens and other stakeholders must be to ensure that patients have access to high-quality, preventive and affordable care.** Patients must be treated with dignity and respect, and this includes providing robust protections for their data. **However, privacy interests should not override patients' core interest in receiving quality care.**

Cloud computing is an important part of optimising care and protecting patients' health information. The cloud can deliver the optimal combination of scale, flexibility and choice needed to truly maximise the benefit to patient care while minimising implementation effort and cost and promoting security and privacy.

**Despite raising awareness that better access to data may help save lives, however, legacy health IT systems continue to proliferate. These systems are often incapable of delivering data to the right place or at the right time, affecting quality, efficiency and safety of patient care.** They also limit patients' access to and control over their data as well as access to health data across different care and cure providers.

**Modern, cloud-driven computing technologies and a modern vision of "data for public good" can help to address these challenges.** Today's cloud solutions leverage the power of data analytics and major economies of scale to offer healthcare providers more flexible computing power for lower cost than is possible with traditional, on-premises IT systems. And the cloud's "always-on", mobile-ready accessibility ensures data is always available to those that need it and in a private and secure way.

**Increasingly, the key question for health leaders is not whether to use cloud computing, but rather "why not?"** – and how quickly the cloud can be deployed and what data can be moved to it, and which technology solutions can help further protect health data for greater good. We are therefore starting to see the emergence of "cloud-first" procurement paradigms across Europe, with positive impact on health outcomes and health experiences.

In some instances, however, healthcare providers and researcher organisations find their **cloud-first policies bumping up against outdated legal restrictions, preventing them from unlocking the full benefits for patient care and public health.** There are isolated cases, for example, of laws that still deem outsourcing of data processing to breach patient confidentiality – even where the provider is a trusted data guardian, legally prevented from doing anything with data unless instructed to do so by the patient or the healthcare institution. Addressing these barriers is an imperative for all stakeholders.

**Regulators and healthcare providers should follow a "patient-centric" approach that puts the total needs of the patient first.** In doing so, they should also recognise that different rules and protections may be appropriate for **"primary" uses of patient data** (e.g., to improve an individual patient's care and outcomes) **and a spectrum of "secondary" uses** (e.g., using large sets of (sometimes anonymised) patient data to advance research, drive innovation, and ultimately, to improve human health and the systems that treat us).

**To the extent cloud computing can improve care in “primary” use scenarios, policymakers should eliminate regulatory blockers, and endorse cloud-first policies that encourage cloud use.**

Recent public debates suggest that a more deliberate and thoughtful approach may be warranted in relation to secondary uses of patient data. The vital importance of disease registries, “Million Genome” and clinical study data is testament to the fact that data saves lives. Most public health and biomedical research experts therefore support secondary uses of data, but also accept that such uses are not universally understood, or agreed to, by patients.

Ultimately, **harmonisation on what is appropriate in terms of secondary use of data is desirable for many reasons, not least efficiencies of scale, and the furthering of cross-border care and the “digital single market” for health.** But different populations may have different attitudes to what secondary use should be authorised, and how. Greater public engagement around secondary uses of patient data is needed, including around its value, risks and safeguards, and the appropriate degree of patient control. This paper proposes a possible **framework on “data maturity”** for consideration, to help structure these patient and stakeholder discussions.

Of course, restrictions on the processing of health information can hinder the secondary use of health data regardless of the infrastructure used to process that data – self-hosted, government-provided or cloud-based. But here, as in primary use, the cloud enables a step-change in what society can achieve. **The opportunity has never been greater, and therefore so is the need to find a workable and patient-centric approach.**

There is no question that all entities handling patient data must store and process such data in ways that promote trust and advance the interests of patients – particularly with the deadline for implementation of Europe’s new data protection regime, the General Data Protection Regulation, looming.

This paper aims to contribute to a discussion around how to achieve those objectives while at the same time driving optimal healthcare outcomes. **We propose the following recommendations** for action, and we welcome the opportunity to engage in a vibrant conversation with health and data privacy authorities, patient organisations and health professionals on these proposals:

- **Regulators and policy makers should be sensitive to differences between “primary” and “secondary” uses of health data.**
- **“Cloud-first” policies should be promoted to improve delivery of care across Europe.**
- **All stakeholders should engage in dialogue and awareness raising that drive a better understanding of the value, safeguards and ethics of “secondary use” of data.**
- **Member States should ensure that their GDPR implementation enables privacy and security and improves health outcomes.**
- **Stakeholders should support research on a new ethical framework for health data and “data donation”.**

**Putting those recommendations into practice will ensure that Europe's new privacy framework best serves Europe's citizens – starting with its patients.**

---

## **Cloud-first policies empower better patient care and public health outcomes.**

Health innovation, empowered by cloud computing holds enormous potential to improve human health. By enabling the smart, efficient, and safe use of patient data, cloud computing is transforming many aspects of contemporary healthcare across Europe, for the benefit of patients and the broader public.

Organisations working to save lives and improve health outcomes are benefitting from cloud computing not only when caring for patients (which this paper refers to as “**primary use**” scenarios), but also when re-using patient data for public health, research and innovation (referred to here as “**secondary use**”).

### *A. Primary use: cloud computing for better patient care*

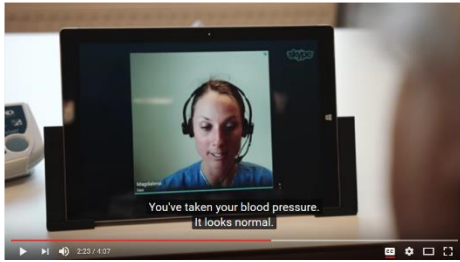
European legislators have decided that primary uses of patient data include, of course, making a diagnosis and delivering care to the individual patient, but also the management of health-care services (including ensuring the quality and cost-effectiveness of procedures, and settling claims for benefits and services in the health insurance system).<sup>1</sup>

Cloud computing enables these primary uses in several ways, among them: (1) improving patient engagement, (2) empowering care teams to be more productive and efficient, and (3) using smart devices to transform the care continuum. There are also some cases that fit into a fourth category of primary use: optimising clinical and operational effectiveness (although many cases aimed at optimising effectiveness, on a more “macro” level, are more aptly described as secondary uses, as discussed below).

The examples below help illustrate some common primary use scenarios for cloud computing and patient data:

### **Improving patient engagement**

**Nordic Health Innovation:** Cloud-based systems can enable healthcare professionals to interact with patients more easily in remote or under-served areas. This can lead to better treatment outcomes by enabling faster and more frequent patient assessment, counselling and follow-up. In Sweden, for example, Nordic Health Innovation, Sigma IT Consulting, Microsoft, Ericsson and Cambio are using the cloud to build self-service “virtual care rooms.” These are capable of ensuring that patients in remote areas are looked after even though in-person medical care is unavailable, by connecting them with carers via video link.<sup>2</sup>



*"Investing in virtual health rooms is an important step in our new, modern health care. They help reduce the accelerating costs, enhance the effectiveness of health care and make it more accessible by bringing us closer to the patients."* Björn Eriksson, regional director for Jämtland Härjedalen

**NHS Blood and Transplant:** Each year, NHS Blood and Transplant (NHSBT) requires 1.6 million units of blood to meet the needs of patients across England. A new cloud-based system helps NHSBT attract and schedule new donors, process their blood, and finally track, distribute and use blood donations.<sup>3</sup>



*"People could register to be a donor and it could take up to a month for them to get access to the website. We went from there, to seeing a donor registering to be a donor, early hours of the morning, donating blood later that day. We had about 20,000 donors using the old website, we're now over 1.1 million donors that have access to our digital service and are using it on a daily basis."* Anthony Evans, Digital Service Manager, NHS Blood & Transplant



**HUS Terveysylä (Health Village):** The Hospital District of Helsinki and Uusimaa (HUS), a joint authority covering 24 Finnish municipalities, have created an online, cloud-based "virtual hospital" / "health village" space for their patients, offering them advice, topical news, self-evaluation surveys and self-care services.

**Empowering care teams to be more productive and efficient**

**Wijkracht:** The social workers at Wijkracht are passionate about helping people. But they know that to deliver meaningful services, they must get into the community, not sit in an office. Wijkracht uses Office365, Skype for Business and OneDrive for Business to ensure their social workers have the information and tools they need in the field, but can keep that information safe and secure.



