HEALTH DATA: GETTING CITIZENS ONBOARD

FOR A BETTER GOVERNANCE AND GREATER EFFICIENCY OF THE HEALTHCARE SYSTEM

JUNE 2021
POLICIES, INSTITUTIONS AND DEMOCRACY

RENAISSANCE
numerique

TABLE OF CONTENTS

INTRODUCTION

A SHARED CONSENSUS ON THE USEFULNESS OF DIGITAL DATA FOR THE HEALTHCARE SYSTEM

If there is one thing that the Covid-19 pandemic, which has affected the world for more than a year and a half, has been able to demonstrate, it is the usefulness of having reliable and up-to-date data in order to manage a healthcare system undergoing a crisis situation. Without daily data feeds from hospitals, nursing homes, biology laboratories, and other healthcare institutions, the development of indicators used to guide public decision-making (e.g. on lockdowns, curfews, etc.), like the incidence rate[1], the reproduction number[2] or the level of hospital bed occupancy[3], would not have been possible. In the field of healthcare, as in many other areas, data is a real tool for steering and management. It is also an important component regarding the transparency of decisions taken by public authorities, and monitoring their effectiveness. The dashboard.covid19.data.gouv.fr platform, for example, allows everyone to consult the progress of the epidemic situation (number of new hospitalised patients, number of people admitted into intensive care, number of vaccine doses administered, etc.) and visualise all the data available in map format. The value of sharing and using data in the healthcare sector goes, however, far beyond crisis management, and if the needs related to the fight against the Covid-19 epidemic have reinforced interest in health data, the link between data and health largely precedes the digital transformation of the sector. Provided it is used with all the guarantees that its sensitivity requires, this data can be used to improve and streamline healthcare pathways, develop telemedicine, move scientific research forward, in particular epidemiological research, steer the healthcare system, or even develop preventive medicine[4] which, despite the priorities it has been given, is lacking today.

---

1   Number of cases per week per 100,000 inhabitants.
2   Number of people infected by one sick person.
3   Number of intensive care beds occupied by Covid19 patients versus the number of beds at the end of 2018.
4   These goals are the ones most often cited by the people interviewed in the context of this report.

It is with this in mind that the French national "*Ma Santé 2022*" ("My Health 2022") strategy was elaborated, particularly its "Accelerating the digital shift" section, which emerged in May 2019 in the form of a roadmap. Led by the Ministry of Solidarity and Health, the roadmap focuses on five objectives: strengthening the governance of digital health (or e-health), intensifying the security and interoperability of healthcare information systems, accelerating the deployment of base digital services, deploying digital health platforms at a national level, and lastly, supporting innovation and promoting stakeholder engagement[5]. Five objectives in which health data is pivotal.

Some of these issues were included in the *Ségur de la Santé*, the consultation of stakeholders within the French healthcare system, which took place between May 25 and July 10, 2020. These negotiations arose in particular from the long-standing tensions within the healthcare system, particularly the difficult situation in which hospitals are at the moment, revealed with greater acuteness by the Covid-19 epidemic. Lack of beds and staff, inadequate funding, top-down decisions that are far removed from the reality on the ground, partitioning between town general practitioners and hospitals, between the healthcare and medico-social fields, complexity of the normative framework, lack of relevance of certain healthcare treatments[6], are the many alarm signals that were raised by the healthcare system stakeholders during this *Ségur*[7]. While they aim to respond to these urgent problems, in particular by upgrading the healthcare establishment and nursing home professions, the agreements resulting from the *Ségur de la Santé* are also intended to "*accelerate the transformation of our healthcare system in all areas.*"[8] Thus, the *Plan France Relance* (French recovery plan, which aims to accelerate the country's ecological, industrial, and social transformation) announced by Prime Minister Jean Castex on July 15, 2020, addressing *Ségur de la Santé* findings, plans to allocate 6 billion euros to the healthcare sector, including 2.1 billion euros

over five years dedicated to "*the transformation, renovation, equipment and digital upgrading of medico-social institutions*", and 1.4 billion over three years in order to "*close the gap within the interoperability and modernisation of digital health tools*"[9][10]. In addition, 136 million euros will be dedicated to cybersecurity issues, part of which will be specifically targeted at healthcare establishments.

At a European level, this ambition to transform the healthcare system through digital technology and data is embodied through the data strategy presented by the European Commission on February 19, 2020, which advocates the implementation of a common European health data space[11].

The observation that the potential of this data could be used for the healthcare system and to benefit citizens is thus widely shared within the European Union, as also shown by the various initiatives underway and the massive investments made in this direction (reinforced by the health crisis). But although there is abundant data, and despite the major projects initiated, we still haven't been able to fully grasp it in order to improve the healthcare system and make it more efficient and democratic.

HIGHLY SENSITIVE ASSETS, WHOSE USAGE RAISES MANY QUESTIONS

Whilst the sharing and use of data in the healthcare sector holds many promises, we must not overlook its highly sensitive nature. Since 2018, the GDPR defines health data as "*personal data related to the physical or mental health of a natural person, including the provision of health care*

5   French Ministry of Solidarity and Health, « Accélérer le virage numérique » ("*Accelerating the digital shift*") information pack, National strategic digital health roadmap, May 2019: https://esante. gouv.fr/sites/default/files/media_entity/documents/Dossier_virage_numerique_masante2022. pdf
6   Fee-per-procedure pricing is particularly called into question, as it leads to an increase in inadequate or unnecessary medical procedures. In order to strengthen the relevance of healthcare procedures, Olivier Véran proposes to extend remuneration based on public health objectives to other specialties than general medicine.
7   Olivier Véran's speech, *Ségur de la Santé* findings, July 21, 2020: https://solidarites-sante.gouv. fr/IMG/pdf/200721_-_discours_d_olivier_veran_-_conclusions_du_segur_de_la_sante.pdf
8   *Ibid*.

9   French Ministry of Economy, Finance, and Economic Recovery, « *Plan massif d'investissement en santé* » ("*Massive Investment Plan for Healthcare*"): https://www.economie.gouv.fr/files/files/ directions_services/plan-de-relance/plan-massif-investissement-sante.pdf
10   Of these 1.4 billion, 800 million will be dedicated to the integration of technical prerequisites for the modernisation, interoperability, reversibility and security of healthcare information systems (IS), 200 million will go towards strengthening digital teams and to support services within the operators concerned (in particular the *Agence du Numérique en Santé* (Digital Health Agency or ANS) and *l'Assurance Maladie* (French Public Healthcare Insurance System)), and 400 million to help the distribution of health data.
11   European Commission, Statement from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", COM (2020) 66 final, 19 February 2020, pp. 29-30: https://ec.europa.eu/ info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

services, which reveal information about his or her health status"[12]. This definition is broadly accepted by the World Health Organization (WHO), which defines health as "*a state of complete physical, mental and social well-being*". This report addresses health from this same viewpoint, and not as the absence or presence of a pathology. From this perspective, the term "citizen" is preferred to that of "patient" or "user". The scope of health data is thus very broad. Beyond so-called "medical" data, collected as part of the healthcare pathway by healthcare professionals, this concept encompasses, for example, data from connected objects (watches, bracelets, scales, etc.) which, depending on their usage, can be considered as health data. This data reveals information about a person's health status. In doing so, it touches upon individuals' most private information, making it particularly sensitive.

Because of this sensitivity, the sharing and use of health data raises important ethical questions. For example, is it acceptable to sell this data and, if so, under what conditions? Doesn't the use of this data, which is leading to the development of new "digital health" tools, run the risk of reinforcing inequalities in access to healthcare at a time when one in six people do not use the Internet in France?[13] ... If we intend to take the use of health data to the next level, be it as part of the healthcare pathway or for scientific research purposes, these questions deserve collective attention, and all stakeholders of the healthcare chain must be involved in this debate.

THE NEED TO QUESTION THE GOVERNANCE AND CONDITIONS FOR SHARING HEALTH DATA

These issues are at the heart of Renaissance Numérique's work, which has historically been involved in subjects related to the digital transformation of the healthcare system, the latter having a particularly citizen-oriented

dimension. Thus, in 2014, the think tank published a white paper[14] on the digital transformation of the sector, and drew up sixteen proposals to ensure the transition from a curative healthcare system to a preventive model. More than six years later, it is clear that this transition has not happened. As the 2017 presidential elections approached, Renaissance Numérique took the subject up once again, through a report devoted to e-health, describing proposals for developing a political ambition in this area[15]. This new publication was intended to provide food for thought on what would then become the digital component of the national "*Ma Santé 2022*" strategy.

As an extension of this work, in February 2020, Renaissance Numérique launched a working group dedicated to the governance and to the conditions for sharing health data. Because of their highly sensitive nature and inherent characteristics – they are extremely heterogeneous, often not interoperable, and sometimes carry tremendous value – health data are a difficult asset to govern. This difficulty is reinforced by the growing diversity of stakeholders involved in their production, collection, sharing, and reuse. Since the term "governance" can be subject to various interpretations, it is important to note that it is defined here as what "*determines who makes decisions, how they are made, and how decision-makers are held accountable for them with regards to the collection, use, sharing, or control of health data*"[16]. Apart from the topic regarding its governance, moving towards greater use of health data also raises many technical (interoperability, cybersecurity) and legal (protection of privacy and personal data) questions, linked to how it is shared.

For more than a year, a working group thus brought together a dozen members of the think tank – researchers, healthcare professionals, lawyers, healthcare and digital sector industry players –, who combined their expertise in order to come up with concrete recommendations on these

---

12   Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 / 46 / EC (hereinafter General Data Protection Regulation or "GDPR"), Article 4 (15).

13   Insee (French National Institute for Statistics and Economic Studies), « Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base » ("*One in six people do not use the Internet, more than one in three users lack basic digital skills*"), Insee Première No 1780, October 30, 2019: https://www.insee.fr/fr/statistiques/4241397

14   Renaissance Numérique (2014), « D'un système de santé curatif à un modèle préventif grâce aux outils numériques » ("*From a curative healthcare system to a preventive model, using digital tools*"), 119 pp. : https://www.renaissancenumerique.org/publications/d-un-systeme-de-sante-curatif-a-un-modele-preventif-grace-aux-outils-numeriques

15   Renaissance Numérique (2017), « 17 Experts / 36 propositions pour une ambition politique en matière de e-santé » ("*17 Experts / 36 Proposals for a political ambition in terms of eHealth*"), 44 pp. : https://www.renaissancenumerique.org/publications/17-experts-36-propositions-pour-une-ambition-politique-en-matiere-de-e-sante

16   Coutts, S., Gagnon-Turcotte, S., Sculthorp, M. (2021), « Les partenariats de données numériques » ("*Digital data partnerships*"), p. 33: https://downloads.ctfassets.net/e4wa7sgik5wa/6mV2HLHbhK-bU2sgtXSTMQX/e769babb86049cd1c5f73e8ba6aebc1a/Digital_Data_Partnerships_Report-FR.pdf

issues. In addition to this internal process, the think tank also interviewed stakeholders that were likely to provide feedback on the subject, by carrying out a series of interviews representative of the diversity within the health data value chain, including at European level. Nearly forty key stakeholders, representing the public and private sectors, as well as civil society, thus contributed to the ideas presented here[17]. This multidisciplinary approach now allows Renaissance Numérique to present possible courses of action directed at all stakeholders in the system, in order to make data a pillar of the healthcare system's transformation. In addition to providing food for thought, these interviews also reinforced the working group's belief that this exercise was necessary in order to promote the emergence of a "data culture" in the health sector. Some stakeholders still find it difficult to understand and deal with the subject of health data. However, the issues related to the conditions in which this data is shared, and its governance, raise questions that require their attention.

A NEW MOMENTUM FOR HEALTH DEMOCRACY?

