Empowered by the cloud: How cross-border health data flows can create value for patients and boost health system efficiency

HIMSS

In collaboration with:

Roche

EXECUTIVE SUMMARY

Enabling cross-border health data flows without compromising patient privacy and data protections is one of the greatest challenges faced by policymakers around the world. To overcome that challenge, legislators need to anchor their work in frameworks and models that balance the benefits of shared health data for every stakeholder in a country's health ecosystem with robust governance of that data. Yet, the process of developing such guidelines is necessarily slow and painstaking.

This paper makes the case for why governments, policymakers, and healthcare institutions should facilitate cross-border health data flows and examines the expected benefits from the perspective of advancements in **research**, **patient access**, and **economic gains**. As a case in point, COVID-19 demonstrated the value of sharing health data for collaborative operational and research purposes. The speed with which digital health services were implemented for the benefit and safety of patients and clinicians, and the development of highly effective vaccines at an unprecedented pace, were notable achievements. But without a degree of collaboration enabled by some adjustment – however temporary – in data sharing policy and regulation, that scale of success would hardly have been possible.

The paper specifically draws attention to the role of **cloud technology**, which provides capacity to store and process large amounts of sensitive data under strict privacy and security protocols. In the healthcare and public health domains, research is increasingly conducted across cloud-enabled, networked environments equipped with AI-based analytical tools. Taken together, these capabilities can provide a neutral, apolitical interim solution while greater global policy alignment on international health data transfers is achieved.

The paper also reviews **national laws and regulations** that govern cross-border data flows, applying a "data restrictiveness" lens. It offers a glimpse into which countries lean toward open health data sharing, such as Singapore and countries in the Nordic and Baltic regions, and which have – intentionally or unintentionally – erected barriers to it, such as China and the European Union. Additionally, the paper evaluates the **openness of 15 countries toward the utilisation of cloud technology**: Australia, Austria, Brazil, China, France, Germany, Japan, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan, United Kingdom, and United States. Most of those countries have a progressive stance on cloud adoption.

Finally, the paper stresses the need for a global architecture and regulatory framework for managing international data transfers, and suggests that initiatives such as the European Union's European Health Data Space could provide some guidance for this. While the creation of such architecture and framework is ongoing, however, governments, policymakers and healthcare organisations will need to redouble efforts to develop and find alignment on shared standards and principles that facilitate cross-border health data flows.

Empowered by the cloud:
How cross-border health data flows can create value for patients and boost health system efficiency

Table of contents

OVERVIEW

Among the multiple challenges health systems around the world face today, two stand out that call our attention as health information management professionals: the unfinished business of digital transformation, and the dire need for global convergence around laws, regulations, and policies that govern the secure cross-border access to and exchange of health data.

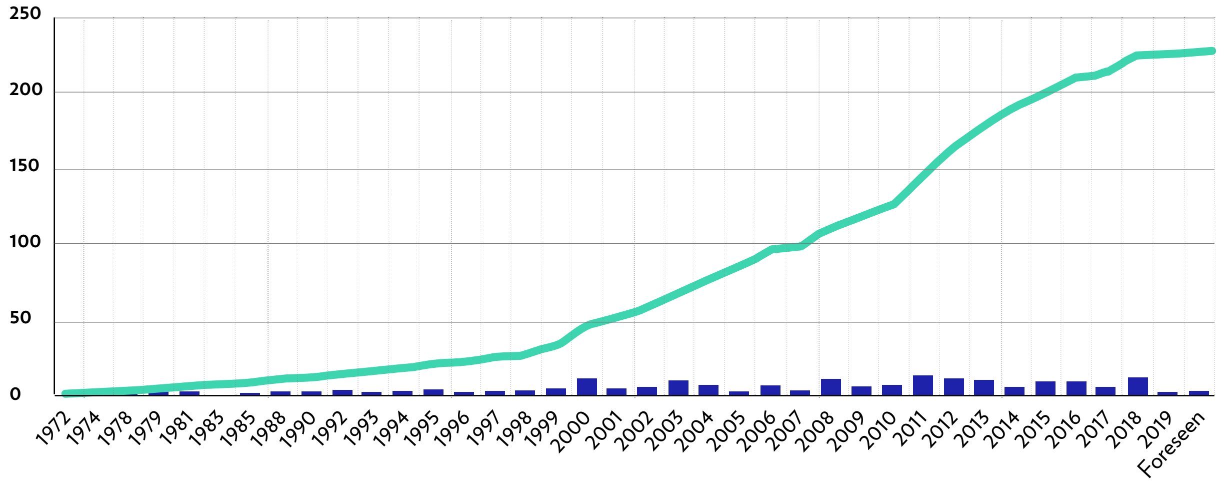
The capacity and willingness of policymakers, governments, industry, and health systems to tackle these challenges directly affect advances in innovation in precision medicine and biomedical research. Such advances increasingly depend on the injection of data-driven insights across all stages of research and development (R&D) and commercialisation of new drugs and therapies – but many of those insights can only be unlocked through the processing of large quantities of data gathered across borders. Thus, while the full potential of cross-border health data flows has yet to be realised, important inferences can be made based on current and emerging practices at a local level.

Beyond research and innovation, cross-border health data flows also matter to routine care delivery in a globalised world: with increased mobility for work, study, and travel – and people's right to be able to receive needed care wherever they are – there is a necessity to enable mechanisms for secure access to personal health information that "travels with the person" instead of being locked within national health system databases.

Yet, with concerns around data privacy, cybersecurity breaches, and national sovereignty growing, the number of regional, national, and local regulations restricting the flow of data and ring-fencing access to it is increasing rather than deflating. Just in the period 1995-2015, data policy measures increased by at least 800%.[1] Looking over a longer timeline, national regulations that impose restrictions on cross-border data flows have been steadily growing since the 1970s (Figure 1).

Figure 1. OECD statistics on data regulation growth, 1972-2019

CUMULATIVE NUMBER OF DATA REGULATIONS



■ Modifications — Count of Data Regulation

Source: OECD, Trade and Cross-Border Data Flows (2019), https://doi.org/10.1787/b2023a47-en

[1] Martina Ferracane, Restrictions on Cross-Border Data flows: A Taxonomy, ECIPE Working Paper (2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf

This creates a seemingly impassable divide between how health data infrastructure ought to evolve toward greater connectedness – powered by new technologies, such as advanced analytics, cloud computing, and artificial intelligence (AI), including generative AI – and how restrictive data measures, often put in place with the best intentions, can sabotage such progress.

Indeed, much of the motivation behind data restrictiveness measures is well founded. In recent years, cybersecurity breaches at healthcare institutions have become increasingly frequent, with potentially serious implications for patients' data.[2] Further, opaque data-sharing practices between hospital website operators, health technology startups, health app makers, and wearables manufacturers on the one hand, and Big Tech companies, ad companies, and data brokers that leverage users' data for marketing purposes on the other, have also undermined citizens' confidence in entrusting organisations with their health data.[3,4]

Striking a balance between the need to facilitate cross-border health data transfers as a core driver of innovation and the need to ensure that personal health data is protected from unauthorised access and tampering is not an easy task, and one where divergence of national policies and attitudes is to be expected. But health systems, patients, and societies demand solutions and cannot afford to languish while endless academic and policy debates take place.

[2] Healthcare Data Breach Statistics. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

[3] "Health apps share your concerns with advertisers. HIPAA can´t stop it." The Washington Post. September 22, 2022. https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/

[4] "Telehealth startup Cerebral shared millions of patients' data with advertisers." TechCrunch. March 10, 2023. https://techcrunch.com/2023/03/10/cerebral-shared-millions-patient-data-advertisers/

BENEFITS OF CROSS-BORDER HEALTH DATA FLOWS

Health data is the lifeblood of modern life sciences and healthcare organisations. In particular, the secondary use of health data – that is, the use of health data for purposes other than the one for which it was generated, such as direct patient care – can fuel discovery of critical insights, patterns, and associations that accelerate research and advance innovation in care delivery. But to unlock these capabilities, researchers and innovators need health data that is both voluminous and representative of diverse patient populations – conditions that cross-border transfers can make reality.

In this section, we provide an overview of the expected benefits and challenges of cross-border health data transfers across three key areas: research, patient access, and the economy.

RESEARCH

Health research is increasingly a global endeavour that depends on the collection, processing, and dissemination of de-identified personal data. To appreciate the potential of cross-border health data flows for advancing scientific research, improving healthcare delivery, strengthening health systems, and enriching statistical knowledge, it is useful to consider two key modalities of health data utilisation.

PERSONAL DATA (PRIMARY USE)

Primary use of health data refers to the use of individually identifiable health information, generally classed as protected health information (PHI) or GDPR-protected health information, during health service delivery and decision-making about the care of individuals to whom the data belongs.