*"Now the information is available for me on the streets where I work with the youth-- in the neighbourhood, with people at home, wherever I like."* Tim Blanken, Wijkracht Social Worker

**Brighton and Sussex University Hospitals Trust:** Brighton and Sussex University Hospitals (BSUH) Trust turned to Skype for Business to enable a telemedicine program that allows consultants to assess stroke patients much faster, even when they are offsite or out of normal working hours. As an added benefit, BSUH Trust realised cost savings by using Skype for

Business over a bespoke Telemedicine system – allowing those savings to be redirected to other pressing patient needs.



*"The patient is likely to do better, because we know if you treat people quicker, less brain cells are impacted."* Ingrid Kane, Consultant Stroke Physician

### **Use of intelligent devices to transform the care continuum**

**DERPi:** The Diabetes Education Research and Prevention Institute (DERPi) created the Hyperglycemia in Pregnancy Trinidad and Tobago (HiPTT) app, which facilitates a system of data logging, analysis, visualisation, archiving and communications necessary to provide efficient support to pregnant women and identify diabetes risk early in pregnancy.



*"At the heart of HiPTT is a web portal which supports the full cycle of data entry, flow and visualization between patient, doctor and medical laboratories for the management of diabetes in pregnancy."* Surujpal Teelucksingh, DERPi Board Member.

**Poole Hospital NHS Foundation Trust, the University of Kent, Shearwater Systems and Graphnet Health:** This collaborative group of organisations is leveraging Azure to collect and analyse data from targeted patient groups supported by a wearable device in order to determine the feasibility of developing tools for patient care management.

*"I do feel excited about the idea that we can do something which meets the needs of the patient to actually improve their quality of life"* Dr Rupert Page, Consultant Neurologist, Poole Hospital

### **Optimising clinical and operational effectiveness**

**Epimed:** By better aggregating data and making use of predictive analytics through Azure Machine Learning, Epimed is helping clinicians define the best care pathways for each patient. In one health system this has resulted in a 21% reduction in Hospital Acquired Infections in the Intensive Care Unit (ICU) and a drop in ICU mortality rates.



*"Being able to deliver data driven care, you can actually save lives in the end."* Dr. Jorge Salluh, Epimed CEO

**NHS Blood & Transplant:** NHSBT offers a real-world example of use of the cloud to drive operational and clinical efficiency around DNA sequencing.

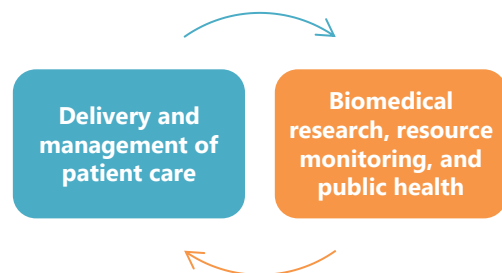


*"We're the first blood service in the world to sequence people's DNA for the purposes of stem cell transplants. With the cloud, we're able to store and manipulate enormous amounts of data, which we simply couldn't do if we were using on-premises technology. That means we can get a sample to a hospital within days whereas before it used to take many months to achieve the same objective. And with patients who have things like leukaemia and need stem cell transplants, days do really matter. . . . We reckon we're saving about £1.2m a year initially and that's going to go up to £1.6m a year just on the booking service alone."* Ian Trenholm, Chief Executive, NHS Blood & Transplant

Health institutions are also using the cloud for more routine but nonetheless important day-to-day research and analysis tasks, such as monitoring clinical efficiency and safe equipment use. Siemens has created a cloud-based platform, *Teamplay*, for at-a-glance sharing, analysis, and comparison of data from radiology machines spread across multiple locations. Teamplay allows radiologists to check that equipment is being used appropriately, and that patients are neither being exposed to overly high doses of radiation (e.g., X-rays), nor being kept waiting due to slow equipment turnaround times. The technology is already part of daily radiologist routines at Augustinian Hospital in Cologne, Germany.<sup>4</sup>

*B. Secondary use: leveraging health data and the cloud to improve research and innovation for patients and society as whole*

In addition to primary use, patient data – and cloud computing – can have extraordinarily valuable *secondary* uses. These secondary uses traditionally include statistical and scientific research. But they also include a range of uses that help public health and optimise clinical and operational effectiveness across the system, such as monitoring and combatting causes of mortality, morbidity and disability in society, understanding health care needs, ensuring optimal financing and allocation of resources, and other efforts to ensure high standards of quality and safety of health care, drugs and medical devices.<sup>5</sup>





Broadly, primary uses will be characterised by direct relevance to the services delivered to the patient – making a diagnosis, providing the treatment, billing, and ensuring that their care is delivered in a safe and efficient fashion. Secondary uses, meanwhile, are generally motivated by the wider public interest, even if the patient might be among the intended beneficiaries (e.g., improving outcomes for all patients with a similar disease).<sup>6</sup>

Ultimately, however, the precise line between primary and secondary uses may not always be clear, and may itself be up for debate as policymakers work through these issues. For instance, there are many opportunities for healthcare providers to use basic facility operations data to spot trends in care outcomes more quickly (for example, a spike in post-operative infections) that will enable the facility to take faster remedial action. Many of these types of uses are traditionally grouped within primary uses. Use of that same data for tracking the spread of a disease *across regions*, however, might typically be seen as secondary use.

Fullerton Health offers another example of secondary use:

**Fullerton Health:** Fullerton Health operates over 200 medical centres across 5 markets in Asia Pacific. They used cloud based analytics to identify for one client that 10% of the client's employees were behind 70% of claims. Additional analytics information subsequently allowed Fullerton to develop a chronic disease program that ultimately reduced claims among this group of patients by 60%.






*"Once the problem was defined and quantified, prescriptive analytics helped to create a plan to tailor processes for this employer to include better care pathways resulting in improved care for employees with chronic conditions." Tom Lawry, Director, Worldwide Health, Microsoft Corporation*

Secondary use could in principle be conducted on in-house, nationally-maintained or cloud-based platforms. The legacy restrictions discussed below, such as a need for patients to consent to the minute details of each research project, can prevent secondary use whatever infrastructure it would propose to use.

Yet cloud computing can be uniquely *transformational* in helping researchers conduct better, faster and more powerful secondary use. After decades of purchasing and maintaining on-premises mainframes and computing clusters – often at great expense – many research centres are turning to cloud computing. This allows these institutions to meet their ever-increasing processing needs in a secure, resilient, cost-effective, and scalable fashion, without the loss of flexibility, choice, innovation or national exclusivity (preventing international collaboration) that can characterise attempts to create national self-hosted IT platforms.



	In-house IT	National (public) IT	Cloud
<b>Affected by secondary use restrictions?</b>	Yes	Yes	Yes
<b>Potential benefits for society</b>	-	+	++
<b>Effort and cost for implementation and future modifications</b>	 <p>Most institutions likely <b>cannot</b> build and maintain their own reliable hyper-scale computing infrastructure <u>and</u> a broad library of data analysis tools (including machine learning and AI).</p>	 <p>National IT projects have a track record of <b>over-promising, under-delivering and vastly exceeding budgets.</b> Construction and operating costs are essentially <b>fixed</b> - there is no way to reduce costs during periods of low use.</p>	 <p>Each user benefits from the cloud's <b>scale and competitiveness</b>, driving quality and choice up, and prices down. Users only <b>pay for what they need.</b></p>

Hamburg-Eppendorf University Hospital is a case in point: it recently migrated its DNA sequencing data analytics to the cloud. Its researchers praised the “enormous” step forward this represented, as analyses that used to take weeks can now be done in a matter of days. The effort has been so successful that the Hospital is currently looking to expand the gene analytics platform beyond its original research purpose, for use in direct cancer patient care.<sup>7</sup> Other countries are beginning to emulate this approach. In Finland, for example, Helsinki University Hospital and BC Platforms are building a cloud-based cancer data management and analysis platform for the University’s researchers.<sup>8</sup>