The thinking presented here questions the general framework of "health democracy" in the French healthcare system. Sanctioned in Title III of the Law of 4 March 2002 on patients' rights and the quality of the healthcare system[18], this concept refers to the fact of associating "*all the stakeholders in the healthcare system in the development and implementation of health policy, in a spirit of dialogue and consultation*"[19]. This effort involves, in particular, the organisation of public debates, as well as the promotion of citizens' healthcare rights. If the various stakeholders in the healthcare chain manage to grasp it, health data could help breathe new life into this framework of health democracy that is struggling to take shape. So how can we redefine health democracy in the era of health data? Patients and patient associations, citizens, healthcare professionals, the central administration, the French Public Healthcare Insurance System (*Assurance Maladie*), regional healthcare agencies (ARS), health-

care establishments, local authorities, private complementary healthcare insurances (*mutuelles*), the healthcare industry, digital stakeholders, start-ups … all of them must be considered in the governance of the system, which requires taking into account the changing roles and responsibilities of each one of them throughout the healthcare chain. Patients are becoming users, contributors, evaluators, and even carers or experts, thanks to increasingly connected medical devices. The role of healthcare professionals and medico-social stakeholders is changing thanks to new clinical decision support tools, for instance in imaging or biology. On their side, digital stakeholders are increasingly investing in the healthcare field. In this constantly evolving environment, how can we ensure legible and effective governance of health data? This question raises two issues.

On the one hand, it is about better understanding[20] this data. Employed correctly, this data could, for example, be used to monitor the effectiveness of public health reforms[21], or even the effectiveness of the healthcare system itself (treatment waiting time, quality of care, etc.). This approach could make it possible not only to better integrate all the links in the healthcare chain, up to citizens, in the governance of the healthcare system, but also to help the system's intermediary bodies (e.g. patients' associations) in their actions. However, leveraging data for the governance of the healthcare system requires that all stakeholders in the chain be empowered to understand "digital health" challenges; which is not currently the case. Furthermore, the interviews conducted as part of this study showed that the "new entrants" who enter the health field, coming from the digital world, and often embodied by start-ups, are not always aware of the issues that underpin this sector. Ensuring that innovation meets specific needs identified within the healthcare system, however, is essential.

On the other hand, its governance needs to be clarified. Due to the great heterogeneity that characterises health data and the multitude of

---

17   For the full list of people who were interviewed, see the "Acknowledgments" section of this report.
18   Law n° 2002-303 of March 4, 2002 relating to the rights of patients and the quality of the healthcare system. Accessible online: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000227015/
19   Regional Health Agency, « Qu'est-ce que la démocratie sanitaire ? » ("*What is health democracy?*"), October 3, 2018: https://www.ars.sante.fr/quest-ce-que-la-democratie-sanitaire-10#:~:text=Faire%20vivre%20la%20d%C3%A9mocratie%20sanitaire,individuels%20et%20collectifs%20des%20usagers

20   In the sense of understanding it, being able to think about it
21   As recalled in the report « Pour une politique publique de la donnée » ("*For a public policy on data*"), prepared as part of the parliamentary mission led by MP Éric Bothorel and made public in December 2020, "*data is a way of correctly assessing our public policies. On the one hand, using data is only about increasing reliability and enabling good old management control in real time; and it also means finally giving oneself the means with which to monitor the execution of public expenditure.*", p. 7: https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020_0.pdf

stakeholders involved, its governance is relatively unclear. However, only a clear governance of health data can help it be shared in the correct manner, i.e. a secure and smooth sharing, which respects citizens' fundamental rights, and is not sabotaged by data hoarding, which some stakeholders in the healthcare chain could be tempted by.

Ultimately, taking a step forward in the use of health data, while adhering to the principle of health democracy, requires not only acculturation efforts, but also political, technical, and legal arbitrations within a clarified governance framework.

Finally, it should be noted that although the think tank's reflections were initiated before the peak of the health crisis, the latter has reshuffled the cards in certain respects. Forced changes, such as the massive use of teleconsultations and their full reimbursement until the end of the health status emergency[22], as well as the extension of the specifications for remote monitoring, or the implementation of the SI-DEP[23] (screening information system) and Contact-COVID[24] platforms, were therefore not anticipated. The crisis has also led to the accelerated deployment of certain digital health tools, such as the national health data platform (Health Data Hub), launched ahead of schedule to facilitate the processing of data related to the virus[25]. Finally, political support, as well as the technological choices implemented to develop these tools, in particular the Health Data Hub and the former StopCovid[26] contact case tracing application, have strongly

polarised the debates around issues related to health data. As far as possible, this report takes into account the most recent developments in this regard. Given that it was propelled to centre stage throughout the past eighteen months, understanding the many issues that health data raises, as well as the opportunities that its exploitation represents for our healthcare system, appears, all the more so necessary.

---

22 *Assurance Maladie*, « Covid-19 : tout savoir sur la téléconsultation et les actes à distance », ("*Covid-19: all you need to know about teleconsultation and remote healthcare procedures*"), November 9, 2020: https://www.ameli.fr/paris/assure/actualites/covid-19-tout-savoir-sur-la-teleconsultation-et-les-actes-distance

23 SI-DEP is the secure platform where Covid-19 testing laboratories' results are systematically recorded.

24 As indicated on the website of the French Ministry of Solidarity and Health, Contact-COVID is "*a digital tool used by all healthcare professionals (doctors, pharmacists, biologists in COVID screening laboratories, and professionals authorised by the CNAM (French Public Healthcare Insurance Funds), SpF (French National Public Health Agency) and ARS), which helps manage Covid-19 cases. People that have been in contact with a Covid-19 case are identified as quickly as possible. It enables verification that everyone has been called, informed, tested, and supported.*"

25 This accelerated implementation was ordered by the decree of April 21, 2020 complementing the decree of March 23, 2020 prescribing the healthcare system's organisational and operating measures needed to deal with theCcovid-19 epidemic within the context of the public health emergency: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041812657/. In particular, it enabled the pairing of the first health data on the Covid-19 epidemic.

26 The first version of the application, called StopCovid (which was a simple contact case tracing application), evolved in October 2020 to a new, enhanced, and more interactive version: TousAntiCovid.

PART 1

DIGITAL DATA: A GAME CHANGER FOR THE GOVERNANCE OF THE HEALTHCARE SYSTEM?
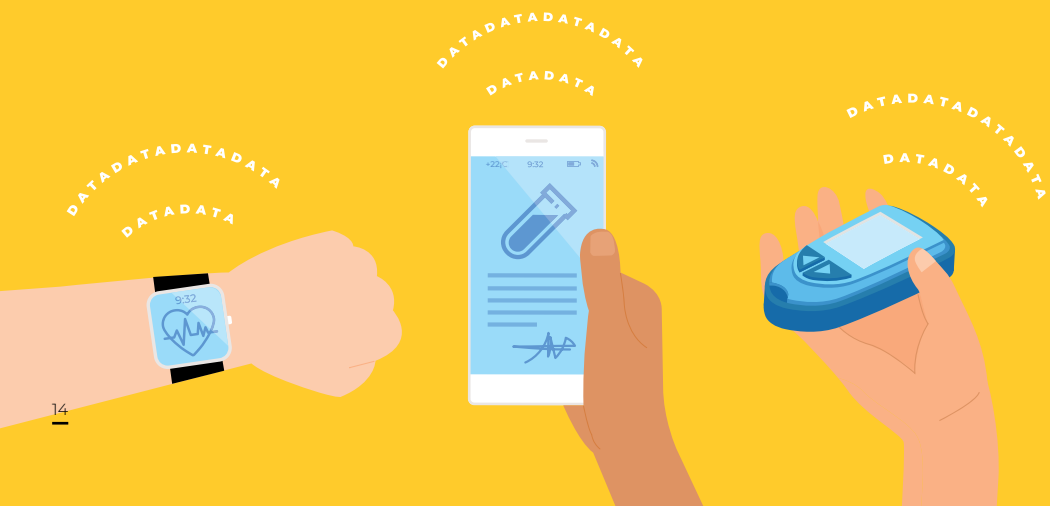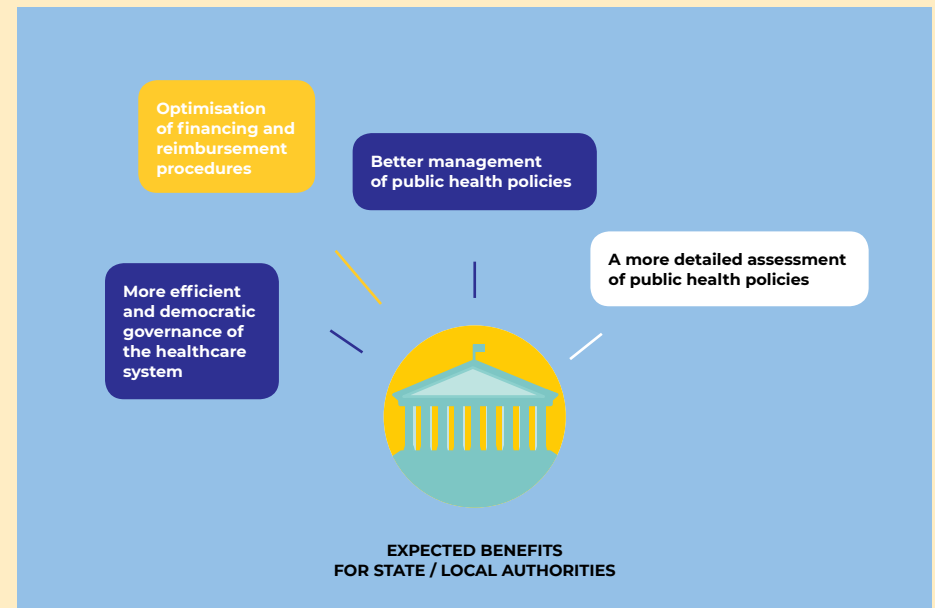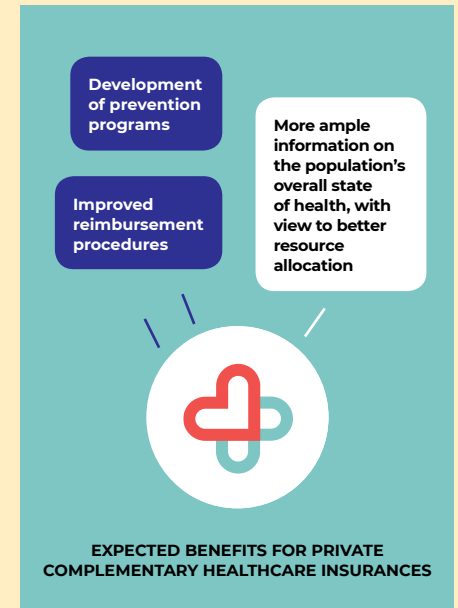
While the accelerated development of digital technologies has given data in the healthcare sector a new acuity, health is historically a data rich field. This is particularly the case in France, where national databases containing data from millions of individuals were set up in the 1990s. For isntance, the SNIIRAM (National Inter-Regime Information System for the French Public Healthcare Insurance System), created by the Social Security Financing Act in 1999, has four main goals: improve the quality of healthcare, contribute to better management of the French Public Healthcare Insurance System and health policies, and provide healthcare providers with information relevant to their work[27].

The expected benefits of sharing and exploiting health data are well known, and are the subject of a relative consensus, as demonstrated by the series of interviews conducted as part of this report's preparation. These include:

- improving healthcare pathways and their coordination: providing the right treatment at the right time, improving the relevance of treatments, streamlining healthcare pathways;

- pushing scientific research forward: improving the effectiveness of drugs and medical devices, reducing unwanted side effects, developing algorithms to aid diagnosis or decision-making;

- steering the healthcare system "through data": developing and revising public policies based on data, using data for the logistical organisation of healthcare establishments, and assessing the quality and relevance of healthcare;

- pushing preventive medicine forward: instead of purely curative medicine, moving towards medicine that proactively reaches out to citizens (prevention of risky behaviours, promoting screening for certain pathologies and virtuous behaviours, etc.).