The main uses of such data are to make confident therapy and treatment decisions and to personalise patient journeys (personalised medicine).

The following types of data may fall within the scope of PHI:

- Demographic data
- Medical records/histories
- Health status, lab test results
- Insurance policy details
- Other information that can be used to identify or contact a person

As per the U.S. definition of PHI, *protected* means that the information is protected under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Meanwhile, while there is no specific regulation governing PHI in Europe, health and genetic data are classed as *sensitive data* and as such benefit from additional protections under the European Union General Data Protection Regulation (GDPR).

REUSE OF DATA (SECONDARY USE)

Secondary use of health data refers to the use of health data for a different purpose than the one for which it was initially collected.[5]

The data being reused is typically owned by hospitals and health systems and includes administrative data, insurance claims or billing data, and patient health data contained in electronic medical records. This type of data is often reused for research and applications in patient safety and improving quality of treatments.[6] Because such data is stripped of individual identifiers, it can be processed at scale, combed for patterns and insights, and any learnings gleaned from it can be leveraged across the continuum of R&D and health service delivery.

Secondary use of health data can enable researchers, physicians, and data scientists to:

- Develop new therapies or fine-tune existing ones by harnessing AI algorithms with data from past clinical trials
- Correlate real-world data (RWD) and patient-reported outcomes with therapy effectiveness, including in subgroups of patients with similar characteristics or genetic profiles
- Propel cross-border public health collaboration, as evidenced in the coordinated vaccine development and health surveillance responses to the COVID-19 pandemic

[5] Meeting on secondary use of health data. World Health Organization. December 2022. https://www.who.int/europe/news-room/events/item/2022/12/13/default-calendar/meeting-on-secondary-use-of-health-data

[6] Schlegel DR, Ficheur G. Secondary Use of Patient Data: Review of the Literature Published in 2016. Yearb Med Inform. 2017 Aug;26(1):68-71. doi: 10.15265/IY-2017-032. Epub 2017 Sep 11. PMID: 29063536; PMCID: PMC6250993.

Outlined below are some of the most relevant use cases for cross-border data transfers in the context of primary and secondary uses of health data, whereby data sharing can facilitate continuity of care across countries and enrich the pool of data points from which insights are drawn.

Supercharging population health research and innovation

From a population health perspective, a prime example of how cross-border health data exchanges fit within and can add value to health systems is the European Health Data Space (EHDS). The EHDS is an initiative of the European Commission seen as a potential solution to some of the issues that the GDPR has raised for international health research.

The EHDS

- The EHDS legislation aims to **provide access to health data electronically to health professionals and researchers across the EU**, while safeguarding citizens' rights to retain full control of their data, restrict access to it, or obtain information on how it is used.

- To enable these data flows, the EHDS aims to **develop a common interoperable European format for patient summaries, e-prescriptions, medical images and image reports, lab results, and discharge reports accessible in healthcare providers' local language, in situations of cross-border healthcare**. Under a new legal framework, access to this data for researchers will be granted only for specific research purposes in closed, secure environments that eliminate the risk of identifying individual data contributors. The big picture that frames these efforts is the creation of a supranational health data governance structure for secure, controlled, yet seamless on-demand access to health data for legitimate research purposes.

- While the final form of the EHDS legislation is expected to emerge after discussions that will take place throughout 2023 and possibly 2024, the prospect of formalising a legal mechanism for health data flows across the EU is raising hopes that the region could lay the foundation for broader international guidance. As the authors of a recent article in the journal *Healthcare (Basel)* wrote, "The timing of the proposal is also apt in that **it places Europe at the forefront of attempts to intelligently regulate the sharing of health data** – a tangled issue that has so far received only limited and piecemeal treatment in other jurisdictions and regions. It offers a lead that could – as has happened in many other areas – see EU rules inspire international guidance."[7]

Indeed, the negotiations around the EHDS are taking place in the context of a growing need for a supranational data governance framework for the secure collection, storage, and use of health data to advance care access and health research.

> ***"Delivering research innovation and data-enabled services is going to be dependent on data in other jurisdictions. While existing and emerging trade and financial data flow models will provide frameworks, they don't deal with the specificity and unique aspects of health data and the benefits that can result from cross-border health data flows. The EHDS will set out what data governance will look like specific to some of the nuances within health data.***
>
> Jennifer Pougnet
> Global Data Policy
> Strategy Lead, Roche

[7] Horgan D, Hajduch M, Vrana M, Soderberg J, Hughes N, Omar MI, Lal JA, Kozaric M, Cascini F, Thaler V, Solà-Morales O, Romão M, Destrebecq F, Sky Gross E. European Health Data Space-An Opportunity Now to Grasp the Future of Data-Driven Healthcare. Healthcare (Basel). 2022 Aug 26;10(9):1629. doi: 10.3390/healthcare10091629. PMID: 36141241; PMCID: PMC9498352

Achieving data economies of scale for rare disease R&D

It is estimated that around 300 million people are living with a rare disease around the world and up to 1 in 7 people in G20 countries are affected by a rare disease.[8] By their nature, rare diseases – which number around 7,000 – affect a small number of patients in any one jurisdiction and, because they are uncommon individually, prevalence and incidence data for any one country or region is limited.

On an individual level, for many persons with a rare disease, access to medicines and care is inadequate due to a lack of known treatment, knowledge gaps in understanding of the disease, or limited research. Depending on the country, those factors may affect patients to a greater or lesser degree; patients in low- and middle-income countries generally face higher barriers. In addition, available disease expertise is often scattered across borders. This presents a problem not only for individuals and caregivers affected by rare diseases, but also for researchers working to develop therapies for treating them.

Patient registries – the tool most commonly used to manage rare disease patient data – attempt to address these concerns by collecting data on therapy effectiveness, clinical endpoints, clinical trial recruitment, clinical decision-making, patient-reported outcomes, cost-effectiveness, natural disease progression, and other variables. However, as registries are typically administered by different institutions/countries, from different perspectives (e.g., clinical, patient advocacy, service planning, industry, and academic perspectives), and are at different levels of maturity, the data is often spread across numerous, non-homogenous disparate repositories. This makes a comprehensive analysis and interpretation of the data for the purpose of research and drug development difficult.

To tackle the challenge of rare disease data collection and curation structurally, it is essential to pool data, research capabilities, insight generation, and knowledge sharing – both at a cross-institutional and a cross-border level.

[8] Bellgard, M.I., Snelling, T. & McGree, J.M. RD-RAP: beyond rare disease patient registries, devising a comprehensive data and analytic framework. Orphanet J Rare Dis 14, 176 (2019). https://doi.org/10.1186/s13023-019-1139-9

Case study: Asia-Pacific countries band around cross-border pooling of rare disease data

In 2018, the 21 countries that comprise the Asia-Pacific Economic Cooperation (APEC) intergovernmental forum ratified the first-ever *APEC Action Plan on Rare Diseases*,[9] one of whose key pillars (Pillar 9) is the pooling and use of patient data securely and effectively. The plan is intended to provide a framework for regional collaboration to overcome the disjointed approach to rare disease data collection, which derives from the fact that datasets are often owned by individual institutions or groups of clinicians across different jurisdictions.

One of the targets of the action plan is for all APEC countries to facilitate cross-border data flows by 2025, while respecting data privacy and domestic laws and regulations. Admittedly, striking the right balance is challenging, since most APEC countries each have their version of a medical records legislation which stipulates that medical records – including electronic medical records – should be kept locally, on a licensed premise. Nevertheless, as an indicator of progress, the plan considers the percentage of APEC economies that will have put in place policies to facilitate cross-border data flows by that date. (Incidentally, this may be an opportunity for those countries to revise or amend their respective medical records acts, notes Dr. Dhesi Raja, vice chair of HIMSS APAC Advisory Board.) One recommendation for achieving this goal is working with academia to pool trial data related to small patient cohorts across jurisdictions and designing a single regional registry focused on rare diseases, accessible to all APEC economies.

To support the implementation of Pillar 9 of the action plan, three Australian researchers developed a conceptual framework for a Rare Disease Registry and Analytics Platform (“RD-RAP”), with the goal of enabling data to be used across jurisdictions and borders. Encapsulating the problem the researchers saw, they wrote, “In rare diseases, there is inherent heterogeneity in the population such that individualised treatment and care is needed. However, of equal importance is building the evidence base for the rare disease population where it is critical to learn from individual experiences and aggregate these learnings across the rare disease population to find generality in disease progression, management and treatment.”[9]

The solution was built around interoperable components for each form of required analysis for the rare disease patient data journey. Citing the APEC plan’s target of facilitating cross-border data flows and calling on industry, clinicians, and patient advocacy groups to design an enabling environment for sharing patient data, the researchers explained that RD-RAP is architected not only to aggregate data exchanges between EHRs and patient registries, but also to evolve over time so as to capture data beyond what is currently available in any electronic capture system.