Ethical use of machine learning and artificial intelligence (AI) could mark the next frontier in cloud-powered healthcare innovation.<sup>9</sup> Using the cloud, scientists are already analysing massive datasets to drive major advances in language and image recognition, self-improving computational algorithms, and pattern or anomaly detection<sup>10</sup> – all of which could have direct applications to many important healthcare challenges. They could revolutionise machine-assisted diagnosis, biomedical and epidemiological research, and routine risk stratification and preventive care, which ensures that the most at-risk patients get the most immediate attention from healthcare providers. In some cases, image recognition algorithms are already outperforming pathologists, helping physicians form a better picture of patients’ prognosis.<sup>11</sup>

Spain’s Institute of Medical and Molecular Genetics (INGEMM) at La Paz University Hospital (Madrid) is one of Europe’s pioneers in the application of AI to genomics research. It is working to develop and train machine learning algorithms in the cloud, to ultimately help clinicians

spot and diagnose rare genetic diseases in children. Together with the Dravet Syndrome Foundation, for example, INGEMM is helping to find a cure for Dravet Syndrome, a rare but severe form of epilepsy. INGEMM and the Dravet Syndrome Foundation are using the cloud to power next-generation DNA sequence analysis, and for the safe storage of over 40 terabytes of genetic data.<sup>12</sup>

The use of AI and machine learning in health is also receiving support at the international level. The European Commission, for example, is one of several organisations supporting research in this area – including funding for the *INdividual Vascular SignaTure* (INVeST) programme, which seeks to apply machine learning to personalised management of cardiovascular disease risk.<sup>13</sup> The private sector is also actively engaged. For example, Microsoft recently announced Project Hanover, a “moonshot” company initiative to develop new, cloud-based tools for cancer research.<sup>14</sup> It also provides significant support to researchers across disciplines, including health.<sup>15</sup>

The application of AI and machine learning to secondary use of data means creating tools that can continually improve based on real-world data; in effect, they would help us learn from today’s care to improve tomorrow’s. Cloud computing and AI are therefore essential to integrated and intelligent health systems: they strengthen and accelerate the positive feedback loop between primary and secondary uses of data.

To seize the benefits of health innovation and empower better health outcomes, health authorities and data protection authorities can embrace the following **ideas and recommendation for action**, fostering a healthy debate with key stakeholders at national and international level.

---

## **1. Regulators and policy makers should be sensitive to differences between “primary” and “secondary” uses of health data.**

As with any other policy decision in the health sector, choices need to put “patients first,” and focused on advancing the overall interests and welfare of patients.

We can – and should – be going “cloud-first”, since infrastructure type, by and large, has no appreciable impact on patient privacy (on the contrary, by improving data security and information governance, it can enhance it). Instead, the key issue for stakeholders is working with patients to understand, and weigh in the balance, their perspectives and interests with regard to the different ways in which their data can be used.

- At one extreme, placing few or no limits on the use of patient data may mean that progress is quicker, care is more efficient, and overall health benefits increase for both individual patients and wider society. However, patients may be left feeling they have little control over their own private information, and no confidence that their data is being used appropriately. They may even fear discrimination, higher insurance costs, or other adverse effects, which might lead them not to seek medical help in the first instance. While some patient groups (*e.g.*, those with life-threatening or chronic illnesses) may be more comfortable with this approach, others may not.

- At the other extreme, placing excessive restrictions on patient data may prevent effective and timely treatment of the patient by all members of the care team – a risk that might be particularly acute in complex or urgent care cases. Overly rigid consent requirements might prevent effective treatment altogether, such as where the patient is incapable of providing the necessary consent or understanding what consent is being sought. Patient data may end up being *less* secure where restrictions have the effect of mandating storage of data in outdated on-premise computer systems, or even paper files. In some cases this is overly complicating cloud deployments, requiring hybridised systems where there might otherwise be no need to deploy them. And of course, excessive restrictions on secondary uses will slow research into new treatments and cures, and prevent people from discovering healthcare system inefficiencies and inequalities.

Having the patient as sole custodian and gatekeeper of their data can work in limited circumstances – for instance, patients allowing doctors to access data from their wearable devices, or volunteering for “data donation”-type projects. But it comes at a major cost to society (and even to their own care) if pushed to an extreme: it skews studies in favour of volunteers, it makes delivery of care less efficient, and it cripples potentially life-saving research and innovation.

The need to balance privacy against other important interests when setting health policy is a well-established issue. The European Standards on Confidentiality and Privacy in Healthcare (the “Principles”) were developed by ethicists, healthcare practitioners and privacy experts a decade ago, with the support of the European Commission. The Principles state that:

*“Healthcare professionals should respect the following three key principles of healthcare confidentiality:*

- *Individuals have a fundamental right to the privacy and confidentiality of their health information.*
- *Individuals have a right to control access to and disclosure of their own health information by giving, withholding or withdrawing consent.*
- *For any non-consensual disclosure of confidential information healthcare professionals must have regard to its necessity, proportionality and attendant risks.”<sup>16</sup>*

The Principles mirror European data protection law, including Article 8 of the EU Charter of Fundamental Rights,<sup>17</sup> Article 8 of the European Convention on Human Rights,<sup>18</sup> and Article 8 of the EU Data Protection Directive (95/46/EC).

These fundamental European rules all highlight that consent-driven, patient-controlled approaches to the use of patient data are superficially attractive, but that there is nevertheless a strong need for such data to be available for use even in certain cases where express consent is not available.

The rules therefore generally permit use of health data without the patient’s consent for (*inter alia*) medical purposes, some forms of research, and other substantial public interest situations, so long as this is proportionate. Determining where the appropriate balance should be struck may depend in significant part on whether the data is being used for primary or secondary purposes. More specifically:

- For primary uses, patients are likely to be concerned first and foremost with effective and efficient delivery of care, and that any information about their care is stored in a manner that unauthorised third parties cannot access it. Rules and policies should be appropriate to those considerations. With regard to cloud computing, this means that technology providers should ensure their cloud technologies meet robust industry security standards, that healthcare providers should pro-actively adopt those robust cloud-based solutions for patient care, and that policymakers should seek to eliminate unnecessary regulatory “blockers” to use of secure and effective technologies. This position should be harmonised across Europe.
- For secondary uses, in contrast, patients might have greater concerns about how their health data is being used and with whom and in what form it is being shared – and in particular that their data is not being used in ways that could adversely affect the patient’s own interests at a later point in time. Patients may also be concerned about the quality and scope of data held about them in a healthcare record they have never seen. All stakeholders in the healthcare ecosystem should take these and similar concerns into account and should not neglect the importance of public consultation around secondary uses.<sup>19</sup>

This approach is consistent with data protection rules in other major jurisdictions, including the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related U.S. rules, which lay down strict patient privacy protections. There, the question is not whether patient data can be stored in the cloud (it can, and often is), but rather whether it will be handled securely and confidentially. As for patient control, the HIPAA Privacy Rule makes a distinction between primary and secondary uses, imposing substantially more stringent restrictions on the disclosure of identifiable patient data for secondary uses.

Crucially for Europe, this position is also consistent with the Data Protection Directive, and its replacement, the General Data Protection Regulation (GDPR).<sup>20</sup> The basic EU rules are agnostic as to how health data is stored (in paper files, or digitally; on the premises, or in the cloud), so long as it is safe and patients’ rights are respected. Those rules specifically seek to eliminate barriers to the free flow of such data within the EU, and also permit its transfer to non-EU countries, so long as similarly high levels of data protection can be ensured there.

The EU rules also support the distinction between primary and secondary uses of patient data. Specifically, the Directive and the GDPR lay down a basic EEA-wide framework for confidential processing of patient data, without consent, where necessary for medical purposes, including management of healthcare services.<sup>21</sup> They impose stricter conditions around secondary uses – for instance, they permit use of patient data for research without the patient’s consent only when doing so is in the public interest – and leave Member States with greater discretion in determining how and when such secondary uses are permitted.<sup>22</sup>

This distinction between primary and secondary uses is an important one and should be carried forward in Member States’ thinking about policy around cloud computing in healthcare.

---

## 2. “Cloud-first” policies should be promoted to improve delivery of care across Europe.

Patients are less likely to have concerns about consent and the location of their data (for instance in the cloud), when their data is used for primary purposes. This is a view shared by many physicians and an increasing number of policymakers.

