

Global Digital Health Diplomacy: The Global-EHR and First Steps for a Global Treaty on Digital Health

Henrique Martins,^a Jeremy M Thorp,^b
Paula Amorim^c

^aISCTE Business School, ISCTE-IUL, Lisbon, Portugal; Faculty of Health Sciences, University of Beira Interior, Covilhã, Portugal

^bIndependent Consultant

^cCentro de Medicina de Reabilitação da Região Centro – Rovisco Pais, Unidade Local de Saúde de Coimbra, Coimbra, Portugal; Faculty of Health Science, University of Beira Interior, Covilhã, Portugal

DOI: 10.25929/tnev8s71

ABSTRACT

Successful globalisation in health is dependent on Global Digital Health. As of today, however, we do not enjoy the interoperability needed to enable a global health care delivery system that is equitable, safe, effective, patient-centered, timely and efficient. People are afraid to travel to a remote location where access to their device or health data is not possible. They are aware that healthcare services in another country may not be of the same quality and these factors leave them feeling unsafe to travel and ‘chained’ to their locality.

A real worldwide cross-border digital health service includes a Global Electronic Health Record (G-EHR). This could be realized with co-ordinated efforts across countries. Some progress is possible through international agreements for mutual health data transmission, recognition of information systems and common approaches to the use of an international standard. To achieve full interoperability, however, political consensus is needed: Digital Health Diplomacy (DHD) efforts can deliver such alignment. DHD refers to concentrated international efforts towards supranational interoperability in Digital Health leading to cross-jurisdictional digital health services and data access and/or exchange.

KEYWORDS

Global digital health, electronic health record, digital health dipolomacy

1. Introduction

Global Digital Health should not just be limited to the “global” adoption of Digital Health. A global approach to disease management and health promotion is dependent on a co-ordinated effort to address the interoperability of people, processes and information systems crucial for this purpose; this requires Global Digital Health. This, however, cannot be limited to just the “global” adoption of Digital Health

by each country and territory but to the adoption of Digital Health across the whole world in all its interconnected complexity.

Orchestrated strategies emerge only where there are common perspectives on regional and world health and disease. The World Health Organization (WHO) strategy on Digital Health ¹ aims to improve health for everyone and everywhere by accelerating the development and adoption of appropriate, accessible, affordable, scalable and sustainable person-centric digital health solutions. These solutions would prevent, detect, and respond to epidemics and pandemics, developing infrastructures and applications that enable countries to use health data. This strategy requires contributors to:

1. Acknowledge that institutionalization of digital health in the national health system requires a decision and commitment by countries;
2. Recognize that successful digital health initiatives require an integrated strategy;
3. Promote the appropriate use of digital technologies for health;
4. Recognize the urgent need to address the major impediments faced by least-developed countries implementing digital health technologies.

However, it is not easy to serve every citizen worldwide through digital health. The challenges for digital health in the present and particularly into the future include:

- **Digital inclusion** – The capacity to ensure advanced tech is equitably accessible to both organizations and to all individuals.
- **Minimally disruptive telehealth/metahealth services** – The introduction of telehealth and “metahealth” services that offer high quality of care without significant disruption of health systems and paradigms.
- **Trustworthy digital clinical services** – Ensuring that people will trust the mHealth Apps they are offered, especially when these embed AI-based decision support systems or provide digital therapeutics (DTx)
- **Health data economy & health innovation** – Health data spaces for data exploration and care integration and innovation
- **Digital sovereignty & sustainability** – **Creation of digitally advanced infrastructures and processes that reflect cybersecurity, governmental sovereignty and cost-effective architectures.**

2. Global Electronic Health Record

Key to global digital health is the availability of a global Electronic Health Record (G-EHR), a set of interconnected digital systems and services that enable the sharing of personal health data across the globe. G-EHR supports the primary use of health data regardless of geographical, jurisdictional and language barriers. It is person-centric and citizen-driven, based on standards and de-facto enables the promotion of data harmonization, leading to a potential “Global Health Data Space” of anonymized health data for potential secondary and tertiary use. ²

A G-EHR is not a utopian idea. It does, however, require focus, concrete steps, value creation and determination to explore the following elements:

1. Creating worldwide voluntary patient and health professionals’ registries

2. Setting up a global regime/governance forum for the advancement of agreements and common creations
3. Enacting legally binding agreements grounded in international treaties of voluntary participation, in three areas:
 - i. global rules for telehealth
 - ii. global rules for the detailed reporting and information exchange in cross-border health threats
 - iii. decisions on the implementation and governance of concrete digital health services.