Eventually, the framework is expected to become “trial-ready” such that clinical trial participants can be recruited within the platform rather than by relying on word-of-mouth or advertising campaigns with uncertain reach. These strategic and technological developments in the Asia-Pacific region highlight the criticality of cross-border health data flows for achieving economies of scale and their importance to the rare disease stakeholder community at large.

[9] APEC Action Plan on Rare Diseases. https://rarevoices.org.au/wp-content/uploads/2020/09/APECActionPlan.pdf

Accelerating novel drug discovery and precision medicine

The increasing availability and decreasing costs of genomics data and sequencing technologies make it possible for these assets, when leveraged in combination with clinical and real-world evidence (RWE) data derived from EHRs and insurance claims, to yield unique, high-precision insights for drug development and clinical decision-making.[10]

Specifically, clinicogenomics and pharmacogenomics data can be analysed to identify new drug targets, validate new drug indications, and discover new drug response biomarkers. These implications point to another pathway through which cross-border health data transfers can benefit the life sciences and healthcare industries by enabling analyses of clinicogenomics and pharmacogenomics data *at scale*.

With regard to drug discovery, cross-border data flows can function as a mechanism for interlinking clinical and genomic data contained across disjointed, multi-jurisdiction datasets – much like the rare disease patient registries previously discussed – and turning them into big data. Generally speaking, meta-analyses of this big data can accelerate novel drug discovery because drug target patterns found across geographically, racially, and ethnically diverse data tend to increase the size of the evidence base and render it more representative, compared to data originating in a single jurisdiction. This in turn can help to mitigate potential bias and the need for time-consuming external validation, which can be especially valuable in the context of clinical trials for rare diseases, where small patient populations limit statistical power and can even hinder patient recruitment and enrolment efforts.

With regard to precision medicine, cross-border data flows can propel biomarker discovery to new highs by making possible large-scale generation of pharmacogenomic data – that is, the matching of drugs' pharmacological profiles to cell lines with various gene expressions, copy numbers, and mutations – and comparisons between the genomic profiles of tissue samples obtained via international exchanges of clinical trial data.

Because genomic biomarkers are essential for predicting treatment responses and thereby for selecting precision treatments for patients, the capacity of cross-border data flows to amplify the process by which novel genomic biomarkers get discovered represents a significant opportunity. This is especially true in the context of researching novel biomarkers for uncommon cancers, for which a large enough number of clinical trial participants and amount of data are often hard to find within the confines of a single country or jurisdiction. The opportunity to scale research that cross-border data flows usher in is complemented by the possibility to consult clinical outcomes, prior treatments, and other patient characteristics beyond the scope of clinical trials or R&D labs.

Addressing regulatory post-marketing commitments

Cross-border health data flows can play an important role in helping pharmaceutical and medical device companies improve post-marketing surveillance for safety and efficacy for their products. By facilitating insights derived from combined genomic data, clinical data, and RWD related to product performance and backed by the statistical power that a border-agnostic approach to data collection affords, international data transfers can thus offer benefits to the life sciences, healthcare, and regulatory industries across the full life cycle of drugs and devices.

[10] For a primer on clinicogenomics, see the Optum 2022 white paper, "Clinicogenomics: How new, linked data is advancing life sciences research." https://cdn-aem.optum.com/content/dam/optum4/resources/pdf/wf4340714-clinicogenomics-white-paper.pdf

ACCESS

Cross-border health data flows can be instrumental not only in advancing scientific discovery, population health research, and precision medicine, but also in expanding and improving access to innovative therapies (via accelerated approval) and to health services (via data portability). There are a few ways in which this can occur.

ACCELERATED APPROVAL OF INNOVATIVE THERAPIES

In addition to supporting post-marketing evaluation of product performance, RWD and its derivative, real-world evidence (RWE), can accelerate drug discovery, clinical trials, regulatory approvals, and commercialisation. In effect, this acceleration along the entire value chain translates into faster time-to-market for new therapies and – in a perfect world where access is not conditioned on national reimbursement decisions – into improved access to novel treatments.

DATA PORTABILITY

Ensuring patient safety, continuity, and quality of care across borders

As people travel across countries for professional or personal reasons, it is not uncommon for some to need emergency or non-emergency health services while they are abroad. In such situations, ensuring correct treatment often depends on the treating physician having access to patients' medical history. Yet, carrying one's medical history on a trip is unusual, while having access to it electronically is still the exception. As a result, in the event of needing medical assistance while abroad, patients often receive suboptimal care due to clinicians' lack of visibility into prior treatments or conditions.

Operationalising cross-border health data flows can help address this gap by making medical histories portable and "consultable" without undue barriers.

The HL7 International Patient Summary (IPS), a project of the Global Digital Health Partnership (GDHP), speaks to such efforts.[11] Developed within the GDHP's Interoperability Work Stream, in the context of the 2010

[11] International Patient Summary Implementation Guide. Published by Health Level Seven International – Patient Care Work Group. https://build.fhir.org/ig/HL7/fhir-ips/

U.S.-EU Memorandum of Understanding on advancing digital health, the IPS is an electronic health record containing essential, minimal, and non-exhaustive patient healthcare information intended for use in unplanned cross-border healthcare scenarios. The concept behind it – potentially replicable in the context of cross-border health data flows – is defining a standardised set of robust, potentially reusable core clinical data items that lend themselves to global interpretation and application beyond a particular region or country.

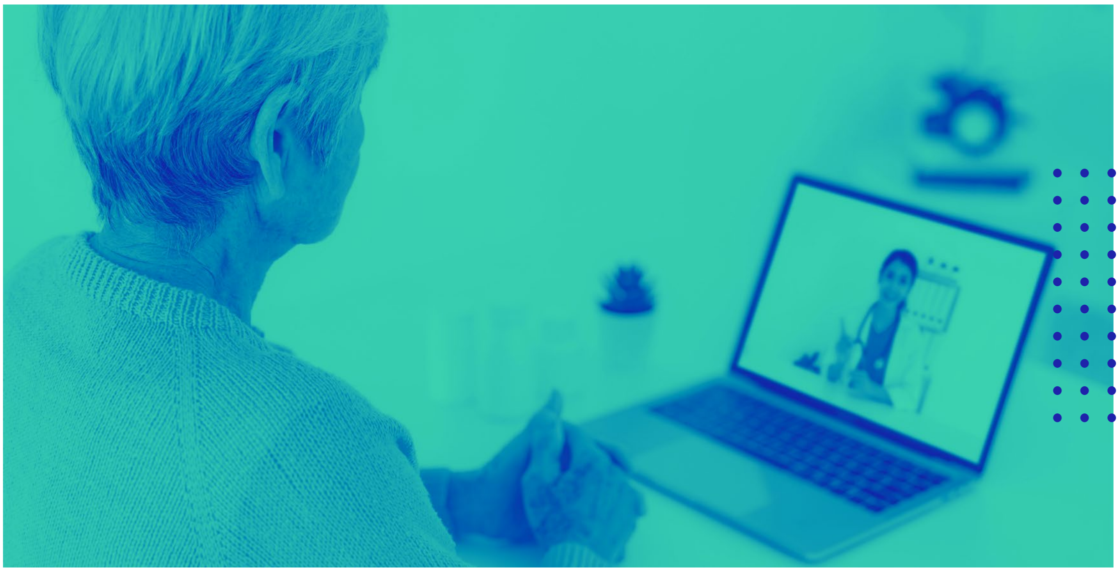
Facilitating use of digital health services

The COVID-19 pandemic accelerated acceptance and adoption of digitally delivered health services, interactions, and applications, including telehealth visits, remote patient monitoring, asynchronous patient-provider communications, digital therapeutics, and digitally performed diagnostics.

While data privacy and security policies relevant to digital health services are typically developed at local or, at best, national level, there are situations in which amplifying the scope of such services and interactions beyond national borders can have clear benefits for patients.

One such scenario presents itself in the form of patients seeking a second medical opinion, which for various reasons they may wish to obtain internationally (e.g., due to uninsured status combined with high out-of-pocket national healthcare costs, excessive administrative delays, etc.). This capability can be highly relevant in the context of histopathology, where slides and tissue blocks are routinely physically forwarded for a second opinion, which often leads to processing bottlenecks and diagnostic delay.[12] In fact, some health technology startups have already built a capability for digitally forwarded slide images for second opinion into their business model – a form of data portability.[13]

From a technology perspective, broadband connectivity and a telehealth software license are all that is needed to enable the provision of second opinion services across borders. From a data governance perspective, however, international health data sharing is still in for an uphill battle.