Requirements that data remains physically within a hospital or clinic, or even in a particular country, can impede the healthcare system’s key objectives: ensuring patient safety, well-being, and access to affordable care. Opportunities to use regional, national or cloud-based infrastructure for better patient care can all be hamstrung by local retention requirements (or outsourcing prohibitions), but given that cloud computing arguably carries the greatest potential for improving care, that is where these legacy requirements are most harmful.

Healthcare laws requiring local storage or processing of health data are particularly unnecessary, as national and EU data protection laws ensure high levels of protection throughout the territory, and restrict personal data from being sent to other countries unless there are effective guarantees in place that the data will receive an equivalent level of protection there.<sup>23</sup>

There is also a general consensus that patient care would be hamstrung if healthcare providers needed to obtain prior patient consent for all uses of patient data in all cases. To give just some examples of why prior consent can be unworkable for use of patient data:

- The patient may be unconscious or otherwise incapable of providing informed consent;
- Medical records might be unreliable or misleading if vital information were omitted following a patient’s refusal of consent (or later withdrawal of consent) for only some data;<sup>24</sup> and
- Preventing medical professionals from accessing a patient’s data may hinder the proper and cost-effective delivery of care.<sup>25</sup>

Instead, regulation should focus on ensuring that data is used for appropriate purposes, that it is sufficiently secure, and that the data processing can take advantage of cloud computing’s significant benefits, especially at scale. EU data protection law already does this, by imposing strict security, confidentiality, training, compliance and accountability obligations on data controllers and processors. These obligations apply to all processing of health data, whether or not cloud computing platforms are used. In particular:

- Unless the patient consents, health data processed for primary purposes must be “subject . . . to the obligation of professional secrecy or . . . an equivalent obligation of secrecy.”<sup>26</sup>
- A cloud provider, and all its employees, must strictly respect confidentiality and the instructions of the institution or doctor that entrusted the data to it.<sup>27</sup>
- Security is all-important: all parties handling the data must ensure that they “implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access . . . and against all other unlawful forms of processing. . . . [Such] measures shall

ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.”<sup>28</sup>

Despite the protections above – and the fact that a key goal of the EU’s data protection regime is to eliminate barriers to the free flow of data (including patient data) across EU borders – some EU Member States (or individual regions within them) have taken steps to impose additional, country-specific requirements on the collection or processing of patient data. These requirements sit on top of the protections afforded by EU law – but having been designed around traditional (on-premises, highly-localised) computing paradigms, they are now holding back the healthcare sector’s use of cloud computing to improve patient care tackle funding shortages.

The desire to provide additional protections to patient data may have noble origins. But the result has been a heavily fragmented regulatory framework around primary uses of cloud computing in European healthcare. In several countries, the regulatory environment is marked by legacy rules and requirements that offer few, if any, real protections for patient data, but impose major barriers to beneficial uses of cloud computing and related technologies in the healthcare sector. These barriers include:<sup>29</sup>

- **Restrictions on data flows out of the country/region in question.** Many countries allow health data to be stored anywhere in the Union. But there are exceptions. For example, the English National Health Service (NHS) currently requires special dispensation before certain patient data can be stored outside England.<sup>30</sup> Such data localisation rules mean that healthcare providers may be blocked from using cloud-based or other services that involve cross-border transfers of patient data – even if the service complies fully with EU data protection rules, and even if the service adheres to *stronger* data protection practices than the healthcare provider can achieve on its own.
- **Some Member States retain outsourcing prohibitions.** For example, it used to be the case that patient records in Belgium had to be kept “in” hospitals (following amendment of the rules in 2014, such records can now be kept “by” hospitals, but potentially offsite, or in the cloud).<sup>31</sup> Likewise, some German states restrict the ability to use third parties to process “social data,” including certain patient data.<sup>32</sup> As in the preceding example, these and similar restrictions may prevent healthcare providers in these jurisdictions from taking advantage of cloud technologies, even if they provide superior outcomes and stronger protections than the available alternatives.
- **Some Member States impose burdensome, highly localised accreditation or other assurance requirements.** For example, France’s health sector has been held back by its mandatory “patient data host” accreditation requirements. Despite initial interest, few companies applied for the accreditation, and even fewer managed to complete the procedure, prompting the French legislature and government to comprehensively reform the scheme in 2016. Highly localised requirements and procedures almost always increase costs – sometimes considerably – but may not provide corresponding benefits to patients.
- **Opt-in consent often stands in the way of digitisation and care team collaboration** (in which cloud computing can play a major role). For example, the French Dossier Medical Personnel (DMP), a national electronic health record, was launched in 2011. It cost more



than EUR 500 million to develop and deploy. But by October 2016, fewer than 1% of France's citizens had opted into the system.<sup>33</sup>

By contrast, less consent-driven systems have fared significantly better; for instance NIECR, the Northern Irish equivalent to the DMP, has seen major take-up. By contrast to the French DMP, the record's creation is based on an opt-out system; opt-in consent is generally required, however, to view its contents (with appropriate exceptions to that restriction).<sup>34</sup>

The UK, meanwhile, decided in 2013 that it was essential to encourage physicians to share patient data more widely. Historical over-emphasis on the duty of confidentiality had been thrown into stark relief, tragically, when it was found to have contributed to public authorities' failure to detect and stop the routine abuse and eventual death of two infants at the hands of their relatives.<sup>35</sup>

Thankfully, the number of Member States that still maintain these restrictions is decreasing, potentially in anticipation of the advent of the GDPR. But for those that do, these and similar national rules continue to adversely affect patients because they prevent healthcare providers from reaping the full benefits of cloud computing and related technology advances. And for those not affected by those rules directly, uncertainty nevertheless remains. Without additional policy stimulus, this lingering uncertainty will continue to hold back adoption of technologies that could significantly improve healthcare quality and reduce costs in Europe.

In June 2016, this unsatisfactory state of affairs led a diverse coalition of healthcare stakeholders – the European Cloud in Health Advisory Council – to call for comprehensive local, national and EU-wide action to remove needless restrictions on the use of cloud computing for patient care and, conversely, to consider making it the default option for future IT deployments in healthcare.<sup>36</sup>

In addition, 14 EU Member States declared in May 2016 that “[i]t should be ensured that data can move freely across borders, both within and outside the EU, by removing all unjustified barriers to the free flow of data.”<sup>37</sup>

Likewise, the European Commission's Vice-President for the Digital Single Market has similarly emphasised that data localisation is a “dead end”,<sup>38</sup> since such rules “will not lead to better protection, but to fragmentation.”<sup>39</sup> The European Commission is leading a significant “free flow of data” review of data localisation requirements around Europe.<sup>40</sup> In a January 2017 Communication on the topic, the Commission concluded that, in addition to strong economic justifications, there was also a security need to remove data localisation restrictions, given that they impede use of cloud computing services, “which are much less vulnerable to attacks.”<sup>41</sup> The Commission committed to “launch infringement proceedings to address unjustified or disproportionate data location measures” in Member States, and to explore further initiatives to promote the free flow of data in the Union if necessary.<sup>42</sup>

These and other policy statements have brought welcome scrutiny around the main obstacles to use of cloud computing for patient care. France, for example, is making its patient data host accreditation/certification procedures less burdensome and more internationally-aligned.<sup>43</sup> Meanwhile, the English NHS is looking at its patient data “offshoring” restrictions,<sup>44</sup> potentially to make them more agnostic about where the patient data is stored.

Wherever possible, local requirements should be aligned with existing European or global standards, such as ISO/IEC 27001, 27002, and 27018, which set forth robust data protection requirements (ISO/IEC 27018 is specifically focused on cloud computing). These standards are already widely used in the private sector, and increasingly referenced in national regulatory and procurement rules.

Reliance on such international standards helps to promote efficiency both for cloud providers (since they do not face different requirements in every market), and regulators (who can readily approve providers that have already been certified to comply with the standard in a different market).

International alignment also significantly benefits healthcare providers, as it ensures that they can choose from an international range of providers and services. This, in turn, helps patients most of all, since they more easily can obtain the medical benefits and cost savings that cloud-based services and applications can unleash.

With that in mind, countries are increasingly looking to adopt these international standards. France, for example, is expected to replace its current unique national requirements with a streamlined certification framework built around ISO/IEC 27001. Providers who already have an ISO/IEC 27001 certification will be able to rely on it, ensuring rapid and efficient progress through the French certification procedure.