---

27 Social Security Code, article L161-28-1.

FIGURE 1 - THE EXPECTED BENEFITS OF USING DIGITAL HEALTH DATA

EXPECTED BENEFITS FOR CITIZENS / PATIENTS

- Contribution to the evaluation of healthcare quality
- More personalised follow-up
- Improved prevention of pathologies
- Greater autonomy in the monitoring of certain pathologies

EXPECTED BENEFITS FOR PATIENT ASSOCIATIONS

- Improved information to be leveraged with public authorities
- Improved knowledge of patients and their pathologies in order to support them

EXPECTED BENEFITS FOR RESEARCHERS

- Enhancement of the data available for medical research
- Access to real-world data
- Access to up-to-date data

EXPECTED BENEFITS FOR PRIVATE COMPLEMENTARY HEALTHCARE INSURANCES

- Development of prevention programs
- Improved reimbursement procedures
- More ample information on the population's overall state of health, with view to better resource allocation

EXPECTED BENEFITS FOR HEALTHCARE PROFESSIONALS / INSTITUTIONS

- Better knowledge of patient profiles and behaviours
- Improved monitoring of patients and their healthcare pathways (inter-professional)
- Optimised decision making thanks to diagnostic / decision support tools

EXPECTED BENEFITS FOR THE HEALTHCARE INDUSTRY

- Development of digital therapies
- Improved drugs and medical device efficiency
- Monitoring of therapeutic efficacy in real life conditions

EXPECTED BENEFITS FOR STATE / LOCAL AUTHORITIES

- Optimisation of financing and reimbursement procedures
- Better management of public health policies
- More efficient and democratic governance of the healthcare system
- A more detailed assessment of public health policies

While the usefulness of digital data in the healthcare sector is irrefutable, increasing its use within healthcare pathways or for research purposes still raises many economic, political, legal, and technical challenges. Addressing these questions requires a good understanding of this complex subject which is health data. What exactly do we mean by "health data"? Who produces it and who owns it? What legal framework regulates its sharing and usage?

FROM DATA HETEROGENEITY IN THE HEALTHCARE VALUE CHAIN ...

Although we had to wait until 2018 for the GDPR to come into effect in order to have a legal definition, applicable in French law, of personal data concerning health, this doesn't mean that such data didn't exist before and wasn't subject to strictly regulated processing.

A BROAD LEGAL DEFINITION OF HEALTH DATA, WHICH MAKES IT AN EXTREMELY HETEROGENEOUS LANDSCAPE

PERSONAL DATA CONCERNING HEALTH: A BROAD DEFINITION, ENSHRINED IN THE GDPR

According to article 4 of the GDPR, "data concerning health" is "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*". This definition is very broad and is not limited to medical data only, as defined in Article L1111-7 of the Public Health Code[28]. It includes, as specified in recital 35 of the GDPR:

· "*information about the natural person collected in the course of the registration for, or the provision of, health care services [...] to that natural*

person : a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;

· *information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;*

· *and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."*

Given the very broad definition of the GDPR, the classification of information as "personal data concerning health", within the meaning of the regulation, must be analysed on a case-by-case basis. Data can be health data by nature, by cross-referencing or by purpose. Health data "by nature" is data that is inherently and evidently health data. For example, the results of a biological examination, consultation reports, or the list of treatments followed by a person constitute health data "by nature". Then there is data which, taken independently, doesn't constitute health data, but which, when cross-referenced with other data, can give an indication of a person's health status. This is known as "cross-referenced" health data. A person's weight, by itself, is not health data. If it is cross-referenced with the person's height, however, it is possible to calculate the person's body mass index (BMI), which makes it possible to deduce information on the person's health status. Finally, there is health data "by purpose", which becomes health data due to its use for medical purposes. If a person fills in a daily diary with the list of foods he or she eats, the information collected in this diary does not constitute health data. If, on the other hand, this person sends their logbook to a healthcare professional as part of their healthcare pathway, then the information it contains becomes health data. Health data therefore forms an extremely heterogeneous category of data, the legal nature of which varies according to whether they are produced within the framework of the healthcare pathway or outside of it, but also according to the intention of the person processing the data.

28   See Table 1 – General typology of health data.

This great heterogeneity results not only in a certain difficulty in fully grasping health data, in understanding what it is exactly, and what it can be used for, but also a significant degree of complexity in terms of governance. Due to the wide definition of health data highlighted in the GDPR, there are a vast number of stakeholders involved in its production, collection, sharing, and use: holders, users, intermediaries, regulatory authorities and bodies, beneficiaries, etc. Familiarising ourselves with health data therefore requires familiarising ourselves with these stakeholders, and the interconnected ecosystem that they constitute.

TABLE 1 - GENERAL TYPOLOGY OF HEALTH DATA

It is important to note that this typology is only one of the several possible typologies of health data. If the choice of categorisation made here is that of the source (or "producer") of the data, the latter could very well be categorised according to its purpose, legal status, function, format, or degree of openness (ranging from private data to open access data). The different categories of data mentioned below are also porous and non-exclusive: some data can be found in more than one category in the table. According to the French National Health Authority (HAS), for example, real-world data includes medico-administrative data. Likewise, this data can constitute scientific data. Finally, neither the examples nor the lists of data "producers" / "collectors" mentioned in the table are exhaustive.

Category	Definition	Examples	Produced / Collected by...
Medical data	A patient's medical data includes "*all the information held concerning the patient's health, for whatever reason, by healthcare professionals, healthcare establishments, healthcare centres, the Army Healthcare Service, or by the National Institution for Invalids, which are formalised or have been the subject of written communication between healthcare professionals, [...] with the exception of information indicating that it was collected from third parties not involved in the healthcare treatment plan or concerning such a third party.*" *Source: article L1111-7 of the Public Health Code*	• Examination results • Medical consultation, intervention, exploration, or hospitalisation reports • Implemented treatment protocols and prescriptions • Monitoring sheets • Correspondence between healthcare professionals	• Healthcare and medico-social sector professionals • Healthcare and medico-social sector establishments • Healthcare centres • The Army Healthcare Service • The National Institution for Invalids

Category	Definition	Examples	Produced / Collected by...
Medico-administrative data	*"Administrative data [...] contained in medical documents relating to a patient's treatment."* *G 29, Letter on mHealth, Appendix, February 5, 2015, p. 2 ; G 29, Working document on the processing of personal data concerning health included in electronic medical records (EMRs), February 15, 2007, p. 8*	• Information such as the social security number or hospital admission date (or any other traceability data from a healthcare establishment linked to the monitoring of patients) • Data contained in the Pharmaceutical Record (medication dispensed during of the last four months) and the National Health Data System (nomenclature and date of healthcare procedures provided, invoices, etc.) • Product data (version, composition, characteristics, usage constraints, etc.)	• Healthcare and medico-social sector professionals, establishments, and centres, the Army Healthcare Service, the National Institution for Invalids • Pharmacies • French Public Healthcare Insurance System • Private complementary healthcare insurances
Statistical data	Statistical data is codified, fixed, and transmissible information. It can be quantitative as well as qualitative.	• Aggregated data (epidemiology, etc.)	• Healthcare and medico-social sector professionals, establishments, and centres, the Army Healthcare Service, the National Institution for Invalids • The central administration (e.g. Ministry of Solidarity and Health, Ministry of Higher Education and Research, French National Public Health Agency) • French Public Healthcare Insurance System • Private complementary healthcare insurances • ARS

Category	Definition	Examples	Produced / Collected by...
Real-world data	*"Data that doesn't interfere with usual methods of patient care and that is not collected in an experimental setting (e.g., randomised controlled trials, RCTs), but which is generated during routine patient care, and therefore a priori reflect current practice. This type of data can come from multiple sources: it can be extracted from computerised patient records, or be an information by-product used for healthcare reimbursement; it can be collected in a specific way, for example within pharmacovigilance procedures, or to constitute registers or cohorts, or more occasionally within the framework of ad hoc studies; it can also come from the web, social networks, connected objects, etc. "* *Source : Bégaud, B., Polton, D., and von Lennep, F., « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé : L'exemple du médicament » ("Real-world data, a major issue for the quality of healthcare and the regulation of the healthcare system : The example of medication"), May 2017.*	• Blood pressure • Heart rate • Blood sugar • Weight • Information on mental and psychological state, on the quality of sleep, on physical activity (e.g. number of steps), on the menstrual cycle, the act of performing several searches related to health topics in a search engine	**In cases where the data is collected by medical devices (MD):** • Healthcare and medico-social sector professionals • Citizens • Industry players • Patient associations and federations **In cases where the data is collected by connected objects, applications (non-MD) or during a person's online activities:** • Healthcare and medico-social sector professionals • Citizens themselves • Developers of connected applications / objects and other digital stakeholders
Scientific data	Data from medical research and scientific experiments.	• Registers and cohorts • Results of epidemiological surveys • Clinical studies	• Medical researchers • Public authorities • Industry players • Patient associations and federations
Contributory data	Contributory data is data that is voluntarily shared by citizens, in a bottom-up logic. *Source : Renaissance Numérique & Syntec Numérique (2019), « Tous acteurs des données. Appréhender les données pour mieux les valoriser » ("We're all data stakeholders. Understanding data to make better use of it"), p.85*	• Answers to questionnaires • Data shared in the context of clinical studies / research programs (e.g. anonymised epidemiological data voluntarily submitted by certain individuals in the context of the fight against Covid-19)	• Citizens • Patient associations and federations • Researchers • Industry players • Public authorities • Private complementary healthcare insurances

Although healthcare is a historically data rich sector, its digitalisation has multiplied the quantity of data produced and has strengthened the diversity of its sources.

Not only do healthcare stakeholders, like pharmaceutical laboratories, offer their own connected devices (blood glucose self-monitoring systems, pacemakers), but new stakeholders (start-ups, large digital groups) are also increasingly investing in the health sector. In March 2019, Apple introduced a new version of its connected watch into the French market, which allows any user to perform an electrocardiogram[29], an examination of cardiac activity usually performed by cardiologists. Google in turn, through its X subsidiary (formerly Google X Lab), has embarked on the development of smart contact lenses, which can detect the level of glucose in tears, in order to monitor diabetes. The Mountain View firm has also launched a large study in which genetic data and biochemical characteristics of healthy volunteers are collected, in order to identify the traits that are lacking in individuals with pathologies[30]. Moreover, in France, no less than 685 start-ups invest in the healthtech[31] field, and the potential of the e-health market in the country is estimated at between 16 and 22 billion euros per year[32]. In addition to the data collected or generated via digital tools, there is also data produced as part of healthcare pathways (so-called "medical" data), such as, for example, examination results, medical consultation, intervention, exploration, or hospitalisation reports, implemented treatment protocols and prescriptions, monitoring sheets or even correspondence between healthcare professionals. As specified in Table 1, health data can also be medico-administrative, statistical, real-world, scientific or even contributory. It can just as well be collected by a healthcare or medico-social sector professional as part of a healthcare pathway (for example, during a medical consultation at a practice or at a hospital) or by a patient association, through a questionnaire, or by an industry player via a connected medical device (CMD). Depending on the context in which it is used, it can be nominative, aggregated, pseudonymised, anonymised, etc. The forms in which it exists are also extremely varied: text (e.g. hospital re-

port), numbers (e.g. glucose level in interstitial fluid), images (e.g. ankle x-ray), sounds, videos. As illustrated by the infographic hereinafter, it is produced, collected, and used in a wide variety of contexts.

THE SNDS: A DATABASE THAT IS UNIQUE IN THE WORLD

The National Health Data System (SNDS), a database managed by the French Public Healthcare Insurance System, was created by the Law on the modernisation of the healthcare system, on 26 January 2016. More precisely, it is a combination of several databases:

· the National Inter-Regime Information System of the French Public Healthcare Insurance System (SNIIRAM): a data repository grouping together information from reimbursements made by all French public healthcare insurance schemes for healthcare delivered by private practitioners;

· data from hospitals and other healthcare establishments, obtained from the PMSI (Program for the medicalisation of information systems);

· Inserm's (French National Institute for Health and Medical Research) CépiDC, (Centre for Epidemiology on Medical Causes of Death) database, which collects data on medical causes of death for the whole population.