[12] Palmieri B, Laurino C, Vadalà M (2017). The "Second Opinion Medical Network". Int J Pathol Clin Res 3:056. doi.org/10.23937/2469-5807/1510056

[13] Livo.ai, a point-of-care blood analysis and whole-slide imaging startup, provides telepathology services via a global network of certified pathologists. It markets its telepathology platform as a solution to delays and bottlenecks that patients encounter in the lab test environment, which can fast-track diagnosis and beginning of treatment. To learn more, visit https://livo.ai/digital-pathology

A patient's view on why cross-border data sharing matters for access

Beyond removing obstacles to consulting medical records and operationalising digital health services, international data transfers can be instrumental in empowering patients to gain insight into how others like them have fared under different treatment options. As precision medicine advances and molecular tumor boards make increasingly complex customised treatment decisions, there is a real risk of the treatment decision logic generated in the process – and the resulting outcomes – remaining sequestered within the confines of individual hospitals. This prevents not only cross learnings between and among institutions, but also access to information by the patients on whose behalf N-of-1 experimental treatments decisions get made and by their physicians.

In 2020, a patient voiced those concerns in a blog post published on the World Economic Forum's Centre for Health and Healthcare website. A summary of the problem the blog author saw, and his proposed solution, are provided below.

THE BACKGROUND

Brad Power, a cancer survivor, shared in a World Economic Forum blog post[14] his experience with follicular lymphoma. He underwent several months of standard chemotherapy and at the time he shared his story, he had responded well to treatment and showed no evidence of disease. However, as his type of cancer has a high likelihood of recurrence, he wanted to be prepared with his next line of therapy, in case it was needed. He needed to know what worked and what did not for patients like him.

THE PROBLEM(s)

At a medical conference in January 2020, Brad listened to several health institutions describe improvements in decision-making and health outcomes for complex cancer patient situations. When he spoke to a few of the presenters, however, he was told they did not share their decisions or results across institutions.

In his post, Power wrote: "We need a global learning system to access each treatment decision and the associated outcomes. Why do health institutions not actively address the treatment data challenge and share their decisions and the associated patient outcomes?"

Power identified three barriers hindering global access to patient data:

01 **Privacy concerns:** Researchers and healthcare providers are concerned that sharing a wide range of data about each patient will make it easy to identify patients.

02 **Malpractice concerns:** Healthcare providers are hesitant to publicise their decisions as they fear that they would be liable for review and malpractice suits by patients and their families.

03 **Institutional and interpersonal competition:** Researchers who discover a new therapy gain recognition and money – as a result, they prefer to protect their intellectual property from competing researchers. They do not want to share data until it has been published, and even then, they prefer to share only the data that supports the approval of their therapy.

[14] Why we need access to global health data: a cancer patient's view. Brad Power. August 3, 2020. https://www.weforum.org/agenda/2020/08/why-patients-need-access-to-global-data-sharing-privacy-healthcare-medicine/

The end result of withholding patient data is that institutions and physicians fail to learn what may have worked, or worked better, in similar disease scenarios approached with alternative treatment logic. As Power highlighted, "A physician or board knows why they made a recommendation and may track the results, but they do not have much insight into the decisions of other physicians or other boards and the associated outcomes."

A CALL TO ACTION

Power called for a breaking down of barriers between health institutions to enable patients and clinicians to access global data about individual patient treatment decisions and outcomes. He observed: "Currently, health institutions have more power than patients, and their objectives do not always line up perfectly with ours. The entire healthcare industry finds this acceptable, but we should refuse to accept it. Patients need to fight to open access to relevant data from other patients."

Power cited the US-based non-profit organisation Cancer Commons as a model for how this can work. Patients get treatment advice from Cancer Commons, similar to how they would get a second opinion from a specialist at an academic cancer research centre. The organisation captures all treatment options discussed, as well as the rationale for why an option has been recommended or not for a given patient. It then monitors patient progress using both patient-reported outcomes and real-world data contained in records accessed under HIPAA with patients' permission. To encourage sharing and learning, Cancer Commons works with academics within ongoing pilot programmes for various types of cancers.

Power concluded: "Patients need to join together to share our data – especially treatment decision logic and outcomes – with other patients with our disease, providers and researchers. Meanwhile, physicians and researchers need to apply emerging global data standards by partnering with patients in small groups. These focused experiments must capture the logic behind treatment decisions, monitor the progress of individual patients and enable sharing of real-world evidence globally for continuous learning."

ECONOMIC BENEFITS AND COSTS OF CROSS-BORDER HEALTH DATA FLOWS

While it is difficult to put an exact number on the economic benefits that could be realised through better cross-border data exchange legislation and implementation, there are various studies and proposals that point to the potential economic gains and cost savings from the enablement of cross-border health data flows.

Looking back, the COVID-19 pandemic demonstrated the economic benefits of sharing the expertise of professionals with different skill sets in terms of developing treatments and vaccines at speed – successes that could not have been achieved if barriers were not removed to enable the minds of researchers to come together. A paper by the International Monetary Fund proposing a cost-benefit analysis cited findings that for an expedited rollout of vaccines in an equitable manner across all countries, it was found that while "vaccinating 40 percent of the world's population by 2021 could cost around $50 billion, its engendered benefits could reach about $9 trillion in economic gains."[15]

As we mentioned earlier, once finalised, the EHDS will similarly enable the secure collection, storage, and use of health data to advance care access and health research. It is expected to save the EU around €11 billion over ten years: €5.5 billion will be saved from better access and exchange of health data in healthcare, and another €5.4 billion will be saved from better use of health data for research, innovation and policy making.[16]

In terms of reducing costs, University College of London study estimated the cost of drafting and negotiating standard contractual clauses (SCCs) – a set of contractual terms and conditions issued by the European Commission to protect personal data leaving the EU – to be between $68,000 and $136,000 for a data sharing agreement between a UK university and a US organisation receiving data and tissue samples.[17] It is worth noting, though, that while SCCs can provide a workaround for non-EU/EEA research organisations and initiatives dealing with the obstacles the GDPR has raised for international health research, SCCs are not viable when the entity is an extension of the U.S. government, such as the the National Institutes of Health (NIH) or public universities, because U.S. entities cannot agree to audits or dispute resolution in European courts, which SCCs require.

[15] Agarwal, R., & Gita G. (2021). A proposal to end the COVID-19 pandemic. IMF Staff Discussion Notes 2021, no. 004.

[16] Questions and answers - EU Health: European Health Data Space (EHDS). https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_2712

[17] "How to Build Back Better the Transatlantic Data Relationship." Information Technology & Innovation Foundation. March 2021. https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship/

CURRENT STATE OF HEALTH DATA RESTRICTIVENESS AROUND THE WORLD

On the issue of cross-border data flows, countries around the world find themselves at different levels of regulatory and technological maturity and are therefore progressing at different speeds. Before we dive into a discussion about the state of health data restrictiveness and how it impacts the implementations of cross-border data flows, it is useful to get familiarised with three key concepts that underpin this complex and dynamic topic.

Definitions

Data residency refers to the physical or geographic location where data about a nation's citizens or residents is stored. It is typically determined in compliance with local data protection and privacy laws. Organisations that provide cloud services across different sites and businesses that entrust them with their data may be especially susceptible to ever-changing data protection and privacy laws, and subsequently to data residency norms.

Data sovereignty refers to the privacy regulations and governance structures that data is subject to, depending on where such data resides and is processed. Data hosted or curated by one organisation may be stored across different geographic locations with different data sovereignty rules. Conversely, data subjects who reside in the same country may be impacted differently by data sovereignty rules, depending on the location of the data centres where their information is stored.

Data localisation refers to the requirement for, and practice of, storing and processing data originating from a given country within that country's borders. This is the strictest of the three data restrictiveness concepts. According to a recent article by McKinsey, 75 percent of countries have implemented some level of data localisation rules.[18]

A 2021 white paper by the Information Technology & Innovation Foundation (ITIF) painted a grim picture of the implications of excessive data restrictiveness rules: for every 1-point increase in a country's data restrictiveness, its gross trade output is reduced by 7 percent and its productivity slowed by 2.9 percent.[19] Even as the quantifiable impact on cross-border health data flows is currently unknown, as countries around the world continue to develop overlapping regulations concerning data privacy, residency, sovereignty, and localisation, taking stock of those laws and policies can advance understanding of the challenges for international health data transfers.