But efforts to update legacy, cloud-impeding rules need to go further and faster, and need to be supported by broader policy work. Healthcare institutions need a clear message that not only is it possible to use cloud computing to help their patients, they should *actively* be looking to do so. Ireland is a shining example. A new Cloud First Digital Policy was recently adopted by the national Health Service Executive's (HSE) eHealth Agency. According to official HSE policy, this means that "all future procurements are to be developed as 'Cloud First' solutions and will have to create a special case to not be considered in this manner."<sup>45</sup>

---

### **3. All stakeholders should engage in dialogue and awareness raising that drive a better understanding of the value, safeguards and ethics of "secondary use" of data.**

Given the many ways in which healthcare professionals are already beginning to use cloud platforms and cloud-based services to improve patient care, it is encouraging to see growing momentum around efforts to remove regulatory blockers to these uses. Nevertheless, when it comes to secondary uses of patient data, including (but not limited to) in the cloud, greater discussion and public engagement is needed, given patient concerns around the perceived potential risks of such secondary uses.

There is widespread consensus in many circles that data saves lives, and secondary use - like the examples given in section 1 above - must therefore be supported. Researchers, policymakers, and some patient groups are enthusiastic about the tremendous potential value of secondary use of personal data in improving healthcare and health outcomes. The European Patients' Forum (EPF),<sup>46</sup> for instance, explained that:

“Patients are increasingly aware of the value and importance of sharing their data. From the patients’ perspective, use of health and genetic data is vital to advancing health research – this includes public health, medical and social science research (including psycho-social research). This is both in the patient’s interest and for the benefit of the wider community.”

As a result, the EPF concluded that it is “of vital importance that [revised EU data protection legislation] strikes the right balance between guaranteeing patients’ fundamental right to protection of their personal data while ensuring these data can be processed for research and health purpose[s].”<sup>47</sup> This call for balance has been echoed in statements by healthcare research charities,<sup>48</sup> legislators,<sup>49</sup> and official reports to a number of European governments.<sup>50</sup>

For example, the UK Clinical Practice Research Datalink (CPRD) collates data from over 650 primary care databases throughout the UK, ensuring that it is uniquely informative and representative of the wider population’s ages, gender and geographical distribution. It has resulted in over 1,700 research publications that have helped improve public health and the treatment of patients – for example seminal studies of vaccine safety, cancer treatment best practice, and the management of hypertension in diabetics.<sup>51</sup> At the international level, the DECIPHER project holds genetic and clinical data from over 22,000 rare disease patients in over 30 countries. It helps clinicians diagnose and treat their patients by comparing their DNA to the database, and helps researchers cast light on rare genetic disorders - dozens of which have been identified thanks to DECIPHER, as part of the 1,000+ peer-reviewed publications that used its data.<sup>52</sup>

At the same time, members of the public – and sometimes even their carers – can have significant concerns around secondary data usage. A report for the UK government, for instance, found that “[i]n general, people were content with their personal confidential data being used for the care they received. However, people hold contrasting views about information being used for purposes beyond direct care.”<sup>53</sup>

This situation is not unique to the UK. Europe-wide, patients are more likely to be concerned about the secondary use of their health data than about using their data for primary-care purposes. Even though data is often de-identified before re-use, and the parties handling it can adopt strict controls over its security, use and dissemination – which assuages many concerns<sup>54</sup> – some remain worried that patients could be re-identified from the data.

These are important concerns. If not addressed, they could cause patients to feel that their privacy is threatened and their dignity undermined. To the extent patients worry that their data could be re-identified, they may have legitimate concerns that they could suffer embarrassment, discrimination, loss of housing, welfare benefits, insurance coverage, or employment. The resulting lack of trust might even dissuade some individuals from seeking medical treatment in the first instance. Despite the scarcity of examples of any such risks actually materialising,<sup>55</sup> they may be front-of-mind for some patients (or their doctors) when they do not feel sufficiently informed about the risks and benefits of secondary use.

Public engagement and discussion around secondary use is therefore critical.<sup>56</sup> That debate needs to explore and weigh the relevant benefits and risks – *e.g.*, improved societal outcomes in health versus potential impacts on patient privacy. Society as a whole would benefit from a

stronger understanding of the effects of *not* engaging in secondary use, and of the safeguards that can and are being used to minimise any risks. Informed by that debate, privacy regulators and policymakers need to strike a reasonable balance between patient privacy concerns, and the public (including patient) interest in secondary use.

Today, countries sometimes err in favour of what they believe to be the measures that will best protect patient privacy, especially in the secondary use setting, irrespective of their possible impact on health research and society's ability to improve health outcomes and reduce costs. This may not be an optimal balance, however, and patient care, both in the short and long term, may suffer as a result.

Indeed, many of the "blockers" to cloud computing for primary healthcare uses<sup>57</sup> also apply to secondary use – sometimes even more so. For instance, when giving researchers access to de-identified patient datasets for secondary use, England's "NHS Digital" authority imposes contractual restrictions preventing them from taking that data out of the EEA without prior approval, even though doing so is permitted by UK law.<sup>58</sup> This limits international collaboration by depriving UK researchers of access to some of the most advanced research tools and platforms.

Consent is an important factor in secondary use. Although under EU law, consent is not always necessary for secondary uses of sensitive personal data (provided that such uses are in the substantial public interest, and the relevant country has a legal framework in place to permit and regulate such use), some countries nonetheless require it.<sup>59</sup>

Researchers can and often do raise important objections to opt-in consent requirements. For instance, conducting new and important analyses of patient data can be impossible if such use is considered "new" and is not covered by the original consent. In such cases, patients often can no longer be contacted for a new consent, while the cost of contacting and obtaining consents from patients that are contactable may be prohibitively high. This is a problem that plagues disease registries, for example, in some countries.

Given the practical challenges of obtaining opt-in consent for all uses, and fears that patients may lose too much control over their health data if *no* consent is required, some have suggested that "opt-out" consent represents the best compromise: consent is assumed for an identified, accepted range of secondary uses, but individuals are given the ability to opt out if they wish. This is a model that the UK Department of Health is actively considering for secondary use of patient data from the UK National Health Service.<sup>60</sup>

Opt-out approaches could be valuable, but face limitations of their own – for instance, datasets can become unreliable and lead to biased results if some patients opt out. For this reason, some researchers are not in favour of opt-out consent for secondary uses.<sup>61</sup>

It is clear that a population's preferred solution may vary from case to case (and country by country) – hence the importance of dialogue on these issues. While there are many potential frameworks for this dialogue, one way to structure a discussion around the various options is a secondary use "maturity spectrum", building on similar frameworks in use in other contexts.<sup>62</sup> In the healthcare space, this maturity spectrum is shown here:

*Appetite for smarter care through secondary use*

<b>Maturity level</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
<b>Main legal basis for secondary use</b>	Only with specific (use-by-use) opt-in consent from individuals	Only with "broad" consent from individuals describing the types / general objectives of secondary use	Narrow laws authorise specific secondary uses (without opt-in consent, but with safeguards)	Flexible laws authorise secondary use in broad terms, so long as strong safeguards are used
<b>Data made available for secondary use</b>				
<b>Value for society and patients</b>	-	+	+ +	+ + +
	<p>Secondary use is confined to short, specific projects, or other narrow opt-in scenarios.</p> <p>Small sample sizes means data is often unreliable.</p> <p>Testing new ideas and uses requires a new consent each time, which entails significant administrative costs and delays.</p>	<p>Initial set-up costs are still high, because of the need to obtain consent.</p> <p>And although the consents are broader than in maturity level 1, allowing more secondary uses, researchers will still experience severe limits.</p>	<p>Setting up projects for the authorised uses is easier, but new laws need to be passed (or consents need to be obtained) before other beneficial secondary uses can take place.</p> <p>Significant legal differences between countries are likely, preventing collaboration.</p>	<p>Secondary use is flourishing - the framework is agile enough to tackle new ideas and emerging needs.</p> <p>Healthcare gets smarter, and precision medicine can become a reality, because there is more "real-world" data to correlate symptoms, risk factors, treatment outcomes and costs.</p>

**Figure 1: Secondary use maturity spectrum**

The secondary use maturity spectrum in Figure 1 presents a highly simplified range of options; in practice, it is not unusual to find more complex or "hybrid" solutions. In England, for instance, the law allows medical secondary uses of health data to be authorised, on a case-by-case basis, by a national group of experts (the Confidentiality Advisory Group).<sup>63</sup> This approach sits somewhere between maturity levels 3 and 4.