The SNDS thus constitutes a detailed database on patient pathways and the organisation of the healthcare system on French territory.

DATA THAT IS OFTEN COMPARTMENTALISED AND NOT VERY INTEROPERABLE

Because of this great diversity, both in its nature, its source of production, or even its purpose, health data is scattered within a multitude of databases, which don't necessarily communicate with each other, and are administered
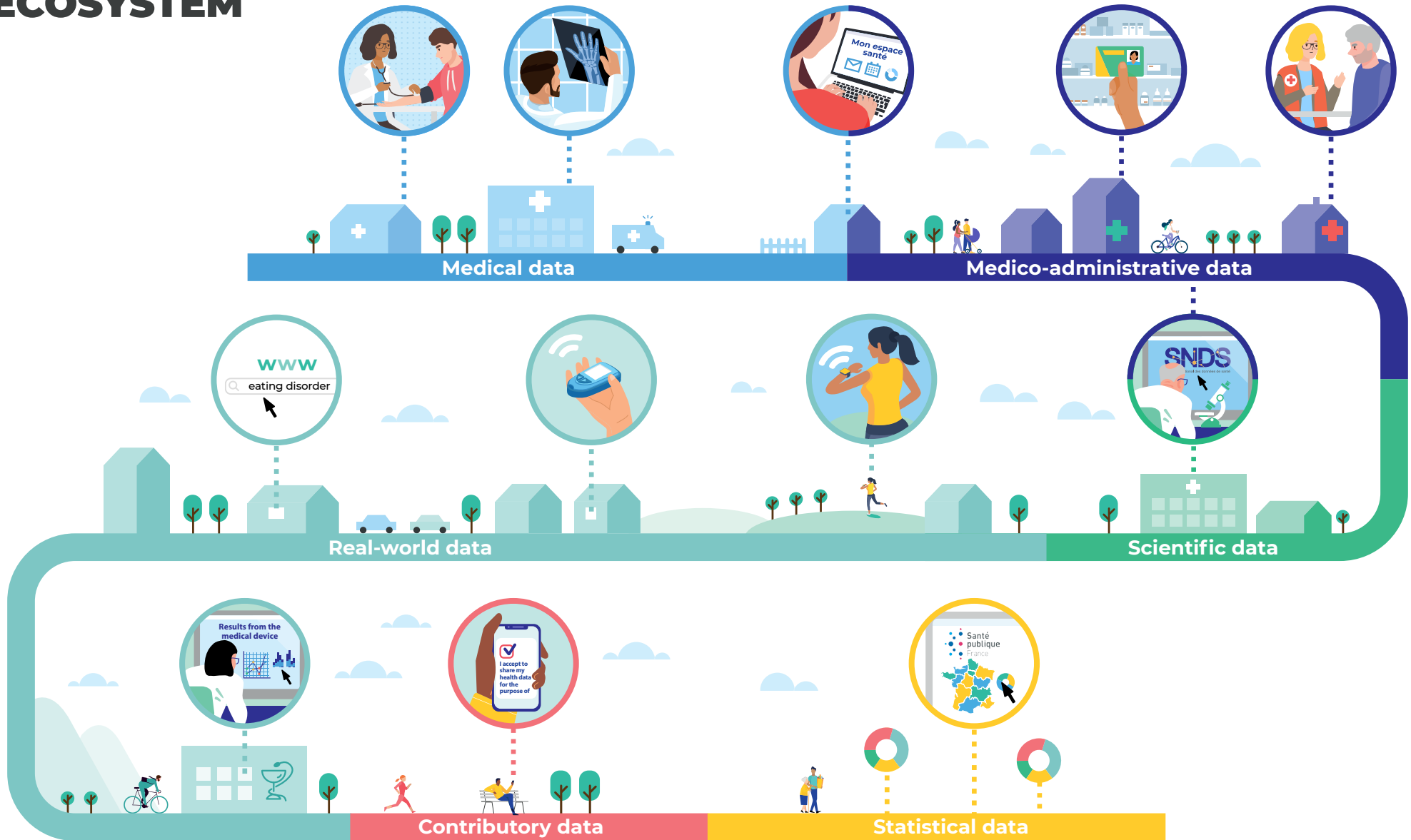
---

29 Apple support, "Take an ECG with the ECG app on Apple Watch": https://support.apple.com/fr-fr/HT208955

30 University of Illinois Chicago, "How Google's 'Moonshot' Initiatives Could Change Healthcare": https://healthinformatics.uic.edu/blog/how-googles-moonshot-initiatives-could-change-health-care/

31 This figure is taken from the dynamic database Motherbase (https://www.motherbase.ai/), accessed on 4 March 2021.

32 Institut Montaigne (2020), « E-Santé: Augmentons la dose ! », ("E-health: let's up the dose!"), 220 pp.: https://www.institutmontaigne.org/publications/e-sante-augmentons-la-dose

HEALTH DATA: A HETEROGENEOUS ECOSYSTEM

Medical data

Medico-administrative data

Real-world data

Scientific data

Contributory data

Statistical data

by different stakeholders in the healthcare chain. Among the latter, France has a national database that is unique in Europe, or even in the world, the National Health Data System (SNDS), which gathers pseudonymised health data collected by several public organisations. This database is managed by the French Public Healthcare Insurance System.

The SNDS is an exception. Most of the existing health databases in France are managed at a very local level, for example by medical practices and healthcare establishments (hospitals, nursing homes), which hold all the information relating to the monitoring of their patients. There are also databases at intermediate levels, such as those held by patient associations and communities, research centres such as the French National Institute for Health and Medical Research (*Inserm*) or even private sector stakeholders. All of the health data available in the country thus often follows different procedures and reference systems for collection and reporting. This results in data of extremely varied quality, reference systems, and formats, which makes it difficult to match them[33]. However, it is precisely on the possibility of cross-referencing data from different databases, that its value and many improvements (or even innovations) within health are based, which can make it possible, for example, to diagnose pathologies more quickly or to develop more effective treatments and medical devices. In addition to the fact that this data is difficult to match, it can also sometimes remain "in silos", thus not allowing its full potential to be exploited, either because the stakeholders don't have the necessary resources for its exploitation, or because its exploitation is not considered relevant. For example, if medical researchers in a hospital wish to conduct a study on a rare disease, it is very likely that the data available in their data repository alone will not be sufficient to reach meaningful conclusions.

THE VALUE OF DATA

Data taken in isolation is of little value. Primary data must be aggregated and processed so that sufficient value can be derived from it. Most often,

data is only usable when it is contextualised, used in combination with its accompanying metadata[34].

Moreover, the mere fact of collecting a large amount of data does not guarantee value creation. Value creation is the result of complex mechanisms for collecting, storing and processing data to produce value-added goods or services.

A prerequisite for extracting value from data is the production of quality data. Much data is in fact made inaccessible or unusable due to the poor quality of its production. Most data therefore needs to be reprocessed before it can be used. The purpose of this processing is to make the data reliable, consistent, accessible to users, and compliant with security and confidentiality standards.

Once the quality of the databases has been ensured, their processing by analysis methods is an essential step in creating value. For example, algorithmic processing allows the creation of high value-added services, which continuously learn from usage data. The value of data is therefore not only related to its abundance and quality. Its processing appears to be just as essential to the creation of efficient goods and services.

At the very end of the chain, the last step in the process of creating value from data is its restitution in the form of services to the user.

Source: Renaissance Numérique & Syntec Numérique (2019), « Tous acteurs des données. Appréhender les données pour mieux les valoriser » ("We're all data stakeholders. Understanding data to make better use of it"), 97 pp.

MOVING TOWARDS HEALTH DATA PLATFORMISATION

Partly for these reasons, we've been witnessing, for several years now, a trend where certain health databases group together within digital platforms.

---

33 Pairing of separate datasets, using the same type of information (e.g. grouping of patient data from different sources).

34 Metadata refers to all the data used to describe another piece of data, whether it be the name, size, or creation date of a file, the title of a song or an album associated to an audio file, or the description of a photograph.

The objective of these initiatives: promote secure, simplified, and accelerated access to health data, leverage the power of internal research (particularly in hospitals and research centres), pool complementary skills (medical researchers, data scientists, statisticians) and have a technological platform that facilitates data processing and offers increased calculation and storage capacities. It is precisely with this in mind, that the *Ouest Data Hub* (West Data Hub) was launched in December 2020 (see Table 2). It is the first hospital data platform in Europe, which ultimately aims to bring together data from six hospitals[35] in order to support medical research. HUGO, the *Grand Ouest* (geographical area of France that encompasses Brittany and Pays de la Loire) Teaching Hospitals grouping, which manages this platform, is also working with other teaching hospital networks to develop this original "interregional hub" model. At a national level, this momentum is embodied by the launch, also in 2020, of the Health Data Hub (see box pp. 42-43). As shown in Table 2, these different health data platforms each have their own rationales and aim to meet different objectives (research, organisational issues, healthcare, coordination, etc.). Specialised private platforms, for example, respond to a healthcare offer, to a health need. They therefore have a different vocation than platforms bringing together databases intended for research, such as the Health Data Hub, or those managed by *Inserm*.

TABLE 2 - THE PLATFORMISATION OF HEALTH DATA

National public platforms	**HDH** HEALTH DATA HUB	Accessible to public and private stakeholders for research, study, or assessment purposes
Inter-regional and regional public platforms	**OUEST DATA HUB**	Accessible only to researchers of the *Grand Ouest* Teaching Hospitals grouping (HUGO)
	Regional health data repositories (HDR) project in the *Grand Est* region	Accessible to healthcare professionals, researchers, hospital administrators, and possibly industry players
Cross-border / European public platforms	**The future European health data space**	Accessible to all healthcare professionals in the Member States
Specialised private platforms	**LibreView**	Accessible to diabetic patients with FreeStyleLibre continuous glucose monitors and healthcare professionals who monitor them
	eCareCoordinator[36]	Accessible to clinicians for daily monitoring of their patients (gathers data available in real time, such as vital parameters, blood pressure, and patient weight)

Among the different scales of health data sharing via digital platforms, the European level should not be forgotten. In its data strategy published in February 2020[37], the European Commission has, in fact, laid the foundations for a "common European health data space". The objective: strengthen and expand the use and reuse of health data at an EU level. The Health Data Hub is also France's competent authority, as part of the joint action launched by the

35   Anger, Brest, Nantes, Rennes and Tour teaching hospitals, and the Orléans regional hospital.

36   See: https://www.philips.fr/healthcare/innovation/a-propos-de-healthsuite/applications
37   European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", COM (2020) 66 final, 19 February 2020, 35 pp.

European Commission, to define the contours of this common data space[38]. A legislative proposal in this respect is expected in the fourth quarter of 2021. Finally, as highlighted in Table 2, certain health data is made available within platforms developed by private stakeholders. This is the case, for example, of data related to the monitoring of diabetic patients equipped with the "FreeStyle Libre" type continuous glucose monitoring devices, which are accessible to patients and their doctors via the LibreView platform. Although they have different rationales and objectives, the various existing health data platforms don't necessarily operate in silos with respect to each other. They are part of an ecosystem which is increasingly coordinated. Certain platforms developed by stakeholders in the digital sector may, in particular, be the subject of partnerships with industry players in the healthcare sector, or even be included in the catalogue of services referenced by the public authorities via the *Espace Numérique de Santé* (Digital Health Space, ENS) called "*Mon Espace Santé*" ("My Health Space"), the personal space where French citizens will be able to access services and manage their health data as from January 1, 2022 (see box p. 70). While initiatives to collect and make health data available via digital platforms are multiplying at various levels, the question of how to link them together becomes increasingly important, which makes readability and governance of this data all the more complex.