3. Interoperability

A vital feature of G-EHR is interoperability, defined as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged”.³ The European “LOST” framework for interoperability is based around legal, organisational, semantic and technical aspects.⁴

Efforts such as the collaboration with ISO, HL7 and SNOMED International on the International Patient Summary address the semantic and technical levels and could help lead to the open sharing of digital health standards. There are issues about languages, but the use of standardized terminology and codes would allow for local translations to be made available.

This is a start, but it is not sufficient. To take an example, medical devices (e.g. insulin infusion pumps or non-invasive home ventilators) are increasingly globally produced and standardised, yet the information that they require and generate is constrained to local, regional or national health systems. This in turn restricts citizens to their institutions, or even their homes. People fear to travel to a remote location where access to their device or health data is not possible. They know healthcare may not be equally safe, which makes them feel ‘chained’ and unable to travel. What is needed is full interoperability.

In 2022, the European Commission issued the Proposal for a Regulation on the European Health Data Space (EHDS).⁵ The EHDS Proposal has two main aims: 1) to grant citizens increased access to and control of their (electronic) health data across the European Union (EU), and 2) to facilitate health data re-use for research, innovation, and policymaking. The EHDS proposal for “natural persons” or citizens to have the right to a copy of their health data means that a traveller could take their record with them on a smart device, according to an agreed format, and show and/or share their data with anyone treating them.

The sharing of data is based around the European Electronic Health Record Exchange Format (EEHRxF). This is promoted by projects such as X-eHealth, XpanDH, xShare, Xt-EHR that, starting in the European Union, can be progressively road-tested and used across the globe with benefit for all as it also is being built on a set of international standards and SDOs contributions. Each country could have the specification and hence would be able to consume such data and make sense of the health record produced in both ways.

An approach could be to start with the essential information and progress to more complex data. The following worldwide cross-border eHealth services might be logical initial steps:

1. Global ePrescription system
2. Global sharing of minimum sets of data (for example, the ISO International Patient Summary) and, progressively, bigger components, such as vaccination passports/summary/e-cards

3. Exploring the global use of the EU EHRxFormat
4. Internationally approved minimum information sets for advanced data-rich medical devices
5. Internationally approved and maintained digital information leaflets for prescribed drugs
6. International sharing of large datasets for research/public health based on commonly agreed specifications

The availability of (free) open standards and the ubiquitous availability of smart devices would allow for early substantive progress in the area of primary use of data.

This is an ambitious mission, but with two principal barriers:

- First, it is not clear how health professionals take responsibility for data when data is transferred across borders and or when patients are given the right to upload data to their electronic health record, health professionals cannot control the data they receive, its language, or format.
- Second, different national healthcare systems with different disease classification systems in place, and differing levels of specialization and medical specialties could make it difficult to consolidate or compare data.

More work, therefore, is needed on joint approaches to legal and organisational issues. Two examples: health information cybersecurity, which presents particular challenges requiring global positioning and response, and artificial intelligence where the challenge is to exploit the opportunities it provides.

4. Cybersecurity for Digital Health is a Global Task

The high value of the sensitive patient data that healthcare organizations hold makes them prime targets for cyberattacks. ⁶ With the COVID-19 pandemic, remote work, virtual care, and electronic consultations became new targets for cybercriminals. ⁷

Current efforts in international cooperation in cybersecurity for healthcare, as those happening under the Global Digital Health Partnership (GDHP), should continue. They can be expanded, and this is likely to be of benefit to healthcare systems and societies in multiple countries. Such expansion can happen by:

1. Making existing cooperation in health cybersecurity more sustainable and structured
2. Expanding stakeholders' engagement to involve, in particular:
 - i. patient associations and professional scientific societies
 - ii. industry, from medical device and equipment manufacturers to software development companies
 - iii) research and higher education institutions
 - iv) standards setting organisations
3. Enlarging the number of involved countries and working under the auspices of larger, well-established international bodies like the Organisation for Economic Cooperation and Development (OECD) or the WHO.

At the global level, following this direction means ensuring such collaboration with regard to cybersecurity in general could eventually be hosted in a sustainable manner under the UN umbrella, or at the WHO. As we see the global discourse on the increased speed in the digitalization of healthcare and the increased need for international collaboration, we need to make sure that digital health comes with solid defence. Otherwise, whilst digital is good for health, it may bring more risks than benefits. Countries should implement national digital health strategies and be willing to support and contribute to international efforts and agencies where the sharing of that implementation can help them and boost these much-needed efforts.

Inspired by the WHO definition of health, we should see information security and health cybersecurity as a total state of integrity, availability and privacy, and not just the absence of cyber incidents. Cybersecurity in healthcare includes network security, application security, information security, operational security, disaster recovery, operational continuity, and end-user training.⁸ In this environment, cybersecurity concerns are critical as the essence of the health system functioning depends on the ‘health’ of the information systems that support it.