In other countries, some broad categories of secondary use (e.g., Ministry of Health management and audits of the healthcare system) might have a broad and flexible legal authorisation (level 4), but others (e.g., clinical research) might usually need opt-in consent, and therefore still be at maturity level 1.

---

#### **4. Member States should ensure that their GDPR implementation enables privacy and security, and improves health outcomes.**

After two decades of steadfast operation, the EU's venerable Data Protection Directive is on the verge of retirement. Like the Directive before it, the GDPR is expected to provide the basic framework for patient privacy for the foreseeable future. The GDPR covers both primary and secondary uses of data, including patient data. Its adoption is forcing EU Member States to look again at their national health data rules and policies.

Driven by a need to keep up with rapid advances in technology as well as a handful of highly publicised privacy breaches since the Directive was enacted, the GDPR offers several major wins for patients concerned about their privacy – whilst still enabling patients to benefit from the use of new technologies such as cloud computing (Figure 2).

##### **Increased international protection**

- Under the GDPR, EU privacy protections will apply even more broadly across the world than they do today. They will apply to all entities that offer "goods or services" in the EU, or that process data relating to people based in the EU, even if the processing entity does not have a physical presence in the EU. This will ensure worldwide privacy protection for EU patients, wherever their data is stored.

##### **Greater harmonisation within the EU**

- Although EU Member States retain some discretion to tailor the GDPR rules, the GDPR will still bring greater harmonisation across the EU. This will give patients and policymakers greater confidence that patient data is protected to the same high standards wherever the data happens to be located. This will promote health solutions and innovations that involve cross-border care and the free flow of data.

##### **More accountability from organisations using the data**

- Organisations will be required to take significant steps to ensure (and be able to demonstrate) that they comply with the GDPR rules and respect patient privacy. New requirements include mandatory data protection impact assessments, "privacy by design," data breach notification, recordkeeping, and prior consultation of regulators before engaging in high-risk processing.

##### **Direct processor liability**

- Data processors - including cloud service providers - will now face their own statutory responsibilities and be directly subject to regulators' enforcement powers. Previously, if the provider was at fault, regulators were often restricted to prosecuting the organisation that hired them (the "data controller").

##### **New certification opportunities**

- The GDPR lays down detailed rules for certification schemes and codes of conduct. This could lead to greater cross-border recognition of certifications, which could make it easier for patients and healthcare providers to know that a third party can be trusted with patient data.

##### **More efficient and more secure data flows to the rest of the world**

- New ways to ensure that data stays protected to EU standards when it leaves the EEA (including certification of overseas data recipients, and EEA-wide Binding Corporate Rules) will give organisations greater flexibility around international data transfers.
- The Regulation imposes more stringent standards on organisations, even overseas, for instance with new rules around parental consent for use of childrens' data.

**Figure 2: The GDPR enhances the privacy protections of EU patients worldwide**

One of the greatest expected benefits of the GDPR is the further elimination of barriers to the free flow of data. As discussed earlier, the flexibility offered to Member States under the



Directive has allowed rules to proliferate at the national and local level that are not always conducive to patient care or innovation.

The GDPR deliberately restricts the proliferation of unique and potentially conflicting national rules. GDPR Article 1 lays down a fundamental, pro-cloud limitation on such divergent rules: “[t]he free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.”

GDPR Recital 53 makes clear that this rule applies even in the health sector: it states that any supplemental conditions on the use of health data, genetic data or biometric data “should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.” This “free flow of data” principle may help healthcare organisations unlock major benefits of cloud computing and cross-border care for their patients; no longer will doctors and patients be unable to use a cloud service simply because it is in a different EEA country.

---

## **5. Stakeholders should support research on a new ethical framework for health data and “data donation”.**

While Artificial Intelligence has the potential to democratise access to better healthcare outcomes, its application also carries significant ethical implications. Our society, our regulators and our regulatory landscape haven’t charted such implications yet. As a consequence, today’s ethical frameworks seem insufficient to address the specific challenges faced in health data analytics.

As recently noted in a [blog](#) by Professor Floridi at the Oxford Internet Institute (OII) at the University of Oxford, “we must ensure that the right frameworks are in place so that new technologies help rather than harm, human welfare, and that we avoid missing opportunities to improve living standards.” In this context, health authorities, research organisations and data protection authorities together with health stakeholders should aim to facilitate and explore the best frameworks for “citizen participation in research efforts”, including the concept of “data donations”, in a way to “respecting individuals’ rights as well as ensuring proper regulatory oversight of existing and future data exchange partnerships between governments and tech companies.”

Exploring new ethical frameworks for the use of health data and supporting research projects that consider the applicability of “data donation” for better health outcomes seem necessary to pave the next wave of sustainable and predictive healthcare. One source of inspiration could be a research project between the Digital Ethics Lab of the Oxford Internet Institute (OII) at the University of Oxford, the Data Ethics Group at the Alan Turing Institute (ATI), and Microsoft. The project, called “The Ethics of Medical Data & Advanced Analytics”, aims to foster research around the ethics of health data in Europe.<sup>64</sup>

---

## **Putting those recommendations into practice will ensure that Europe's new privacy framework best serves Europe's citizens – starting with its patients**

Faced with developments such as new opportunities from advanced technologies, increasing public health challenges, the entry into force of the GDPR, and the European Commission's focus on removing barriers to the free flow of data within the EU, several Member States are actively considering what an optimal patient data privacy regulatory framework looks like – *i.e.*, how best to balance privacy, patient health, and the public interest. Patients and providers must be integral to that discussion.

This is not a zero-sum game. If done thoughtfully, Member States and the EU can achieve a number of “easy wins” – policy actions that have clear benefits for patients and healthcare systems, without having any adverse impact on patient privacy. This includes:

1. Eliminating local (in-country or on-premise) data storage mandates. Recent hacking incidents<sup>65</sup> and hardware failures<sup>66</sup> strongly call into question any presumption that patient data is safer on hospital premises. Eliminating localisation mandates will help ensure that patients and their carers have access to the best IT services and infrastructure available, even when those services and infrastructures are outside of the carer's premises, or even the carer's country.
2. Further confining some of the more draconian requirements that currently impede cloud adoption – such as rigid opt-in consent rules – to secondary uses, given the more acute privacy concerns that patients may have with regard to such uses. At the same time, policymakers at all levels – local, regional, national and EU – should actively work to improve public awareness of the benefits and available safeguards around secondary uses of data.

Longer-term objectives could include:

- EU-wide certifications or Codes of Conduct for patient data protection. These should specifically address cloud computing, and could potentially distinguish between primary and secondary use cases. Preferably, they would rely on international standards that are already being followed by reputable cloud service providers when handling patient data; for instance ISO/IEC 27001, 27002 and 27018.
- Depending on patient attitudes to secondary use, after thorough public discussion about its risks and benefits, countries could agree on an EU-wide legal framework setting down permitted purposes and necessary safeguards for secondary use of patient data. That said, it is unlikely that the *platform* or *location* of such secondary uses (on-premises versus cloud) ought to be a material consideration. If a secondary use is permitted, it needs to be done as effectively and securely as possible. That typically means having access to scalable, cost-effective, and high-performance cloud computing platforms, wherever they are located.
- Broader adoption of cloud-first policies, particularly for patient care, where the need for effective, pragmatic, and technology-friendly care is most acute.

At the EU level, the eHealth Network, which brings together health IT experts from the health administrations of every Member State and the European Commission, should take an even more active role in coordinating national approaches to the use of cloud computing in healthcare and research.

Some or all of these objectives would ideally be achieved by May 2018, when the GDPR comes into force. This would bring together those elements of reforms needed to ensure that European healthcare and research gets the very best out of cloud computing, for decades to come, all while ensuring a high level of privacy and care for patients.