> *"We're trying to implement an intermediate stage of governance, within Inserm, particularly for cohorts. Teaching hospitals are doing the same with data repositories. Then, it will be necessary to organise the dialogue between the Health Data Hub and these intermediary governance structures"*
>
> **Franck Lethimonnier,**
> **DIRECTOR OF THE "TECHNOLOGIES FOR HEALTH" THEMATIC INSTITUTE AT** *INSERM*

The relative compartmentalisation of health data, which hinders its use, is a major factor in this current "platformisation" dynamic. It also explains the efforts

recently made by the government as part of the national "*Ma Santé 2022*" strategy and the *France Relance* recovery plan. The latter aim in particular to modernise the fleet of IT equipment (software, information systems) used by healthcare professionals and institutions, and to encourage the adoption of baseline interoperability and security reference systems. The objective: decompartmentalise health data in order to encourage its use. However, although major projects have been launched, the governance of health data remains unclear for the time being.

...TO AN UNCLEAR GOVERNANCE OF THIS DATA

A SOMEWHAT VAGUE STEERING OF PUBLIC POLICY ON HEALTH DATA

Any questions relating to the steering of public policy on health data must necessarily be placed within a broader framework, which goes beyond this data alone: that of "digital health" and the issues that underlie it and, more generally, that of the digital transformation of public action. In France, several entities, including the Ministry of Solidarity and Health, the Secretary of State for Digital Affairs, the Digital Health Agency (ANS), the French Public Healthcare Insurance System fund (CNAMTS) and even the National Public Health Agency, share the governance of the digital health policy. Within the Ministry of Health itself, several departments are heavily involved, in particular the Ministerial Delegation for Digital Health (DNS), which is responsible for implementing the strategic roadmap for digital health, the General Directorate for Healthcare Provision (DGOS), which is responsible, among other things, for the Telemedicine Experiments for the Improvement of Healthcare Pathways (ETAPES)[39] programme, and the Directorate for Research, Studies, Evaluation and Statistics (DREES)[40]. Understanding the steering of public policy on health data requires understanding the role of each of these

---

38   For further information, see: https://www.health-data-hub.fr/actualites/kick-officiel-de-laction-conjointe-espace-europeen-des-donnees-de-sante

39   A national programme which, since 2018, has been encouraging and financially supporting the deployment of remote monitoring projects throughout France, through experiments on five pathologies: heart failure, renal failure, respiratory failure, diabetes and implantable cardiac prostheses.

40   Fabrice Lenglart, director of the DREES, was also recently appointed data administrator for the Ministry of Solidarity and Health.

entities in the governance of digital health, which is not always easy, even for insiders. In its report "Trust, innovation, solidarity: For a French vision of digital health"[41] published in June 2020, the National Digital Council (*Conseil National du Numérique* or CNNum) mentioned the example of the development of the *Espace numérique de santé* (ENS). While the strategic steering of this project has been entrusted to the Ministerial Delegation for Digital Health, the French Public Healthcare Insurance System fund is responsible for its operational management, while the Digital Health Agency defines the interoperability framework, and the DGOS is involved in the financial levers[42]. Although this shared governance can be understandable (each stakeholder does indeed exercise a skill for which they have recognised expertise), this multiplicity of stakeholders can contribute to the lack of clarity and agility of decision-making chains and lead to a certain slowness of execution, even deadlock situations.

Indeed, not everyone has necessarily the same perception and use of health data. As observed in the fight against the Covid-19 epidemic, there were some instances, for example, where even when analysing the same dataset, the National Public Health Agency and DREES didn't get the same figures for certain variables. Why? The data in question was not adjusted (or pre-processed) in the same way by the two entities who, in the end, weren't speaking exactly the same language.

This point appears all the more critical as it would seem that some of the organisations involved in the steering of digital health do not have all the necessary resources required to implement the projects entrusted to them. During the interviews carried out for this report, it was pointed out that the Ministerial Delegation for Digital Health is not sufficiently staffed in view of the roadmap that had been set.

This relative shortcoming is also due to the fact that we are at the border between two worlds: that of health and that of digital technologies. Governing (in the political sense of the term) digital health requires these two worlds to coordinate themselves in order to establish a clear and coherent strategy. During the discussions that the think tank was able to have with the stakeholders of the healthcare system, several of them condemned a problem of

political support, in particular (but not only) around the Health Data Hub, which according to them should be driven by the Minister of Solidarity and Health. There are also readability issues for citizens, and their trust in public authorities. These points are all the more critical when it comes to public healthcare. If, in matters as important as the Health Data Hub or Covid-19 case-tracking applications, French citizens witness a disorderly debate, this won't contribute to them feeling confident about these systems, or help their understanding of these issues. As such, it is regrettable that the debates around the StopCovid application have focused almost exclusively on issues of data security and digital sovereignty (which the vast majority of citizens are not familiar with), leaving aside health-related issues. The crisis has revealed the outstanding difficulties in debating both technical and public health issues collectively, with citizens being largely excluded from these debates. In order to get all the stakeholders involved in the digital transformation of the healthcare sector, a clearer steering of public policy on health data is needed.

AN ECOSYSTEM THAT IS DIFFICULT TO GRASP IN ITS ENTIRETY

The sharing and use of data in the health sector offers many opportunities for economic and social development, benefitting citizens and healthcare professionals, as well as companies or the State. However, understanding the health data ecosystem in its entirety is not easy.

HEALTH DATA, MEDICAL DATA, "WELL-BEING" DATA: POROUS CONCEPTS

For several years now, start-ups and large digital companies have invested heavily in the healthcare field. Thus, the health data ecosystem brings together stakeholders in the healthcare chain, such as pharmaceutical companies, private complementary healthcare insurances, and public authorities, but also stakeholders in the digital sector. Inevitably, this arrival of new entrants has led to a complexification of the health data ecosystem, in which the boundaries between concepts such as "medical data" and "well-being data" are relatively blurred. While not all connected objects and digital applications used within healthcare pathways are necessarily considered to be connected devices collecting medical data (medical devices or MD), some

---

41   National Digital Council (2020), « Confiance, innovation, solidarité : pour une vision française du numérique en santé », ("*Trust, innovation, solidarity: For a French vision of digital health*"), 114 pp.: https://cnnumerique.fr/files/uploads/2020/ra-sante-cnnum-web.pdf

42   *Ibid.*, p. 37.

have been certified by the American Food and Drug Administration (FDA)[43] and are on the way to becoming MDs. What is more, the qualification of data as "medical data" or "well-being data" may change during the life of said data, as "well-being" data may well become medical data.

While many of these new stakeholders are developing solutions based on algorithmic data processing, some manufacturers of connected objects market products with specific functionalities that place them somewhere between connected medical devices (CMD) and connected objects (e.g. Fitbit bracelets, Apple's iWatch). However, the regulatory requirements with regards to the marketing of these products are not the same. In this case, those placing medical devices (MD) on the market are more stringent. Companies that develop CMDs are in fact required to comply with a relatively strict legal framework (CE marking, development of clinical studies, validation by health status authorities prior to marketing). These obligations don't apply to connected objects, which aren't considered to be medical devices (even though they allow certain aspects of a person's state of health status to be analysed). They are therefore not reimbursed by the social security system either. They are, however, subject to other existing regulations, for example regarding the protection of personal data (e.g. GDPR).

Indeed, the line between the nature of the data collected by CMDs (medical data) and that of data from connected objects ("well-being" or "good health" data) is blurred. This inevitably raises questions about the legal framework surrounding these technologies, especially in terms of liability. The use of connected objects, if not regulated from a health point of view, could, for example, lead citizens to make decisions about their health based on the measurements sent to them by these devices. Since they measure aspects of a person's state of health, shouldn't these tools be subject to more stringent regulations when they're put on the market? At the very least, enhanced scrutiny on the impact of these tools would be beneficial. Thoughts are starting to emerge on this subject. During our conversations with stakeholders, some have, for example, proposed the introduction of a sort of reference framework for these devices, which at least guarantees their reliability, a lighter version of the standards imposed on manufacturers of connected medical devices (ISO standards, interoperability and safety standards, etc.). Others, on the contrary, are against this idea and believe that the market will automatically select the most reliable solutions. Logic would suggest that it depends on the intention of the manufacturers of these tools. If their aim is to incorporate their solutions into healthcare pathways entitling them to be reimbursed by public funds (i.e. via the public healthcare insurance system), then the legislator must be able to set the conditions for this reimbursement, and guidelines would seem advisable. If, on the other hand, they intend to limit the marketing of their tools to the private market, then it would be up to insurers (e.g. private complementary healthcare insurances) to decide. In any case, it is crucial that, when marketing their innovations in the healthcare sector, digital sector stakeholders take these aspects into account.

Questions also arise regarding the possible use of this data, collected by a whole series of connected objects (bracelets, watches, scales, etc.) benefitting the healthcare system, for example, as part of healthcare pathways, or of medical research. Certain so-called "well-being" data (quality of sleep, physical activity, calories consumed, etc.) could be used by healthcare professionals to back-up their diagnoses. As these objects are not subject to the same specific standards as medical devices, such an approach would require the reliability of the data in question to be examined. For example, a study published in the *Journal of Clinical Sleep and Medicine* in November 2019 showed that Fitbit wearable devices for monitoring sleep show acceptable sensitivity but low specificity, making them still insufficiently accurate for use in clinical environments[44]. In the same year, a study published in the journal *Annals of Translational Medicine*, which examined the effectiveness of several smartwatches in detecting atrial fibrillation[45], reached similar conclusions[46]. Its authors specified in particular that even if these technologies could not constitute the ultimate tool for diagnosing this disorder, they could still serve as warning devices, encouraging their users to consult a doctor for confirmation in the event that an irregular heartbeat is detected. For its part, a study published in the *Journal of Strength and Conditioning Research* concluded that the BioHarness device developed by the Zephyr group, and the Fitbit Charge bracelet demonstrate excellent reliability measures. According to the authors of the study, stable and consistent measurements of heart rate and physical activity can be obtained

---

43   The Food and Drug Administration is the US regulatory authority for food and drugs. Among other things, it has the mandate to authorise the marketing of drugs in the United States.

44   Moreno-Pino, F., Porras-Segovia, A., López-Esteban, P., Artés, A., et Baca-García, E., "Validation of Fitbit Charge 2 and Fitbit Alta HR Against Polysomnography for Assessing Sleep in Adults With Obstructive Sleep Apnea", *Journal of Clinical Sleep Medicine*, Volume 15, Issue 11, November 15, 2019, pp. 1545-1653: https://jcsm.aasm.org/doi/full/10.5664/jcsm.8032
45   A heart rhythm disorder.
46   Raja, JM., Elsakr, C., Roman, S., Cave, B., Pour-Ghaz, I., Nanda, A.,Maturana, M., et Khouzam, RN., "Apple Watch, Wearables, and Heart Rhythm: where do we stand?", *Annals of Translational Medicine*, Volume 7, Issue 17, September 2019: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6787392/

using these devices[47]. These results suggest that there are limits to the use of data collected by connected objects for medical purposes, and that additional research in this area is needed on a case-by-case basis.

Recent work by the CNIL's (*Commission nationale de l'informatique et des libertés*, the National Commission for Information Technology and Liberties) Digital Innovation Laboratory (LINC) has also shown how information concerning people's health status can be inferred from "*innocuous digital traces (online behaviour, clicks, use of social networks, etc.) that have no direct link with their health status*"[48]. Professor and researcher in American law Mason Marks uses the term "emerging health data" to refer to these digital traces which are, a priori, harmless, but which allow users of digital services to be profiled – sometimes for commercial purposes – according to their health status.

In fact, the line between what constitutes health data and what doesn't is relatively blurred. In addition, the health data ecosystem is changing extremely rapidly. As a result, it is difficult to grasp it in its entirety.