5. “First, Do No (Digital) Harm”

There is much discussion on the application of artificial intelligence (AI) to health. The availability and application of medical knowledge can deliver huge benefits but can overwhelm those trying to keep up with the latest data.

Most doctors will follow the “first, do no harm” rule as they have committed to in the Hippocratic Oath. Whilst the absence of digital solutions has been associated with lower patient safety, it is also true that digital threats to human health and dignity can come from misuse or abuse of digital health technologies. Such trade-offs are often the case with any impactful human invention. An increasing number of scientific reports point out to the potential risks of digital technology and its damaging effects on health. Literacy, digital and health literacy are powerful digital vaccines to fight this menace. These digital vaccines and some digital therapeutic interventions face distribution problems, their scope is often limited, the incentives and political visibility are often surpassed by more glamorous and eye-catching technologies. This is the case with blockchain EHRs or robotic physiotherapist care in highly matured digital health settings. A focus on literacy is essential, but it is possible to promote both. This has been shown in examples of mHealth use in low-resource rural areas to help healthcare provision and foster literacy, while capturing valuable data for further sophisticated secondary data uses.

Human dignity is at risk in privacy matters, in cybersecurity breaches, in robotized clinical decisions. It is also at risk when a two-year wait time for a visit to a dermatologist could be cut down to two months with the use of simple teledermatology screening. Reflection, pondering and, sometimes waiting and awaiting – these are old remedies to some of these challenges, although not the panacea.

6. Working together

The two examples of cybersecurity and AI illustrate the need for a co-ordinated international approach.

The GDHP and some regional efforts by WHO Regional Offices are trying to create bridges at the organisational level, but there are no common legal grounds on which to build.

Facing up to these challenges is a task not only for the WHO or any other one global organisation. High-level responsible health agents, such as ministries or public health authorities, need to understand that multinationals and other private or third-sector agents are all key to global development.

An approach to digital health is needed at each nation’s level, but also in the EU, or other regions, and globally for all citizens alike. A combination of policymakers, country digital health leads, suppliers and citizens can work together to make this happen.

globally for all citizens alike. A combination of policymakers, country digital health leads, suppliers and citizens can work together to make this happen.

In Europe, it could mean using the Eastern Partnership (EaP) and/or Central European Initiative (CEI) to enlarge the debate and capacity building outside immediate EU influence. Likewise, other regional organisations like the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), or the African Union (AU) should be more engaged with international health policies, and at the intersection of economic and well-being concerns ensure the security of their increasingly digital national health systems.

There are already relevant global actors co-ordinating efforts across different countries:

- i) Standards Developing Organizations (SDOs) such as the International Organization for Standardization (ISO), Health Level 7 (HL7), Integrating the Healthcare Enterprise (IHE),
- ii) clinical terminology-focussed organizations like SNOMED International or the Regenstrief Institute, responsible for the (LOINC, Logical Observation Identifiers Names and Codes) terminology,
- iii) promoters of digitalization efforts such as the Health Information and Management Systems Society (HIMSS) or the International Data Corporation (IDC) and, the International Medical Informatics Association (IMIA), with regional groups in America, Europe and Asia

Through a holistic, global and sustained approach to digital health worldwide, digital health can be seen as the only way forward for universal health coverage, for fair and balanced healthcare transformation, and for fighting the emergence and prevalence of many diseases and health-threatening conditions. This would lead into a new Digital-First Healthcare System, as Cassese⁹ notes, “in the global space, several global regulatory regimes act without subjection to one hierarchically superior regulatory system”.

7. Digital Health Diplomacy

An international treaty on digital health is urgently needed for two reasons: 1) to address threats from pandemics, present and future, recognizing the increasingly important role of digital health in their deterrence; 2) recognizing telehealth as a globalized phenomenon, where medical liability and privacy issues need to be regulated, however, in such a way that still enables the great benefits that can be achieved in preventative healthcare, health promotion and the provision of health services.

This is the empire of the ‘ad hococracy’», because there is no uniformity and no common pattern. Therefore, building this global digital healthcare system will require new set of skills and forums to face a constrained globalized world. Patient access rights, AI, digital ethics and privacy-as-a-platform are moving targets. These topics will be critical in the future.

To create this global digital health network and explore the value of this international ecosystem, we need Digital Health Diplomacy, which could be defined as follows: Digital Health Diplomacy refers to the concentrated international efforts towards supranational interoperability in eHealth/Digital Health.¹⁰ These may include international agreements for mutual health data transmission, recognition of information systems or common approaches to the use of international standards. It is the basis for real cross-border health data exchange projects, pilots and infrastructure creation, connecting all healthcare actors worldwide through data. It is key to global health cybersecurity risk alert and response, and to the use of digital health to contribute decisively to global health threats.