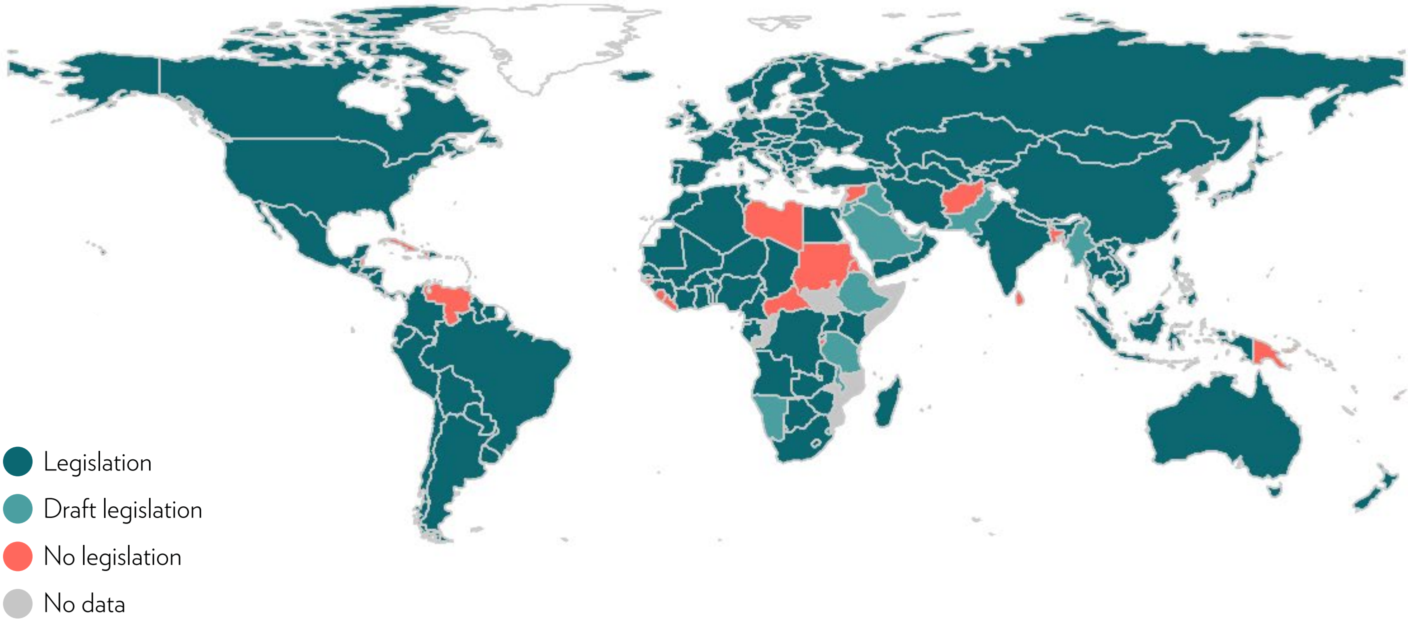
[18] "Localization of data privacy regulations creates competitive opportunities." McKinsey. June 30, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities

[19] "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." Information Technology & Innovation Foundation. July 2021. https://www2.itif.org/2021-data-localization.pdf

GLOBAL DATA RESTRICTIVENESS LAWS, REGULATIONS, AND POLICIES

National regulations that impose restrictions on cross-border data flows have been steadily growing since the 1970s. However, while this trend is not new, it takes on new meaning in the context of overwhelmingly cogent arguments in favour of liberalising international data transfers for the benefit of innovation in healthcare, research, and beyond. The figure below denotes the extent to which countries around the world have data protection and privacy legislation in place.

Figure 2. Data protection and privacy legislation worldwide



Source: UNCD, Data Protection and Privacy Legislation Worldwide (2021).
https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

It is useful at this point to look at the broader data governance status of countries globally and, more specifically, at the extent to which current regulations incorporate health data – and potentially erect barriers to cross-border data flows. Below we provide a brief overview of a selection of those regulations.

Figure 3. Restrictiveness of countries' data regulations and laws

Level of restrictiveness	Restrictive	Restrictive with elements of progressive	Partially restrictive	Progressive with elements of restrictive	Progressive
	🔴	🔴🟡	🟡	🟢🟡	🟢

Country/Region	Year of policy	Summary of policy	Level of restrictiveness
SINGAPORE	2012 Amended in 2021	***Personal Data Protection Act (PDPA)*** The PDPA recognises both the rights of individuals to have their personal data safeguarded and the right of organisations to collect and use personal data for legitimate purposes. Where transfers of personal data outside Singapore are concerned, the PDPA prohibits such transfers unless the receiving institution can ensure a level of data protection comparable to the protection under the Act.	🟢
UNITED STATES	1996 2016 2020	***Health Insurance Portability and Accountability Act (HIPAA)*** ***The 21st Century Cures Act*** ***Information Blocking Provision*** The Information Blocking provision, implemented as an add-on to the 21st Century Act, aims to correct some of the perceived flaws of HIPAA, which under the premise of protecting personal health information is seen to have given broad discretion to healthcare providers, health IT vendors, and other entities that control or process such information over denying researcher access, often imposing conditions for access beyond those required by HIPAA.	🟡

Country/Region	Year of policy	Summary of policy	Level of restrictiveness
CHINA	2021	***Personal Information Protection Law (PIPL)*** The PIPL has a strong data localisation component, which requires that personal data reaching certain thresholds be stored within China; for data that fall below those thresholds, a standard contractual clause (SCC) may be signed with the Cybersecurity Administration of China (CAC). Further, cross-border data transfers are subject to a security assessment by the CAC. Like the GDPR, the PIPL is extraterritorial in scope and applies to all entities that handle the personal information, including health information, of Chinese citizens. Unlike the GDPR, which allows data collection and processing on the basis of "legitimate interest" of the data controller, however, the PIPL does not allow such processing, unless explicit consent by the individuals whose data is processed is first obtained.	🔴
BRAZIL	2020	***General Data Protection Law*** (in Portuguese, Lei Geral de Proteção de Datos, or LGPD) The LGPD was largely modeled after the EU's GDPR, with some important differences concerning data anonymisation (the LGPD has a stricter interpretation than that of the GDPR) and the rationale for initiating cross-border data transfers.	🟡
SUBREGIONAL PARTNERSHIP NORDICS/ BALTICS	2021	***"Achieving the World's Smoothest Cross-border Mobility and Daily Life through Digitalisation"*** This three-year project aims to convert the Nordic and Baltic regions into the world's most integrated region by 2030. As part of that vision, the member states committed to promote the mobility of data necessary to provide health service in another Nordic or Baltic country.	🟢

Country/Region	Year of policy	Summary of policy	Level of restrictiveness
EUROPEAN UNION	2018	***General Data Protection Regulation (GDPR)*** The GDPR is one of the world's strictest data privacy and security laws. It is highly controversial among researchers in the public health, biomedical, and genomics fields due to its restrictive effect on international collaboration. In principle, the GDPR does recognise the legitimacy of processing personal data for scientific research and public health, but stops short of explicitly extending those permissions to research that involves the secondary use of health data.	🟡
TAIWAN	2015	***Personal Data Protection Act (PDPA)*** Under the PDPA, companies are required to give notice and to obtain consent from individuals before collecting, processing, or using their personal information. To promote the advancement of digital health, Taiwan's Ministry of Health and Welfare has enabled mechanisms for secure access to a large database of medical data accumulated through the national health insurance programme. Eligible entities that can apply for access to the data, which is provided in a de-identified form.	🟢🟡
JAPAN	2003 Amended in 2020	***Act on Protection of Personal Information (APPI)*** The APPI imposes various obligations on organisations that handle personal data, including a requirement for notification of the purposes for which the collected information is to be used, the availability of technical and organisational measures to protect the data, supervision of outsourced data processors, and restrictions on cross-border data transfers unless the data subjects have given their consent and the receiving institution has implemented protective measures that are at least as strict as those under the law. The legislaton also requires that the country of the receiving institution is on the whitelist authorised by Japan's Personal Information Protection Committee.	🔴🟡

IMPLICATIONS OF GENERAL DATA RESTRICTIVENESS MEASURES FOR HEALTH DATA

Data restrictiveness measures such as the ones outlined above have serious implications for cross-border secondary use of health data. The fragmentation and uneven quality of the data on the one hand – and the lack of harmonisation in data protection rules, governance models, and technical know-how on the other – contribute to those challenges, which may be categorised across several dimensions:

Legal: The key legal barriers constraining cross-border health data transfers are related to data privacy and information security. These typically manifest as different countries interpreting data privacy and data protection rules differently (e.g., European countries and healthcare organisations interpreting and applying GDPR differently). In addition, most countries around the world do not have national legislation specific to cross-border health data exchange.[20]

Cybersecurity: Continuously growing in complexity yet uncoordinated cybersecurity requirements for institutions that generate or process sensitive health data create additional hurdles for harmonisation.