POORLY HARMONISED COLLECTION AND MANAGEMENT PRACTICES RESTRICT THE INTEROPERABILITY AND SHARING OF HEALTH DATA

The complexity of the healthcare data ecosystem is also a technical issue, particularly in terms of interoperability. Despite general guidelines that apply to all stakeholders involved in the collection of health data, there are variations in the application of the latter. Thus, over time, these stakeholders have developed their own procedures for collecting and managing data, and defined their own rules for accessing their databases (when these are accessible). Thus, at the local level, certain large hospitals have their own data "repositories"[49], the operation and access of which they manage themselves. This is the case,

for example, for AP-HP (teaching hospital trust operating in Paris and its surroundings), which has set up a repository which holds data on 11 million patients[50]. Within the AP-HP itself, a scientific and ethics committee is responsible for analysing requests and granting access to the data in the repository. Nantes and Lille teaching hospitals (CHUs) have similar health data repositories (*entrepôts de données de santé* or EDS). Without going so far as to establish an EDS, every healthcare establishment generally has at least its own information system, enabling its staff to store and consult data relating to patients' follow-ups and the operation of the establishment. Likewise, some research centres have and manage their own databases for medical research. This is the case of the French National Institute for Health and Medical Research (*Inserm*), which is the promoter of, or in charge of organising more than 70 cohorts[51] in France. Although it represents an exceptional heritage, this plethora of data often obeys different standards and is not, in fact, interoperable[52]. This greatly limits its sharing between the different stakeholders of the ecosystem.

HEALTH DATA USE IS ALSO LIMITED BY CERTAIN STAKEHOLDERS' HOARDING PRACTICES

The lack of circulation of health data is not only due to its lack of interoperability. In addition to this technical obstacle, there is the issue of database ownership. Although the data collected may originally be personal data, most institutions involved in collecting health data, such as healthcare establishments or research institutes, consider that the databases they create are their property. According to Stéphanie Combes, Director of the Health Data Hub, issues such as "*the sharing of the value created, and the intellectual property linked to the provision of this data*" are sources of deadlocks. "*Some teaching hospitals or research centres want each private company that accesses the data to sign a contract with them, and agree to share the value created.*"[53] Because they spend a great deal of resources and time collecting this data, some stakeholders are tempted to make their use exclusive, and refuse to share it. Thus, the potential of this data is not exploited beyond the context and the studies for which it was collected, even though it is precisely

47   Nazari, G., MacDermid, JC., Sinden, KE., Richardson, J., et Tang, A., "Reliability of Zephyr Bioharness and Fitbit Charge measures of heart rate and activity at rest, during the modified Canadian Aerobic Fitness Test, and recovery", *Journal of Strength and Conditioning Research*, Volume 33, Issue 2, February 2019, pp. 559-571: https://journals.lww.com/nsca-jscr/Abstract/2019/02000/Reliability_of_Zephyr_Bioharness_and_Fitbit_Charge.32.aspx

48   Biéri, M., « Les données sociales sont des données de santé comme les autres », ("*Social data is health data like any other*"), CNIL's Digital Innovation Laboratory, May 17, 2021: https://linc.cnil.fr/les-donnees-sociales-sont-des-donnees-de-sante-comme-les-autres

49   A health data repository is a "*common information system, which aims to enable research in the field of health and studies relating to hospital management by bringing together all the data collected in institutions into a single database.*" Houdart & Associés, « Les entrepôts hospitaliers de données : du mythe à la réalité », ("*Hospital data repositories: from myth to reality*"), November 12, 2019: https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-realite/

50   AP-HP, « Comprendre les données de l'EDS » ("*Understanding EDS data*"): https://eds.aphp.fr/nos-services/eds-donnees

51   See: https://www.inserm.fr/recherche-inserm/recherche-en-sante-publique/cohortes

52   Interoperability is the ability of a computer system to communicate, run programs, or transfer data with other computer products or systems, existing or future, without constraint for the user in terms of access or implementation, and without multiplying development efforts. Source: https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-realite/

53   « Les données de santé, un trésor mondialement convoité » ("*Health data, a globally coveted treasure*"), *Le Monde*, March 2, 2020: https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html

the cross-referencing of various data that reveals its full value.

In March 2018, the "Villani report" (drafted by MP Cédric Villani) recommended, in a section dedicated to artificial intelligence used as part of health policies, the creation of a national platform "*to access and share data relevant to health research and innovation*"[54]. This is the Health Data Hub's ambition, the national health data platform launched in spring 2020, which has set itself the objectives of providing access to health data, supporting the collection and consolidation of this data, accompanying its development and analysis, and supporting the ecosystem and ensuring the link with civil society.[55] Faced with the data appropriation practices adopted by certain stakeholders in the healthcare system, the Health Data Hub's approach is clear: make sharing the rule, hoarding the exception. In this respect, the platform's prefiguration mission specified that "*data financed by national solidarity must be shared with all stakeholders, public and private, and thus benefit the healthcare system, research, the industrial fabric and ensure the maintenance of national sovereignty over a strategic sector*"[56].

A YEAR AFTER ITS LAUNCH, WHERE'S THE HEALTH DATA HUB AT?

Created by the Law of July 24, 2019 relating to the organisation and transformation of the healthcare system, the Health Data Hub officially began its activities earlier than expected, in April 2020, in order to enable the cross-referencing of data relating to Covid-19. It is organised as a public interest group (GIP), bringing together 56 stakeholders, including the French National Health Authority (HAS), *France Assos Santé* (the reference organisation representing and defending the interests of patients and healthcare system users), the French Public Healthcare Insurance System, CNRS (The French National Centre for Scientific Research), AP-HP, the Toulouse and Limoges teaching hospitals and the

French National council for the Order of Physicians[57].

Any person or organisation, public or private, can request access to the data available via the Health Data Hub in order to carry out a study, research, or assessment of public interest. The relevance (in particular their public interest nature) of the projects submitted is analysed by the Ethics and Scientific Committee for Research, Studies and Evaluations in the Healthcare Sector (CESREES), which brings together scientific, ethical and legal experts, and representatives of patient associations. The CNIL then decides on whether or not to authorise the project. At the moment, 26[58] projects are supported by the platform[59].

While the catalogue of data[60] available within the Health Data Hub is limited at the time of writing this report to the "Organisation for coordinated surveillance of emergencies (OSCOUR)" database, managed by Santé Publique France (National Public Health Agency), and to data from the SNDS, regarding patients with a Covid-19 hospital diagnosis, the Health Data Hub plans to host, among other things, a collection of databases from the SNDS, the France Marrow Registry[61], the i-Share cohort[62] and the 500,000 angioplasties database[63]. It should be noted here that the aim is not to bring this dataset together within a single database or platform. Instead, the relevant databases are replicated and then enriched within the Health Data Hub. Enriching the catalogue of available databases is the Health Data Hub teams' priority for 2021.

Several major projects that are underway, such as the implementation of the Health Data Hub, or the development of national security and interoperability standards, should help to decompartmentalise data and promote its sharing and re-use.

54   Cédric Villani, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » ("*Giving meaning to artificial intelligence: For a national and European strategy*"), March 2018, 201 pp.: https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf

55   Health Data Hub, Prefiguration report, October 2018, p. 32: https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf

56   *Ibid*., p. 19.

57   For the complete list, see the decree of 29 November 2019 approving an amendment to the constitutive agreement of the "National Institute for Health Data" public interest group creating the "Platform for health data" public interest group: https://www.legifrance.gouv.fr/jorf/id/JORF-TEXT000039433105

58   As of 17 March 2021.

59   For the full list see: https://www.health-data-hub.fr/partenariats

60   See: https://www.health-data-hub.fr/catalogue-de-donnees

61   The national registry of voluntary bone marrow donors.

62   The i-Share cohort is the largest scientific study ever carried out on the health of young people, which brings together more than 20,000 volunteers who answer questions on 12 topics related to their health, such as sleep, stress, or even diet.

63   Data to study the impact of stents in real life.

DATA WHOSE SENSITIVITY ENHANCES COMPLEXITY

Beyond the characteristics mentioned above, it is also the high sensitivity of health data that makes it particularly complex for various stakeholders in the healthcare chain to understand. This data is, in fact, extremely intimate data likely, moreover, to be misused. Sharing and using it therefore raises major ethical and technical issues, particularly in terms of confidentiality and security.

HEALTH DATA SENSITIVITY

CONFIDENTIALITY, AN ISSUE THAT IS AT THE HEART OF HEALTH DATA USE

Because it concerns the privacy of individuals, the confidentiality of health data is a key issue. In this respect, it is protected by the right to privacy[64], which is embodied, in particular, by medical confidentiality.

MEDICAL CONFIDENTIALITY: A HISTORIC BULWARK AGAINST THE DISCLOSURE OF PERSONAL HEALTH DATA

In France, medical confidentiality is enshrined in a number of legal texts, including:

- the Public Health Code;
- the Social Security Code;
- the Civil Code;
- the Penal Code;
- the General Local and Regional Authorities Code
- the Sports Code;
- the Family and Social Action Code;
- the French Data Protection Act;

- and the Council of State ruling of 26 September 2018 on the scope of medical confidentiality (patient identity).

In accordance with article L1110-4 of the Public Health Code, "*any person cared for by a healthcare professional, an establishment, or department, a professional, or organisation involved in prevention or treatment, whose conditions of practice or activities are governed by the present code, the military health service, a medico-social or social sector professional, or a social and medico-social establishment or service mentioned in I of article L. 312-1 of the Family and Social Action Code has a right to privacy and confidentiality of the information concerning them.*"

Violation of medical confidentiality may result in professional, civil, and criminal penalties of up to one year's imprisonment and a fine of 15,000 euros[65].

In order to ensure continuity of care, professionals of the same "healthcare team" may, however, be required to exchange medical information that's necessary for a patient's medico-social follow-up[66]. Since 2016, the law has thus defined the idea of "shared secret" (article L1110-4 of the Public Health Code) and specified its limits. The definition of healthcare team is set out in article L1110-12 of the Public Health Code. It should be noted here that the legal framework is not the same in all EU Member States, and that the definition of healthcare team varies from one country to another. This element will be an important consideration if the ambition of a European governance for health data is to materialise.

Because of the detriment (discrimination, risk of social exclusion) that the disclosure of personal health data could cause, the regulations applicable to the protection of this data entail a systematic obligation to inform the patient of any collection, and to obtain their consent should their medical data be used.

It is also important that this data be kept secret vis-à-vis certain stakeholders in particular: for example, insurance companies and employers or potential

---

64   See, on the vie-publique.fr site the following factsheet: https://www.vie-publique.fr/fiches/23879-chaque-citoyen-t-il-droit-au-respect-de-sa-vie-privee

65   Article 226-13 of the Penal Code.
66   Until 2016, it wasn't possible for a doctor to exchange information, for example, with a psychologist, about a patient they have in common. Now, with the idea of "shared secret", this is possible within the same healthcare team.

employers. Among the risks associated with sharing and using health data, several of the stakeholders interviewed for this report mentioned "insurance risk", i.e. the fact that insurance companies may offer different premiums depending on the risks identified by the analysis of the individuals' health data. In order to prevent this risk, the law prohibits any processing of the National Health Data System (SNDS) which could exclude an individual from being able to obtain a healthcare insurance policy, or to modify monthly insurance charges or premiums of an individual or group of individuals presenting the same risk.

It should also be noted that not all personal health data, which forms a very heterogeneous set of data, is equally sensitive. Some data, such as genetic data, is extremely sensitive because of its "multi-personal" dimension. This is the case with our DNA, which contains part of our family members' DNA. This makes the question of consent for the processing of such data particularly difficult. While the processing of genetic data is prohibited in France, a number of products based on genetic tests have developed in recent years. The MyHeritage online platform, for example, offers a DNA test which promises its users to "*find new family members and [...] discover their ethnic origins*"[67]. This development is all the more problematic because if data from DNA tests is leaked, an individual's physiological and psychological characteristics can potentially be identified and exploited by cybercriminals in order to carry out highly targeted computer attacks, such as social engineering and phishing.[68] [69] The National Commission for Information Technology and Liberties (CNIL), who is often solicited on this subject, is monitoring these developments closely.