\* \* \*

---

<sup>1</sup> See Article 8(3) of the Data Protection Directive 95/46/EC (the "Data Protection Directive"): [The prohibition on use of health data without consent] shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services [subject to an obligation of secrecy]." This is repeated in similar terms in Article 9(2)(h) of the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"), which will replace the Data Protection Directive in May 2018 (see also GDPR Recitals 52 and 53).

<sup>2</sup> See <http://nhiab.com/en/solutions/>

<sup>3</sup> See <https://enterprise.microsoft.com/en-gb/roles/it-leader/azure-powers-donor-registration-booking-nhs-blood/>

<sup>4</sup> See <https://www.siemens.com/press/en/pressrelease/2015/healthcare/pr2015110094hcn.htm> for more details.

<sup>5</sup> This range of uses is reflected in EU data protection law - see GDPR Articles 9(2)(i, j), and Recitals 52-54 and 159.

<sup>6</sup> The Article 29 Working Party explains that "[The medical purposes provision in Article 8(3) of the Data Protection Directive] only covers processing of personal data for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these healthcare services, e.g. invoicing, accounting or statistics. Not covered is further processing which is not required for the direct provision of such services, such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims." See Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR) (2007) ("WP 131")*, available online at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf)

<sup>7</sup> See <https://customers.microsoft.com/en-US/story/using-data-analysis-on-azure-for-cancer-research> for more details.

<sup>8</sup> See <http://bcplatforms.com/news/bc-platforms-and-microsoft-to-provide-expanded-genomic-data-management-solutions-in-the-cloud/> and <http://bcplatforms.com/news/bc-platforms-to-collaborate-with-helsinki-university-hospital-to-apply-its-proprietary-genomics-management-platform-to-provide-clinical-benefits-for-cancer-patients/>

<sup>9</sup> See Royal Society, *Machine learning: the power and promise of computers that learn by example* (April 2017); available at <https://royalsociety.org/~media/policy/projects/machine-learning/publications/machine-learning-report.pdf>

<sup>10</sup> See, for instance, <https://azure.microsoft.com/en-us/services/machine-learning/>

---

<sup>11</sup> Beck A et al. 2011 Systematic analysis of breast cancer morphology uncovers stromal features associated with survival. *Sci. Transl. Med.* 3, 108. (doi: 10.1126/scitranslmed.3002564)

<sup>12</sup> See <https://enterprise.microsoft.com/en-us/customer-story/industries/health/dravet-syndrome-foundation/>

<sup>13</sup> See [http://cordis.europa.eu/project/rcn/205225\\_en.html](http://cordis.europa.eu/project/rcn/205225_en.html)

<sup>14</sup> See <https://hanover.azurewebsites.net/>

<sup>15</sup> See <https://www.microsoft.com/en-us/research/academic-program/microsoft-azure-for-research/>

<sup>16</sup> See European Standards on Confidentiality and Privacy in Healthcare, available online at <http://www.tisztesszegesadatkezeles.hu/letoltes/0bfzSIOH5Mng830WW6Qff596DQ57T2>; for more information, see

[http://www.cpme.eu/european\\_standards\\_on\\_confidentiality\\_and\\_privacy\\_in\\_healthcare/](http://www.cpme.eu/european_standards_on_confidentiality_and_privacy_in_healthcare/).

<sup>17</sup> EU Charter of Fundamental Human Rights (2007); available online at <http://eur-lex.europa.eu/collection/eu-law/treaties.html>

<sup>18</sup> Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950), available online at <http://www.echr.coe.int/Pages/home.aspx?p=basictexts>

<sup>19</sup> In the UK, for example, recent Wellcome Trust/ Ipsos MORI research found that (i) over 60% of people surveyed would prefer commercial research organisations to have access to health data, rather than society miss out on the benefits they could potentially create, but even so (ii) more than one in four people were not happy for their data to be used for commercial research; (iii) people were “extremely wary” of even anonymised data being used by insurance and marketing companies; (iv) 17% objected to private companies having *any* access to health data; and (v) 53% felt that strict rules that data cannot be passed on to third parties was an essential condition for any commercial access to health data. See <https://wellcome.ac.uk/sites/default/files/public-attitudes-to-commercial-access-to-health-data-summary-wellcome-mar16.pdf> for more details.

<sup>20</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); available online at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

<sup>21</sup> See reference 1, above.

<sup>22</sup> Member States have discretion to permit further secondary uses under Data Protection Directive Article 8(4), and, from May 2018, under GDPR Articles 9(2)(i-j) and 89. Note that the GDPR will also expressly allow Member States to set additional conditions around the use of health data (Article 9(4)), although it also reminds Member States that whatever rules they adopt cannot restrict the free flow of data within the EU (see GDPR Article 1(3) and Recital 53). Having such flexibility does not mean Member States should exercise it, however – and in fact, exercising it may be detrimental to patients.

<sup>23</sup> Article 25, Data Protection Directive; and Article 25, GDPR.

<sup>24</sup> Reports have indicated that, in France, healthcare providers’ reluctance to sign patients up to the national electronic medical record system (DMP) was driven in part by the fact that it gave patients powers to selectively omit content from their health records – see European Commission, *Overview of the national laws on electronic health records in the EU Member States – National Report for France* (January 2014), at p48; available online at [http://ec.europa.eu/health/ehealth/docs/laws\\_france\\_en.pdf](http://ec.europa.eu/health/ehealth/docs/laws_france_en.pdf)

<sup>25</sup> Data protection regulators, coming together across the EU to form the Article 29 Working Party, stated that “[in] some jurisdictions there is not only a fundamental right to data protection but also a constitutional right to optimal health protection: as a consequence out of this obligation for providing optimal treatment, some Member States have provided health professionals with mandatory access to the data available via the EHR system. This seems acceptable as long as the necessary balance is achieved by means of stressing other safeguards, such as detailed regulations on the circumstances of lawful access and on – severe – consequences in case of misuse of access rights etc.” See Article 29 Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR) – WP 131*; available online at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf)

- 
- <sup>26</sup> Article 8(3), Data Protection Directive. The GDPR clarifies that the data need not be processed by such a professional personally; it can also be processed *under their responsibility* (GDPR, Article 9(3)). So far as the authors are aware, this position is already *de facto* accepted in many EU Member States.
- <sup>27</sup> Article 16, Data Protection Directive: "[a]ny person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."
- <sup>28</sup> Article 17, Data Protection Directive.
- <sup>29</sup> These and other examples are discussed in more detail by Microsoft in its June 2016 whitepaper, *Accelerate Cloud Adoption in Europe's Healthcare Sector*; available online at [https://mscorpmedia.azureedge.net/mscorpmedia/2016/04/Accelerate Cloud-EU Paper with-logo.pdf](https://mscorpmedia.azureedge.net/mscorpmedia/2016/04/Accelerate%20Cloud-EU%20Paper%20with%20logo.pdf)
- <sup>30</sup> See NHS Digital (formerly NHS Connecting for Health), *Information Governance Offshore Support Requirements*, available online at <http://webarchive.nationalarchives.gov.uk/20160729133355/http://systems.hscic.gov.uk/infogov/igsoc/inks/offshoring.pdf>
- <sup>31</sup> Law of 10 April 2014 concerning various aspects in healthcare matters, s164.
- <sup>32</sup> This is derived, in particular, from the German Federal Social Security Codes, Chapter I, s35; and Chapter X, ss67 et seq. and s80. There are also questions as to whether outsourcing of patient data, in some German States, amounts to a criminal breach of professional medical confidentiality, contrary to s203 of the German Criminal Code.
- <sup>33</sup> See <https://web.archive.org/web/20161014015535/http://www.dmp.gouv.fr/>
- <sup>34</sup> See Health and Social Care Board of Northern Ireland, *Effective use of ICT in healthcare - Northern Ireland Electronic Care Record* (presentation given by Sean Donaghy, Director of eHealth and External Collaboration, to the NHS Confederation conference in June 2014); available online at <http://www.nhsconfed.org/~media/Confederation/Files/Events/ACE14/Sean%20Donaghy%20Health%20and%20Social%20Care%20Board.pdf>
- <sup>35</sup> See, for example, UK Department of Health, *To Share or Not to Share* (2013), available online at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/192572/2900774\\_Info Governance accv2.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_Info_Governance_accv2.pdf). The report's major new recommendation was that "[t]he duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies."
- <sup>36</sup> European Cloud in Health Advisory Council, *Accelerating Cloud Adoption in Healthcare: Call to Action* (June 8, 2016); available online at [http://az370354.vo.msecnd.net/wordpress/2016/06/AcceleratingCloudAdoptioninHealthcare\\_June2016v2.pdf](http://az370354.vo.msecnd.net/wordpress/2016/06/AcceleratingCloudAdoptioninHealthcare_June2016v2.pdf)
- <sup>37</sup> See joint letter of Member State Ministers to the Dutch Minister of Economic Affairs, Henk Kamp, dated May 2015. Available online at <http://blogs.ft.com/brusselsblog/files/2016/05/DSM-joint-letter-Kamp-1.pdf>
- <sup>38</sup> Comments made by Andrus Ansip, European Commission Vice President for the Digital Single market, in 2016. See <https://www.euractiv.com/section/digital/news/eu-countries-call-for-the-removal-of-barriers-to-data-flows/> and <http://www.politico.eu/pro/andrus-ansip-data-localization-laws-are-forcing-eu-to-intervene/>
- <sup>39</sup> See J. Fioretti, *EU looks to remove national barriers to data flows* (Reuters, September 29, 2016); available online at <http://www.reuters.com/article/us-eu-data-idUSKCN11Z19Q>
- <sup>40</sup> The European Commission ran several parallel studies into "free flow of data restrictions" throughout 2016, and published its preliminary findings and proposed solutions on January 10, 2017, which it opened to public consultation (on-going at the time of writing). See *European Commission Communication "Building A European Data Economy" COM(2017) 9 final*, available online at <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>; see also <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy>