Interoperability: The main barriers are related to technical and semantic interoperability. Technical barriers include a general lack of accessible electronic health records and electronic identification; semantic barriers include variability in clinical vocabularies and patient summary data sets across countries.

Quality: Issues around data quality abound, particularly where it concerns data that was not originally collected for research purposes but rather in the process of routine clinical care.

Funding: Insufficient resources and financial issues represent significant organisational barriers to cross-border infrastructure development.

[20] Genomic data sharing in Europe is stumbling – Could a code of conduct prevent its fall? EMBO Mol Med (2020)12:e11421 https://doi.org/10.15252/emmm.201911421

One notable "victim" of excessively stringent data restrictiveness measures is genomic research. Genomic datasets are increasingly collected by healthcare providers and shared with researchers – rather than collected by researchers alone – offering remarkable opportunities for advances in biomedical research. However, according to the Global Alliance for Genomics and Health (GA4GH), a standards-setting body working to establish international frameworks for genomic and health-related data sharing, genomic research requires cohorts of 10 million-plus people that represent different populations throughout the world. It is plain to see how data localisation measures could obstruct progress in that regard.

Indeed, GA4GH – which advocates for a global federated architecture – acknowledged as far back as 2017 that conducting genomic research and transferring knowledge from the research domain to healthcare depends on establishing data access mechanisms that are both appropriate to research applications and respectful of the rights of the individuals to whom the data pertains. Without such mechanisms, GA4GH members wrote, "the uptake of genomics into clinical practise will be slower, more expensive and riskier, and will differ country by country with little harmonisation. This would reduce the benefit to patients worldwide substantially and increase costs to healthcare systems."[21]

Noting the challenges that general data privacy frameworks present for genomic research in particular, the global Pan-Cancer Analysis of Whole Genomes (PCAWG) consortium in 2020 published a call for an international code of conduct for genomic data sharing.[22]

Various transatlantic and country-specific examples demonstrate how data restrictiveness measures – or the varying interpretations of such measures in different jurisdictions – may impede health research collaborations. Some of the most prominent ones include a long-running diabetes research project spearheaded by the U.S. National Institutes of Health (NIH), which was stalled after its Finnish partner, the National Institute for Health and Welfare, stopped all data sharing in 2018 because it perceived that the NIH could not guarantee that it would satisfy the Finnish institute's interpretation of the GDPR's requirements. The Statens Serum Institute in Copenhagen, which houses the Danish National Biobank, also suspended data transfers to key partners, including the NIH and the World Health Organization's International Agency for Research in Cancer (IARC).[23] Other cancer registries have also discontinued sharing data with Cancer Incidence in Five Continents (CI5), a series of monographs published every five years by IARC and considered a reference source for data on cancer incidence worldwide.

Transnational Alzheimer's research has also suffered. Since the GDPR came into force, some EU nations that had participated in the International Genomics of Alzheimer's Project – for which researchers from the U.S. and Europe have gathered DNA sequences from more than 90,000 people – limited data sharing, forcing the researchers to run separate data analyses on both sides of the Atlantic.[24]

Summarising how overly restrictive data flow regulations imperil advances in healthcare, researchers at the Information Technology & Innovation Foundation wrote: "While policymakers need to be certain that health data is carefully protected, they also need to ensure that legal frameworks allow for the reasonable, responsible, and ethical sharing of data—including transatlantic sharing—given the enormous potential social and economic benefits of new and improved health services. Unfortunately, there's a real risk that GDPR will impede transatlantic health research."[25]

[21] Genomics in healthcare: GA4GH looks to 2022. Ewan Birney, Jessica Vamathevan, Peter Goodhand. bioRxiv 203554; https://doi.org/10.1101/203554
[22] Genomics: data sharing needs an international code of conduct." Nature. February 5, 2020. https://www.nature.com/articles/d41586-020-00082-9
[23] "European data law is impeding studies on diabetes and Alzheimer's, researchers warn." Science. November 2021. Doi: 10.1126/science.aba2926
[24] Ibid.
[25] How to Build Back Better the Transatlantic Data Relationship. ITIF. March 25,2021. https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship/

CLOUD TECHNOLOGY AND HEALTH DATA FLOWS: OPPORTUNITIES AND CHALLENGES

Cloud technology holds great potential for centralising and streamlining data collection, curation, analysis, and insight generation in the context of cross-border data flows. At the highest level, the cloud can enable healthcare and research organisations to harness the value of international data flows by providing an environment that can enforce jurisdictional constraints and local service agreements while ensuring secure transfers of identity and data.

The utility of cloud technology for cross-border health data flows also lies in that if data flows are sufficiently seamless, it can facilitate solving the kind of complex computational problems that are inherent to large volumes of data being distributed across multiple locations. The data analytics capacities of the cloud could become especially relevant with the use of a federated model, whereby the data does not physically leave its locations but is tokenised or otherwise accessed "in place" by a data processor.

Similar to what having an overarching global legal framework can achieve, the process of moving the analysis to the data, rather than vice versa, can provide assurance to data custodians that may be skeptical of sharing their data internationally. In this way, cloud technology can address some of the existing barriers to operationalising cross-border data transfers by increasing confidence in the way data is handled. Conversely, the power of cloud computing itself increases as greater volumes of more diverse data are introduced into the models deployed within it.

> “
>
> ***Cloud computing is accelerating digital transformation in healthcare by democratising access to high-performance infrastructure at more affordable prices and allowing for more rapid deployment of digital services and solutions. It also enables experimentation and agility, so that policymakers and healthcare systems can fine-tune their solutions to the needs of their citizens, markets, and opportunities. These new generations of digital services allow for more interoperability and networking between systems and providers, and they are able to leverage newer technologies like high-performance computing for genomics and AI for automation and decision support. When matched with sufficiently skilled manpower, they can also deliver higher levels of cybersecurity and privacy protection for patients.***
>
> Leon Jackson
> Digital Transformation Lead, APAC, Roche

According to Leon Jackson, Digital Transformation Lead, APAC, Roche, privacy-preserving technologies and architectures today allow for the amalgamation and aggregation of large datasets for population-level research, which will fuel better drug discovery and precision medicine. Technologies such as federated learning and other modern uses of encryption and anonymisation allow for more seamless secondary use of data from primary sources without compromising patient privacy.

“While the shift to precision medicine and personalisation is easier to understand in our collective battle against chronic disease, we must remember that all of us need portability and continuity of care as we travel beyond our countries' borders. The promise of the cloud is how accessible and available it can be globally, and if our regulations get too hung up on the physicality of our data instead of the technical and legal controls to harmonise the governance of it, we might not be able to fully unlock its value for collaboration and patient portability,” he says.

A potent example of how cloud technology can harness the richness of data and insights that cross-border health data flows contain can be observed in the previously mentioned PCAWG project. An initiative of the International Cancer Genome Consortium, the PCAWG project leverages the cloud for the comprehensive analysis of petabyte-scale genomic datasets supplied by research centers in different countries and jurisdictions.[26] All of this is done in a virtual collaborative environment, within which the cloud's scalable IT capabilities enable the conduct of cohort studies on a massive scale, allowing researchers to address questions and draw insights that would be impossible with much smaller localised cohorts.

The PCAWG project's use of cloud demonstrates the utility of this technology for research where data is so voluminous that it is beyond the capability of a human team to analyse it. Another, opposite scenario in which the cloud can be critically useful is research in disease areas where data is so scarce that in order to obtain statistically significant results and reach valid conclusions, researchers must have access to far more – and more diverse – data. By centralising data from distinct databases, institutions, and jurisdictions, the cloud can scale available data such that it allows meaningful research that ultimately benefits patients.

[26] Molnár-Gábor, F., Lueck, R., Yakneen, S. et al. Computing patient data in the cloud: practical and legal considerations for genetics and genomics research in Europe and internationally. Genome Med 9, 58 (2017). https://doi.org/10.1186/s13073-017-0449-6

> “
> ***We are suffering from data poverty, namely, the inability of some groups of people to benefit from discoveries and innovations because these are developed on the basis of non-representative data.***
>
> Prof Effy Vayena
> Chair, Bioethics,
> Health Ethics and Policy Lab,
> Department of Health Sciences and Technology,
> ETH Zurich

If we engage in a bit of blue-sky thinking, another way in which cloud technology could derive value from cross-border health data flows is by analysing large volumes of data collected through medical-grade wearables and connected devices. The current lack of interoperability between the operating systems of wearables, sensors, everyday smart devices, and connected medical devices, combined with heterogeneous formats of the data they produce, preclude clinical decision-making based on such data (except in the case of implantable devices such as pacemakers, defibrillators, and continuous glucose monitoring systems). However, although the raw data collected by these devices does not flow into patients’ medical records and may be of little use to physicians, much of that information is already stored in proprietary clouds. With appropriate cloud-enabled analytic layers between the data and clinical teams, this trove of health information can be tapped for actionable insights, making physicians more likely to use it. When applied to cross-border data exchanges, these capabilities could create economies of scale for wearables data, with potentially new avenues for real-world data research.