Digital Health Diplomacy is not just a matter of commercial interest or the facilitation of interoperability

amongst Electronic Health Records (EHRs). It is equally a matter of healthcare provision, increased and improved cross-border care, and, so important these days, fighting cross-border health threats. World strategies, memorandums and declarations about telehealth, eHealth and now digital health are not in short supply from many international and global organisations. ¹¹ Real working sandboxes and green fields await. Policy collaboration, technical collaboration and concrete common projects realization are key to establishing a worldwide interoperable health ecosystem, which is urgently needed. Digital health policy is an issue of growing interest in the world health policy. Like many other international efforts, this one equally requires targets and a common mission. Those of global Digital Health Diplomacy should be threefold:

1. To reach full digital health interoperability
1. To uphold health information cybersecurity
1. To guard from digital threats to human health and dignity.

Targets include the enactment of legally binding agreements grounded in international treaties of voluntary participation, in four areas:

- Global rules for telehealth
- Global rules on medicines/devices coding/identification and its usage for global digital health services (e.g. use of IDMP – PhPID)
- Global rules for the detailed reporting and information exchange in cross-border health threats
- Decisions on the implementation and governance of concrete digital health services.

8. Conclusion

Establishing a worldwide interoperable health ecosystem requires policy and technical collaboration as well as common projects' realization.

A global approach to healthcare is only possible through creating interoperability between people, processes and technologies towards a global electronic health record (G-EHR). Necessarily this means refining and stabilizing the vision and concept, linking it to global discourses and assets (e.g. International Patient Summary, Vaccination Passport or EEHRxF) and exploring what could be the first and subsequent steps to aggregate efforts around that common target departing from a set of commonly agreed human rights and digital health interoperability common grounds.

At the level of political and societal understandings, a Global Treaty on Digital Health is needed as cross-jurisdictional and cross-countries and continents digital health services are becoming a widespread reality. Dependencies and fears on data sovereignty are starting to block major cloud investments or rendering clouds to be “on premises”. Cross-country/continent prescription, global medical device production chains, or the need for EHRs and other digital tools certification and the mutual recognition processes all are trends that will need written-down principles, rules and commitments to boost trust and promote investment.

Building a global digital healthcare system is possible through Digital Health Diplomacy efforts. Digital Health Diplomacy is the basis for real cross-border health data exchange between all healthcare actors and is key to the use of digital health for universal health coverage and integrated care systems.

9. Conflicts of interest statement

The authors declare no conflict of interests regarding this publication.

References and notes

- [1] World Health Organization. *Global strategy on digital health 2020–2025*; 2019. Geneva, Switzerland: World Health Organization. <https://iris.who.int/bitstream/handle/10665/344249/9789240020924-eng.pdf>. Accessed August 6, 2024.
- [2] Martins H. Digital Transformation and Digital Leadership. *Healthcare Informatics Research* 2019;25:350. <https://doi.org/10.4258/hir.2019.25.4.350>.
- [3] Lehne M, Sass J, Essenwanger A, Schepers J, Thun S. Why digital medicine depends on interoperability. *NPJ Digital Medicine* 2019;2:79. <https://doi.org/10.1038/s41746-019-0158-1>.
- [4] European Commission: Directorate-General for Digital Services. *New European interoperability framework – Promoting seamless services and data flows for European public administrations*. Publications Office; 2017. <https://data.europa.eu/doi/10.2799/78681>. Accessed September 2, 2024.
- [5] Marelli L, Stevens M, Sharon T, et al. The European health data space: Too big to succeed? *Health Policy* 2023;135:104861. <https://doi.org/10.1016/j.healthpol.2023.104861>.
- [6] Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum* 2024;37(1):17–20. <https://doi.org/10.1177/08404704231195804>.
- [7] He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research* 2021;23(4):e21747. <https://doi.org/10.2196/21747>.
- [8] Giansanti D. Cybersecurity and the Digital-Health: The Challenge of This Millennium. *Healthcare (Basel)* 2021;9(1):62. <https://doi.org/10.3390/healthcare9010062>.
- [9] Cassese S. *Research Handbook on Global Administrative Law (Research Handbooks on Globalisation and the Law series)*. Cheltenham, UK: Edgar Elgard Publishing; 2016.
- [10] Godinho MA, Martins H, Al-Shorbaji N, Quintana Y, Liaw ST. "Digital Health Diplomacy" in Global Digital Health? A call for critique and discourse. *Journal of the American Medical Informatics Association (JAMIA)* 2022;29(5):1019–1024. <https://doi.org/10.1093/jamia/ocab282>.
- [11] World Health Organization Regional Office for Europe. *The World Health Organization in the European Region*. Copenhagen, Denmark: World Health Organization Regional Office for Europe; 2016