---

<sup>41</sup> "Ways to achieve secure data storage or processing include removing obstacles to keep data in larger state of the art data centres, which are much less vulnerable to attacks, and enabling cross-border cooperation, i.e., one data centre being the back-up of another located in a different Member State." *European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, accompanying the document Communication - Building a European data economy (SWD(2017) 2 final)*, page 7; available online at <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>

<sup>42</sup> *European Commission Communication "Building A European Data Economy" COM(2017) 9 final*, page 8.

<sup>43</sup> A draft of the new requirements was published for consultation in September 2016, and is available online at <http://esante.gouv.fr/actus/services/agrement-des-hebergeurs-de-donnees-de-sante-publication-du-referentiel-de>

<sup>44</sup> See reference 30 above.

<sup>45</sup> See eHealth Ireland Strategic Programmes, Cloud First Policy, available online at <http://www.ehealthireland.ie/Strategic-Programmes/Cloud-First%20Policy/>

<sup>46</sup> The EPF is an umbrella organisation that represents, at the European level, 67 pan-European patient organisations and national platforms of patient organisations. See <http://www.eu-patient.eu/Members/The-EPF-Members/>

<sup>47</sup> See EPF letter to Members of the European Parliament regarding the Plenary vote on the Regulation on Data Protection (March 11, 2013); available online at [http://www.eu-patient.eu/globalassets/policy/data-protection/dp\\_letter\\_ep\\_march2013.pdf](http://www.eu-patient.eu/globalassets/policy/data-protection/dp_letter_ep_march2013.pdf)

<sup>48</sup> See, for instance, *Ensuring a healthy future for scientific research through the Data Protection Regulation 2012/0011(COD); Position of academic, patient and non-commercial research organisations* (December 2015), signed by 111 European organisations. Available online at <https://wellcome.ac.uk/sites/default/files/ensuring-healthy-future-for-scientific-research-data-protection-regulation-joint-statement-dec15.pdf>

<sup>49</sup> See, for instance, remarks made by Marisol Touraine (French Minister of Health) in 2015, as she launched a reform intended to lead to enhanced secondary use of French patient data: "The State has a duty to better exploit this data in the public interest, albeit while strictly respecting both the privacy of citizens and the public interest. It's a question of balance." Quotes reported by F. Grenier, in *Marisol Touraine (Ministre De La Santé) - "Pourquoi nous ouvrons les bases de données de santé."* (Journal du Net, February 17, 2015); available online at <http://www.journaldunet.com/ebusiness/le-net/marisol-touraine-ouverture-bases-de-donnees-sante.shtml>.

<sup>50</sup> See, for instance, the UK National Data Guardian for Health and Care, *Review of Data Security, Consent and Opt-Outs (supra)*, paragraph 3.2.3 (p24) available online at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/535024/data-security-review.PDF](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF).

<sup>51</sup> See <https://www.cprd.com/Bibliography/>

<sup>52</sup> See <https://understandingpatientdata.org.uk/case-study/treating-rare-genetic-diseases>

<sup>53</sup> *Ibid*, paragraph 3.1.4 (p23).

<sup>54</sup> *Ibid*, paragraph 3.2.4 (p24).

<sup>55</sup> In a recent analysis published in the British Medical Journal, researchers expressed the view that "[s]everal of us have been sharing data for a decade or more, including around illicit behaviours and stigmatised diseases. Between us we could find few examples of harm – certainly far fewer than examples of benefits – partly because we have worked hard to develop strong governance structures." E. Pisani et al. *Beyond open data: realising the health benefits of sharing data* BMJ 2016; 355 :i5295; available online at <http://www.bmj.com/content/355/bmj.i5295>

<sup>56</sup> See also Coppen, R. et al. *Will the Trilogue on the EU Data Protection Regulation Recognise the Importance of Health Research?* The European Journal of Public Health 25.5 (2015): 757–758; available online at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4582846/>. This paper explains, *inter alia*, that "[o]ur findings also show that trust is the paramount issue here. . . . It seems to us that much



---

more transparency and explanation is needed about how the 'further use' of patient data is the driving force of all improvement in health care and prevention."

<sup>57</sup> These are discussed in section 2 of this paper (see page 14, in particular), and in greater detail in *Accelerate Cloud Adoption in Europe's Healthcare Sector* (see reference 36, above).

<sup>58</sup> See clause 5.2 of the NHS Digital/HSCIC Data Sharing Contract, available here:

[http://content.digital.nhs.uk/media/19179/Data-Sharing-Contract/pdf/HSCIC\\_Data\\_Sharing\\_Framework\\_Contract.pdf](http://content.digital.nhs.uk/media/19179/Data-Sharing-Contract/pdf/HSCIC_Data_Sharing_Framework_Contract.pdf)

<sup>59</sup> Even consent itself is not always sufficient. For example in France, the national data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), must in some circumstances pre-authorise a researcher's anonymisation processes – even if the data subject gives informed consent to the proposed procedure.

<sup>60</sup> See UK Department of Health, *New health data security standards and consent/opt-out model* (consultation dated July 2016). Available online at

<https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care>

<sup>61</sup> See, for example, the testimony of Dr Gatta, leader of the EURO CARE research project, at p17 of the European Parliament Directorate-General for Internal Policies study, *Data Saves Lives: The Impact of the Data Protection Regulation on Personal Data Use in Cancer Research* (2015), available online at

[http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL\\_STU\(2016\)569992](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)569992)

<sup>62</sup> See, for example, <https://www.gartner.com/doc/3135317/introducing-gartner-digital-government-maturity>, and <http://dataevolution.org.uk/the-framework/>

<sup>63</sup> See <http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/>

<sup>64</sup> See <https://blogs.microsoft.com/eupolicy/2017/04/07/ethics-now-shaping-a-new-ethical-framework-for-health-data/#2CWdTYF1xx212Vpk.99>

<sup>65</sup> See, for example, the hacking of Groene Hart Hospital in 2012, which was the result of security flaws in old, legacy on-site software. H. Thole, *Hoe jouw bedrijf miljoenen kan verliezen door één computerhack* (Business Insider Nederland, June 15, 2015); available online at

<https://www.businessinsider.nl/hack-groene-hart-ziekenhuis-kosten-567711/>

<sup>66</sup> See, for example, L. Stevens, *Leeds still working to recover from pathology IT crash* (Digitalhealth.net, September 27, 2016); available online at [http://www.digitalhealth.net/clinical\\_software/48100/leeds-still-working-to-recover-from-pathology-it-crash](http://www.digitalhealth.net/clinical_software/48100/leeds-still-working-to-recover-from-pathology-it-crash)