COUNTRY-SPECIFIC CLOUD TECHNOLOGY RULES, REGULATIONS, AND RESTRICTIONS

Despite the range of possibilities for cloud technology to surface important health insights, the research and healthcare industries cannot realise its potential without enabling policies and regulations that allow its use at national and international level. Below we offer a glimpse of how several countries view cloud computing and the extent to which it is reflected in national guidelines.

Figure 4. Restrictiveness of countries' cloud technology rules and regulations

	Restrictive	Restrictive with elements of progressive	Partially restrictive	Progressive with elements of restrictive	Progressive
Country stance on cloud	🔴	🔴 🟡	🟡	🟢 🟡	🟢

Singapore

Cloud computing is an integral element of Singapore's digital objectives. As far back as 2016, the National Cloud Computing Office, nested within the Ministry of Communications and Information, published a gap analysis report aimed at enabling certified cloud service providers to provide compliant IT services to the healthcare industry.[27]
As a result of the government's strong promotion of cloud adoption across the economy, Singapore led the Asia-Pacific region in the Asia Cloud Computing Association's 2018 Cloud Readiness Index.[28] In addition, the latest edition (2018) of the BSA Global Cloud Computing Scorecard – the only report that tracks the global cloud computing policy landscape – ranked Singapore sixth out of 24 leading IT economies for its cloud computing preparedness, based on its legal and regulatory environment, including its data protection regime.[29]

Country stance on cloud: 🟢

United Kingdom

In 2018, the UK government's Department of Health & Social Care published a policy paper outlining its vision for the use of digital, data and technology in health and care services. Within that vision, it dedicated a section to the role of the public cloud, stating that all health and social care services should eventually run in the public cloud, with no more locally managed servers. The benefits of doing so, as described in the paper, were greater cyber resilience, the ability to run large projects with unpredictable processing needs, and increased security by enabling managed access.[30]

Country stance on cloud: 🟢

[27] Alignment of MTCS to Healthcare IT Security Policy & Standards: A Gap Analysis Report. Infocomm Development Authority of Singapore. 2016. https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Alignment-of-MTCS-to-HITSecPStds--Gap-Analysis-published.pdf

[28] Cloud Readiness Index 2018. Asia Cloud Computing Association. https://www.slideshare.net/accacloud/the-cloud-readiness-index-cri-2018-by-the-asia-cloud-computing-association-227586361

[29] 2018 BSA Global Cloud Computing Scorecard – Country: Singapore. https://www.bsa.org/files/reports/2018_Country_Report_Singapore.pdf

[30] The future of healthcare: our vision for digital, data and technology in health and care. UK Department of Health & Social Care. Published 17 October 2018. https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care

United States

In 2018, the U.S. enacted the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"). Its principal novelty was that it amended the Stored Communications Act of 1986, allowing federal law enforcement to compel U.S.-based technology companies to provide requested data, regardless of whether the data was stored on servers within or outside the U.S. One of the implications of the act is that the U.S. could, at least in theory, access personal data of foreign citizens stored on U.S. companies' overseas servers, which has caused the European Data Protection Supervisor (EDPS) to view the CLOUD Act as conflicting with the GDPR.

Country stance on cloud: 🟡

South Korea

In 2021, South Korea's National Assembly passed an amendment to the Act on Development of Cloud Computing and Protection of Its Users (the "Cloud Computing Act") that seeks to promote the use of cloud computing services by the national and local governments in addition to public sector customers. This move is aligned with a broader initiative spearheaded by the Ministry of Science and ICT to convert all information systems of the national and local governments and public institutions into cloud services by 2025.

Country stance on cloud: 🟢

China

China does not have specific laws or regulations on cloud computing, however a number of laws on adjacent issues provide visibility into the country's stance.

In 2016, the Ministry of Industry and Information Technology (MIIT) published the Classified Catalogue of Telecommunication Services of 2015, which contained the first reference to cloud services (referred to then as "internet resource co-ordination services"), along with a Notice on the Regulation of Cloud Service Market's Business Conduct. Other laws, including PIPL (2021), the Data Security Law (2021), and the Cybersecurity Law (2016) have imposed increasing responsibility on cloud service providers, and in 2021 CAC published a set of Regulations on Network Data Security Management, which included additional restrictions for data processing operations. The overall impact of these laws and regulations, combined with China's strict data localisation policies, is that only domestic cloud service providers are able to own and operate data centers in China. Today, China has the world's second largest cloud market after the U.S.

Country stance on cloud: 🔴

France

In 2018, to reinforce the use of cloud technologies in the healthcare space, the French government implemented a new Health Data Hosting certification mechanism.[31] Hospitals are largely using certified international cloud providers for EHRs. As a result of the measure, most hospitals in France today use internationally certified cloud-based EHR providers.

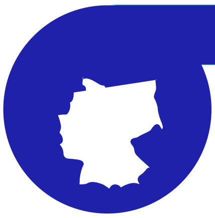
In 2021, the French government announced its National Strategy for Cloud Technology, mostly focused on cloud servers' locations, which may limit cloud providers' ability to transfer data outside of Europe.[32]

Country stance on cloud: 🟡

[31] HDH accreditation reference system. Agence Du Numérique En Santé. June 2018. https://esante.gouv.fr/sites/default/files/media_entity/documents/asip---referentiel-daccreditation-hds----v1.1---en.pdf

[32] French Government Announce National Strategy for Cloud Technology. OneTrust blog. May 18, 2021. https://www.onetrust.com/blog/french-government-announce-national-strategy-for-cloud-technology/

Germany



With comprehensive cybercrime legislation and an up-to-date cybersecurity strategy, Germany provides strong protection for cloud services. The country's privacy law is comprehensive as well, but onerous registration requirements may make cloud computing prohibitively expensive.

Cloud computing services in Germany are governed by general German and EU laws, including IT security laws and the German Civil Code. The most specific legislation governing cloud computing is the German IT Security Act 2.0 (in German, BSIG), enacted into law in 2021, which implements the EU Directive on Security Network and Information Systems ("NIS Directive," replaced by the "NIS 2 Directive" as of January 2023). In 2020, Germany's IT Planning Council adopted a government cloud strategy, and in 2022 Germany published a concept paper for a target architecture framework for the country's government cloud strategy.[33]

Country stance on cloud: 🟢 🟡

Australia

In 2020, the Australian Cyber Security Centre and the Digital Transformation Agency released new cloud security guidance to support the secure adoption of cloud services across the public and private sectors. The guidance is supported by Australia's Information Security Manual, Protective Security Policy Framework and the updated Secure Cloud Strategy, and aims to help organisations make sound decisions about the suitability of cloud service providers to handle their data, including personal data they may work with.

Country stance on cloud: 🟢

Japan

While there is no specific regulation concerning cloud under Japanese laws, the Government of Japan's Digital Agency promotes the use of cloud services by both central and local public administrations. In addition, both public and private cloud models are common and not exclusive of each other, such that an organisation may build its cloud environment on a public cloud, but also keep certain sensitive or important information separately on a private cloud.

Country stance on cloud: 🟢

Austria

There is no legislation in place that restricts the use of cloud in healthcare in Austria. The obligations of cloud service providers in Austria are identical to those of digital service providers. They must take appropriate and proportionate technical and organisational security measures with regard to the network and information systems they use for the provision of their services.[34] The healthcare sector uses software-as-a-service (SaaS) public, private, and hybrid cloud scenarios.

Country stance on cloud: 🟢 🟡

[33] Germany's government cloud strategy: target architecture framework. Version 2.0.1. October 2022. https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/20210813_DVS_-_Germanys_government_cloud_strategy___-_target_architecture_framework_v1.0_final_EN.pdf

[34] Austria: Cybersecurity. June 2022. One Trust Data Guidance. https://www.dataguidance.com/opinion/austria-cybersecurity

Spain

Spain has one of the most comprehensive cybersecurity frameworks in Europe, although its heavy reliance on registration requirements could act as a barrier for cloud services. It distinguishes between operators of essential services (OESs), digital service providers (DSPs), and cloud computing services. Cloud computing services are defined in Article 3 of Decree 12/2018 as "digital services that enable access to a modular and elastic set of computing resources that can be shared." However, the categories of subjects to which current legislation applies include only OESs and DSPs.