FROM THIS NEED FOR CONFIDENTIALITY STEMS A NEED FOR PROTECTION AND SECURITY

Because of the strong need for confidentiality that overhangs health data, the latter inevitably calls for strong protection and security. Another risk, that was often cited by stakeholders interviewed for this report, is the risk of information systems hosting health data being hacked, for malicious purposes. In fact, this risk is an everyday reality. Cyberattacks against healthcare establishments and medical laboratories around the world are on the rise, including in France. In February 2021, the Dax Hospital and the Villefranche-sur-Saône's *Hôpital Nord-Ouest* were victims of ransomware attacks[70]. But while these examples have made headlines, they represent only the tip of the iceberg. The French National Agency for Information Systems Security (ANSSI) lists around one attempted attack per week on infrastructures such as nursing homes, teaching hospitals, hospitals and clinics or other entities linked to healthcare services[71]. In February 2020, Renaissance Numérique warned of the need for the entire healthcare system to ramp up their cybersecurity, as the rapid spread of digital tools and uses within it de facto increases the surface of exposure to cyber risks.[72] The acceleration of the national cybersecurity strategy presented by Emmanuel Macron on February 18, 2021 aims in part to respond to these challenges. Thus, "*for each digital program, healthcare structures will be requested to systematically devote 5 to 10% of the budget to cybersecurity, in particular to maintaining IS security over time*".[73] Following these announcements, a call for expressions of interest was also launched, in order to experiment with innovative solutions designed to meet the cybersecurity needs of three types of structures, including healthcare establishments[74].

Most often, the purpose of cyberattacks against healthcare establishments is to paralyse the operations of the victim establishment while awaiting the payment of a ransom. Their purpose is therefore not necessarily to steal health data from establishments to misuse it, even if this is increasingly the case. This

---

67   See: https://www.myheritage.fr/dna

68   On this subject, see the work of Renaud Lifchitz, specialist in cybersecurity, in particular his presentation "DIY DNA OSINT! or ... how to enhance your social engineering skills using recent genomics "at the 2019 International Cybersecurity Forum: https://speakerdeck.com/rlifchitz/diy-dna-osint-or-dot-dot-dot-how-to-enhance-your-social-engineering-skills-using-recent-genomics

69   « Les tests AND en kit, une nouvelle mine d'or pour les pirates ? » ("*DNA testing kit, a new gold mine for hackers*?"), Interview with Renaud Lifchitz, cybersecurity specialist, *BFM Business*, January 28, 2020: https://www.bfmtv.com/tech/vie-numerique/les-tests-adn-en-kit-une-nouvelle-mine-d-or-pour-les-pirates_AN-202001280085.html

---

70   According to the French National Agency for Information Systems Security (ANSSI), ransomware is a common cybercrime attack technique that consists in sending the victim malicious software that encrypts all of their data and demanding a ransom in exchange for the decryption password.

71   « Pourquoi les cyberattaques contre les hôpitaux ne vont pas s'arrêter » ("*Why cyberattacks on hospitals will not cease*"), *L'Usine Nouvelle*, February 16, 2021: https://www.usinenouvelle.com/article/pourquoi-les-cyberattaques-contre-les-hopitaux-ne-vont-pas-s-arreter.N1061559

72   Renaissance Numérique (2020), « Cybersécurité : accompagner un système de santé en pleine mutation » ("*Cybersecurity: Supporting an evolving healthcare system*"), 23 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/217/original/NOTE_CYBERSANTE.pdf?1582567842

73   Élysée, « Accélération de la stratégie nationale en matière de cybersécurité » ("*Acceleration of the national cybersecurity strategy*"), February 18, 2021: https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite

74   « Cybersécurité à l'hôpital: lancement d'un appel à manifestation d'intérêt pour expérimenter des solutions innovantes » ("*Cybersecurity in hospitals: call to action for expressions of interest to experiment with innovative solutions*"), *Tic Santé*, March 30, 2021: https://www.ticsante.com/story/5622/cybersecurite-a-l-hopital-lancement-d-un-appel-a-manifestation-d-interet-pour-experimenter-des-solutions-innovantes.html

is illustrated by the recent hijacking of a personal database holding health information on nearly 500,000 French citizens, which was sold on chat rooms specialised in the purchase and sale of pirated files, then disseminated in free access on chat rooms[75]. In this specific case, the stolen data came from files from 28 different laboratories, all of which used software that was no longer updated by its publisher.[76] [77] While this example underlines the importance of securing health data from a technical point of view, it also raises questions on the responsibility that the structures that collect and manage health data have. Moreover, according to ANSSI, the so-called "double extortion" phenomenon is increasingly widespread today. In this scenario, the attackers exfiltrate the data, publish some of it to pressure the victim establishment, and even though the latter agrees to pay the requested ransom, sell the data on cyber-criminal forums.[78]

In addition to external threats, data security risks can arise from human errors made by people who have access to this data, these two dimensions not being mutually exclusive. This is particularly the case when security procedures are not followed. As underlined during an interview with Jacques Lucas, president of the Digital Health Agency (ANS), hackings into an information system are often linked to non-compliance (even involuntary) with the security procedures established to access and exit said information system. During the interviews conducted as part of this report, a practice which is apparently widespread within hospitals was also mentioned: it consists in exchanging health data (reports, medical imaging) via messaging services that are not sufficiently secure for this purpose (WhatsApp, Messenger), due to available tele-expertise tools being user-unfriendly, complex, and not available on smartphones. While there may be technological security errors, human errors are also common. This security issue entails strong technical and legal constraints in terms of access to health data and processing methods. The ability of the stakeholders concerned to insure and take financial respon-

sibility for any security breach also weighs particularly heavily on the smallest of them (start-ups, small hospitals).

THE EXPLOITATION OF HEALTH DATA RAISES ETHICAL ISSUES THAT DESERVE PARTICULAR ATTENTION

If the sharing and processing of health data are strictly regulated from a security point of view, it is also because they raise strong ethical considerations, which go beyond the confidentiality issues already mentioned. As the National Consultative Ethics Committee (CCNE) for Life and Health Sciences underlines in its opinion 130, the main challenge in this area is to "*find the right balance between the risk of under-exploiting data, thus limiting research carried out in the public interest, and that of too broad and insufficiently controlled data sharing, which could jeopardise an individual's fundamental human rights.*"[79]

For example, it is worth considering the framework which is applicable to the marketing of this data. In France, personal health data is subject to a specific regime, similar to the one applicable to the human body. In accordance with the Civil Code and the applicable case law, an individual's personal data is in fact not considered as property, but as a right attached to the human person. As such, it cannot be transferred or sold (apart from the exceptions and conditions provided for by law). This position ties in with the same ethical considerations that prompted legislators to ban the processing of data from the SNDS, aimed at differentiating insurance premiums according to risk. But what about so-called "well-being" data, collected by applications or through connected objects such as bracelets, watches and scales, which provide information on people's health status? The Vitality program, run by the insurance company Generali, for example, offers employees who wish to do so, the opportunity to synchronise their connected objects and other physical activity tracking applications with its platform, and in exchange, receive rewards (gift vouchers, discount coupons) to spend with its partners. While the standard GDPR regime applies in this case (the data in question not being considered as health data), this practice, and in particular the fact that the company considers that this data is not health data, may raise questions. Has this qualification of the data collected been submitted to the regulator

75   « Cinq questions sur la fuite des données médicales de 500 000 Français sur le Web » ("*Five questions regarding the leak of medical data of 500,000 French citizens on the Web*"), *Le Monde*, February 25, 2021: https://www.lemonde.fr/pixels/article/2021/02/25/cinq-questions-sur-la-fuite-des-donnees-medicales-de-500-000-francais-sur-le-web_6071223_4408996.html
76   *Ibid.*
77   Dedalus, Press Release, February 26, 2021: https://www.dedalus-france.fr/wp-content/uploads/2021/02/21.02.26_CP-Dedalus-France-confirme-investiguer-sur-un-grave-acte-de-cybercriminalit%C3%A9-et-a-identifi%C3%A9-et-pr%C3%A9venu-les-laboratoires-concern%C3%A9s.pdf
78   ANSSI, Governmental Centre for Monitoring and Alerting and Responding to Computer Attacks, « État de la Menace Rançongiciel à l'encontre des entreprises et institutions » ("*State of the ransomware threat against businesses and institutions*"), March 1, 2021, p. 13: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

79   National Consultative Ethics Committee for Life and Health Sciences (2019), « Données massives et santé : Une nouvelle approche des enjeux éthiques » ("*Big Data and Health: A New Approach to Ethical Issues*"), Opinion 130, p. 8: https://www.ouvrirlascience.fr/donnees-massives-et-sante-une-nouvelle-approche-des-enjeux-ethiques/

for analysis? Even if we accepted that this is well-being data, and not health data, the fact that it is collected by an employer with regards to its employees (with whom there is a subordination relationship, making the latter potentially more vulnerable), should it not lead to a higher level of sensitivity of the data collected? Apart from its nature, the identity of the person in charge of the data can cause the data collected to become more sensitive.

Likewise, we should ensure that the use of tools based on the exploitation of health data doesn't lead to unequal access to healthcare. Indeed, while the lack of digital literacy persists in society, the digitalisation of health is rekindling this risk in some ways. In February, for example, the Covid-19 vaccination centres in the Seine-Saint-Denis department saw an influx of patients from neighbouring departments, who were more connected and used to making appointments on platforms such as Doctolib (a free online service to find nearby health practitioners and book doctor appointments). As a result, among the recipients of the vaccine received at the municipal health centre of the city of La Courneuve in the first two weeks, only 20% were actually from La Courneuve. How can we ensure, therefore, that the digitalisation of the healthcare sector is not to the detriment of the most disadvantaged? How can we ensure equal access to healthcare for people who cannot or simply don't want to use these tools? This question deserves to be placed at the heart of debates aimed at defining tomorrow's healthcare system.

Finally, the possibility of implementing massive data processing (big data) in the healthcare sector, for example to train diagnostic assistance algorithms, also raises questions, particularly in terms of prediction. More precisely, it is about defining how far predictive medicine can go, without infringing on individuals' fundamental rights. If tomorrow, thanks to an algorithm, it were possible to predict that a person has a 96% chance of dying from lung cancer before the age of 50, what should be done with this information? Would it be appropriate to pass it on to the person in question, and if so, at what point in their life? This is not a new question, and has arisen in connection with the detection of genetic diseases for a long time. In this context, the individuals concerned have the choice to know or not to know whether they are carriers of the offending gene. The same logic could then be applied to algorithmic predictions, and we could, for example, imagine a healthcare professional asking his or her patient "Would you like to know or not what the algorithm is predicting?". Whatever solution is chosen, society must choose what our shared vision of the healthcare system is. Moving forward with the sharing and use of health data requires a collective understanding of these issues.

A STRICT LEGAL FRAMEWORK, WHICH ACTS AS A GUARDIAN

Due to the ethical and technical issues surrounding it, health data is subject to a strict legal framework. At a European level, it is considered a special category of personal data within the definition of the General Data Protection Regulation (GDPR), in the same way as data relating to racial or ethnic origin, political opinions, religious or philosophical convictions, or union membership. In accordance with Article 9(1) of the GDPR, its processing is in theory therefore prohibited. There are, however, a number of exceptions to this prohibition principle, listed in subsection 9(2) of the regulation. With regard to health data, several exceptions are likely to apply, including:

· when the processing is necessary for the purposes of preventive or occupational medicine, the assessment of a worker's ability to work, medical diagnoses, health or social care, or the management of health or social care systems and services;

· when the data subject has given their explicit consent;

· when the processing is necessary to protect vital interests;

· when the processing is necessary for important public interest reasons;

· when the processing is necessary for scientific research purposes[80].