Country stance on cloud: 🟢 🟡

Brazil

Brazilian legislation does not directly restrict cloud computing services, either inside of outside of Brazil. As well, the LGPD – Brazil's main data protection law – does not specifically define cybersecurity regulations, such as those that typically govern cloud service providers. For matters related to cybersecurity, the LGPD points to the Brazilian data protection authority as the competent body on such matters.

Country stance on cloud: 🟢 🟡

Sweden

Sweden lacks direct and specific regulations regarding the procurement of cloud computing services. When procuring such services, government and public sector bodies must comply with Sweden's Public Procurement Act and the Act on Procurement in the Water, Energy, Transport and Postal Services Sectors.

Country stance on cloud: 🟡

Switzerland

Switzerland has not introduced any laws or regulations that specifically regulate the procurement of cloud services. However, Switzerland's Federal Data Protection and Information Commissioner points out that cloud service providers must comply with the data protection laws applicable in the country and specifically protect data against the following risks: unauthorised or accidental destruction or accidental loss; technical faults; forgery, theft or unlawful use; unauthorised alteration, copying, access or other unauthorised processing. Similarly, cloud service users must ensure that their cloud service providers protect any personal data by appropriate technical and organisational means.

Country stance on cloud: 🔴 🟡

Taiwan

Taiwan has no general cybersecurity legislation that may pertain to cloud computing other than the Cybersecurity Management Act. Beyond that, services rendered by third-party data centres or cloud providers must comply with the PDPA. However, if organisations in Taiwan wish to procure cloud services outside Taiwan, they should check whether they may be subject to sector-specific regulations for outsourcing data processing or data storage outside Taiwan. For example, for some industries, personal data is prohibited from being transferred to China.

Country stance on cloud: 🟡

While enabling cross-border health data flows and leveraging cloud technology remain under discussion, one domain expert offers a glimpse into what would need to happen at a policy level to "greenlight" data sharing in the cloud.

> **“**
>
> ***There are currently several technological solutions, including privacy-preserving technologies, that can facilitate safe and responsible access of health data. The solution to health data access, especially for cross border transfer of data, is only one part technology – and a big part political will. The recent news about the cooperation between the USA and the EU on research in AI and computing for the public good is a positive development that maybe signals more [forthcoming] cooperation for the critical area of health data access.***

Prof. Effy Vayena
Chair, Bioethics,
Health Ethics and Policy Lab,
Department of Health Sciences and Technology,
ETH Zurich

BORDERLESS INITIATIVES THAT AIM TO ADDRESS CONSTRAINTS

Amid a contentious political, technological, and cultural environment for cross-border data transfers, a number of borderless initiatives – apart from the bi-lateral and sub-regional data sharing partnerships described in Part II – have emerged to create the conditions for secure health data exchanges.

Observational Health Data Sciences and Informatics (OHDSI)

Founded in 2014, OHDSI is a multi-stakeholder, open-science collaborative with an established international network of researchers and collaborators across 74 countries. With access to over 800 million unique patient health records from around the world, OHDSI seeks to improve health outcomes by generating evidence from health data using large-scale analytics. OHDSI's data network is based on the Observational Medical Outcomes Partnership (OOP) Common Data Model, an open community data standard that standardises the structure and content of observational databases and enables federated analytics of the resulting data. OHDSI's coordinating center is housed at Columbia University.

> “
>
> ***Cross-border data sharing can be challenging due to variations in regulations and laws, as well as concerns around data privacy, security, and ownership. However, there is a growing demand for conducting large-scale cross-country clinical studies to generate more robust and timely evidence for better healthcare. To address this, OHDSI provides a data standard and network that enables participating institutions or countries to securely retain their data within their own borders while still participating in international clinical studies in a federated manner.***
>
> Prof. Mengling 'Mornin' Feng
> Senior Assistant Director,
> National University Health System, Singapore
> & OHDSI Singapore Chapter Co-chair

Trans-Atlantic Data Privacy Framework ("EU-U.S. Privacy Shield 2.0")

The Trans-Atlantic Data Privacy Framework, colloquially known as Privacy Shield 2.0, is a data transfer legal framework that replaces the previous EU-U.S. Privacy Shield legal framework, which was deemed invalid by the European Court of Justice in 2020 on the grounds that it did not provide sufficient protections to EU citizens from U.S. government surveillance. Although this framework is not specific to health data, the protections it offers may ease healthcare institutions' concerns around GDPR-compliant data sharing.

The APEC Cross-Border Privacy Rules (CBPR) System

The CBPR System, which was developed by all 21 APEC economies and endorsed for use in 2011, is a government-backed data privacy certification that APEC companies can join to demonstrate compliance with regionally recognised data privacy protections. The system's main benefit to consumers and businesses is that it provides confidence that intra-regional regulatory differences do not block commercial activity and the ability to deliver innovative products and services. While the system does not have a specific focus on companies that generate or process health data, obtaining a CBPR certificate may provide additional safeguards for cross-border health data flows.

> “
>
> ***The APEC CBPR System facilitates interoperability in the Asia-Pacific region and contributes to trusted flows of personal data in the region. Since the system has been established with general business in mind, businesses handling health data may need additional safeguards. Nevertheless, the APEC CBPR system could play an important role in the cross-border flows of health data by helping businesses be accountable partly through backstop enforcement mechanism assured by respective privacy enforcement authorities.***
>
> Junichi Ishii
> Director for International Affairs,
> Personal Information Protection Commission, Japan,
> and Chair of the APEC Digital Economy Steering Group
> (DESG) Data Privacy Subgroup

CONCLUSION: WHY CROSS-BORDER HEALTH DATA FLOWS ARE AN IDEA WHOSE TIME HAS COME

Over the coming years, advances in human knowledge, AI-driven analytics, and technology will almost certainly make the need for a connected global health data infrastructure that enables cross-border collaborative innovation more palpable. In parallel, the volumes of health data stored in local servers and jurisdictions – and the myriad insights hidden within, unless the data is freed to form part of a bigger picture – will continue to multiply. Researchers, data technologists, and healthcare innovation advocates will grow more restless in their demands to safely release health data from its siloes and onto a cloud-based "data superhighway."

Against this backdrop, holding health data hostage under the pretext of data privacy regulations or national sovereignty policies – especially as secure cloud environments become available – will become increasingly difficult to justify. Governments, policymakers, and healthcare institutions that resist cloud adoption and resist doing their part to support regulated cross-border health data flows will likely face mounting pressures to modify their stance, too.

> **"**
>
> ***Our ability to respond to future pandemics or world public health crises demands global cooperation. As we saw with COVID-19, expertise like finding ways of testing effectively and efficiently and at point-of-care was key – and that requires specific skillsets from across the globe. The COVID-19 vaccine was also developed faster than any other vaccine because we enabled the minds of researchers around the world to come together.***
>
> Jennifer Pougnet
> Global Data Policy Strategy Lead,
> Roche

To definitively convince governments and organisations that facilitating cross-border health data transfers and implementing secure cloud computing technology has more benefits than risks, a global architecture and regulatory framework for managing international data transfers is necessary. However, while having such global architecture in place is still a distant reality, governments ought to redouble efforts to find alignment on a set of universal standards and principles that facilitate cross-border health data flows. Only in so doing will there be a chance for cross-country, cross-regional, and global collaboration and convergence around cloud-enabled health data sharing to flourish.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology.

www.himss.org

Roche is a global pioneer in pharmaceuticals and diagnostics focused on advancing science to improve people's lives. The combined strengths of pharmaceuticals and diagnostics under one roof have made Roche the leader in personalised healthcare – a strategy that aims to fit the right treatment to each patient in the best way possible.

www.roche.com

Empowered by the cloud: *How cross-border health data flows can create value for patients and boost health system efficiency*

Authors:

Thiru Gunasegaran
Managing Editor, HIMSS

Gergana Koleva, *MSc, MA*
Healthcare Analyst and Writer

Contributors:

Afua van Haasteren
Manager, Health Policy and External Affairs, Roche

Hang Le
APAC Policy and Health System Shaping Lead, Roche

Varun Veigas
Leader - Policy and Strategic Partnerships, Health Policy and Patient Access Value Stream, Roche

Acknowledgements:

Jennifer Pougnet
Global Data Policy Strategy Lead, Roche

Robert Havasy
Senior Director, Connected Health, HIMSS

Lee Kim, *JD CISSP CIPP/US FHIMSS*
Senior Principal, Cybersecurity and Privacy, HIMSS

Graphic Designer:

Anna Galang