In France, the Data Protection Act also acknowledges it has a particular level of sensitivity, and prohibits its processing (article 6). Like the GDPR, however, it sets out exceptions, which constitute the conditions under which health data can be communicated and used: medical monitoring, diagnostics, healthcare, prevention, medical research, compilation of statistics in the healthcare field, evaluation or analysis of health practices, etc.[81]

This legal framework, which is therefore both European and specific to each country (health remaining a prerogative of the EU Member States), entails a certain number of technical and legal obligations concerning access to health

---

80   In France, this is currently limited to research of public interest. Thus, private organisations wishing to access the data made available through the Health Data Hub, must prove to the Ethics and Scientific Committee for Research, Studies and Evaluations in the Health Field (CESREES) why their research project is of public interest.

81   See: Title II, Chapter III, Section 3 - Processing of personal data in the healthcare sector, of Law n° 78-17 of 6 January 1978 relating to data processing, data files and liberties.

data, its processing and its hosting, which data controllers must respect. The procedure for accessing data also depends on the nature of the research, the organisation requesting it, and the data it wishes to access. As has been pointed out, some health data repositories (HDR) held by hospitals, have their own access rules, sometimes managed by a scientific and ethics committee. Without the harmonisation of data access rules between healthcare stakeholders, it is therefore necessary to refer, for each database in question, to the access request instructions specific to the structure making the data available. Figure 2 details, for example, the process required to access data from the AP-HP HDR.

FIGURE 2 - PROCEDURE FOR REQUESTING ACCESS TO DATA FROM THE AP-HP HEALTH DATA REPOSITORY
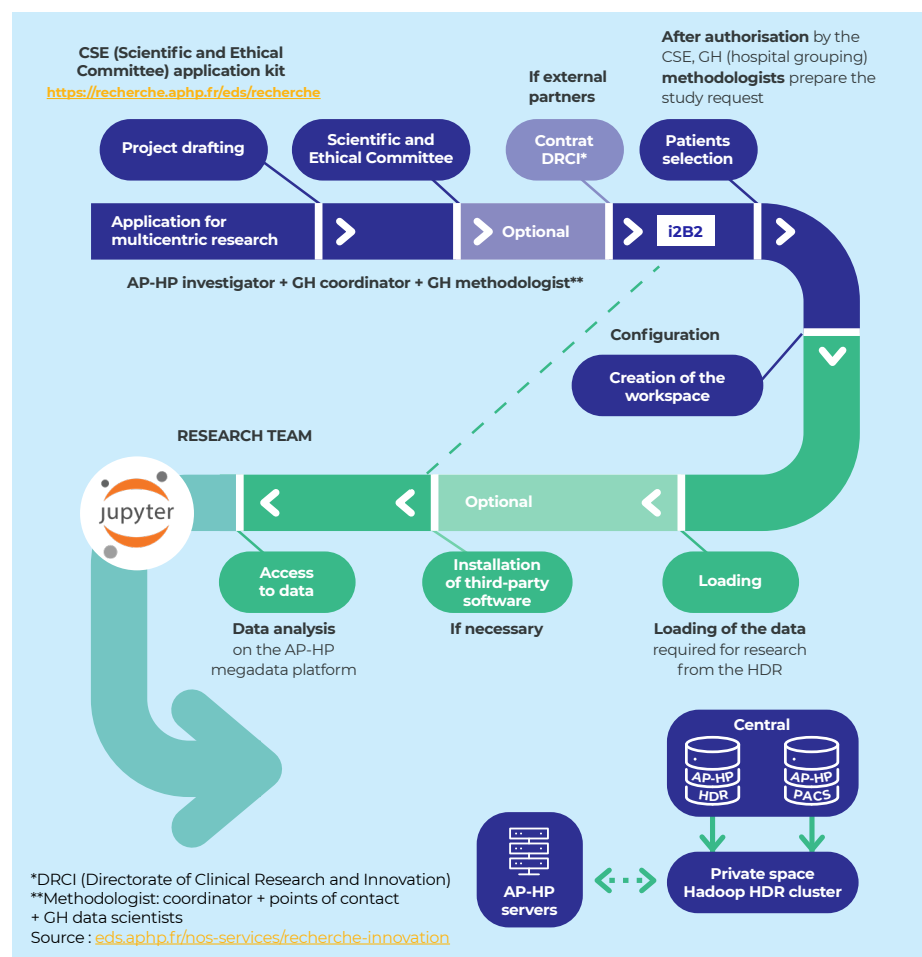
ACCESS TO DATA FROM THE NATIONAL HEALTH DATA SYSTEM

If we take the example of data from the National Health Data System (SNDS), there are two different types of access:

· permanent access, for the benefit of certain public services or bodies (General Directorate of Health, regional health agencies, National Agency for the Safety of Medicines and Healthcare Products (ANSM), etc.) for the completion of their projects and within limits fixed by decree[82];

· one-off access, subject to the prior completion of a formality vis-à-vis the National Commission for Information Technologies and Liberties, for other organisations (private structures, for example), for certain purposes set by the Public Health Code, such as carrying out a study, research, or assessment, and meeting a public interest requirement[83].

Any organisation wishing to obtain a one-off access to SNDS data must complete a CNIL formality. There are two possible procedures for this: either the organisation confirms that the purpose of its request is compliant with one of the reference methodologies developed by the authority[84], or (in the event of non-compliance) it submits an authorisation request to the authority. These formalities can be difficult to implement.

For example, access to SNDS data is strictly restricted for companies that manufacture healthcare products and for insurers. These organisations must either go through an independent research bureau or an independent research laboratory that will process the data on their behalf, and send them aggregated results, or demonstrate that the technical access methods don't allow them to use the data from the SNDS for prohibited purposes. During a webinar on health data, research, and Covid-19, organised on January 27, 2021, Manon de Fallois, a lawyer in CNIL's health department, explained that

---

82   Decree n ° 2016-1871 of December 26, 2016 relating to the processing of personal data known as the "national health data system".
83   See: https://www.health-data-hub.fr/interet-public
84   For the list of reference methodologies related to healthcare developed by the CNIL, see: https://www.cnil.fr/fr/traitements-declaration-conformite?field_norme_numerotation_type_value%5B0%5D=6

demonstrating this wasn't "*particularly straightforward*" and that "*in almost all cases, healthcare industry players or insurers prefer to go through a research laboratory or an independent research bureau*".

> *The GDPR, which is a beneficial European regulation for citizens, has been an issue for researchers' work for a year and a half, in the transposition that is made by different States. The dossiers that we carry on large clinical trials are examined by very specialised lawyers over a period of about 9-10 months, so as to understand what needs to be declared to the CNIL. The risk analysis is very complex, we need to talk to many people, there are a lot of documents to fill in. When we think "health data" and how a collective benefit can be obtained from it, with view to improving healthcare, we're confronted with a very complex situation"*

Franck Lethimonnier,
DIRECTOR OF THE "TECHNOLOGIES FOR HEALTH" THEMATIC INSTITUTE AT *INSERM*

Finally, in order to guarantee sufficient protection of the data in question, the data must not mention the names of individuals, nor any other information which would directly or indirectly identify them: they must be "pseudonymised". Pseudonymisation is a (reversible) processing of personal data which makes it impossible to identify the data subject without resorting to additional information, provided that this additional information is kept separately and subject to safeguards[85]. In practice, pseudonymisation consists of replacing directly identifying data (surname, first name, date of birth, etc.) in a data set with indirectly identifying data (alias, sequential number, etc.). In addition to pseudonymisation, there is another way to process health data without infringing on individual privacy: anonymisation. Anonymisation is a process that uses a set of techniques in such a way as to make it impossible, in practice, to identify the person by any means whatsoever and, this time,

---

85   See in this context, Article 4(5) of the GDPR and point 6.1. of the appendix to the Order of 22 March 2017 on the security reference framework applicable to the National Health Data System.

in an irreversible manner. All directly or indirectly identifying information is deleted or modified. In this case, data protection legislation no longer applies, as the dissemination or reuse of anonymised data has no impact on the privacy of the persons concerned. However, in the healthcare sector, strict anonymisation can make certain research projects almost impossible to carry out. When we anonymise information, we deindividualise it in such a way that there is no more possibility of re-individualising a characteristic, be it by deduction or cross-referencing. At such a level, carrying out research becomes complicated. We can no longer, for example, establish cohorts of people who look alike, because they no longer have characteristics that make them unique. Moreover, some data, like genomic data, cannot be completely anonymised.

In view of the sensitivity that characterises health data, the existence of a legal framework to protect individuals and their data is essential. If the current framework defines protection at an individual level, perhaps it would be possible, in certain areas, to consider protection at a collective interest level, rather than just an individual interest level, of the people whose data is processed.

PERSONAL PROTECTION VS. PUBLIC HEALTH?

Based primarily on the protection of personal data, the legal framework surrounding the processing of health data makes individuals a central concern. This observation can be considered obvious, insofar as this data is data that, by nature, "individualises" people. However, the enormous amount of data produced by the healthcare system and the ability to use it in a secure manner opens up new perspectives in public health (epidemiology, organisation of healthcare, etc.). At present, every effort is made to ensure that individual citizens are protected against any invasion of their privacy. This approach is of course necessary and commendable. Taken to the extreme, it can nevertheless hinder the achievement of certain collective public health objectives.

Processing health data requires falling under one of the exceptions mentioned by the GDPR. In this respect, it emerges from the interviews carried out for the purpose of this report, that the most often adopted legal basis would be that of consent of the persons whose data is being processed (Article 9 (2) (a)). In addition to being informed of the processing of their data and the purpose of the processing, the individual must give their free, specific, informed and

unambiguous consent[86]. For example, when designing the StopCovid (now TousAntiCovid) contact case tracking application, the CNIL, just like the German data protection authority[87], decided to require individuals' consent. Regardless of the questions that this may raise with regard to public health objectives, consent has limits, including from the point of view of individual protection. The difficulty with consent is that it must be free and informed, which is not always the case. Hélène Guimiot-Bréaud, head of CNIL's health department, believes that "*compliance with the obligation to provide information is not always easy: the information provided to individuals may be insufficient or, on the contrary, too detailed and confusing*"[88]. However, for consent to be fully informed, flawless information is needed. More importantly, in the field of healthcare, people who have to give consent to the processing of their data are very often in a vulnerable position. Indeed, in many cases consent is not free and not informed. Therefore, it cannot be a guarantee of compliance with the GDPR and of the proper protection of individuals and their data.

This is undoubtedly why legal texts have specifically allowed for the possibility of not seeking the consent of individuals when it comes to fulfilling a public health requirement. Despite this possibility, the trade-off between personal data protection and public health objectives remains difficult. All European regulators have different views on the subject, and the CNIL, as shown by its decision to require consent for the deployment of the StopCovid application, is being particularly cautious. While the GDPR allows it (in the name of public interest), and the fight against the Covid-19 pandemic offered arguments in favour of public health protection, the authority considered that this was not sufficient to dispense with consent.

These questions are subject to decisions that don't depend on a single regulator, and there is an opportunity to redefine health democracy, by inviting the various stakeholders in the healthcare chain, including citizens, to take part in the debate.

The transformation of our healthcare system through digital data is now well underway. However, this raises questions of an ethical, technical and legal nature, which must be considered collectively. In the context of this data's usage, how can we reconcile the issue of protecting individual freedoms and public health objectives? How far should we go in predictive medicine? What should be the role of the different healthcare chain stakeholders in the governance of this data? How can we ensure equal access to healthcare for people who cannot or simply do not want to use digital health tools? These are all point that must be decided upon by including all stakeholders, right down to the citizens. Redefining health democracy in the light of health data requires, however, first of all, that all stakeholders in the chain be empowered to understand what this data is, and the issues underlying its sharing and use. As presented in this section, the health data ecosystem is indeed extremely rich and complex, evolving constantly and rapidly. So that all stakeholders in the healthcare chain, and in particular citizens, can engage in the related issues, serious efforts to take "ownership" of them are essential.

---

86   Recital (32) of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her*".
87   See the privacy policy of the official German CoronaWarn-App: https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf
Other regulators, for example in the UK, have chosen to prioritise the public interest. See, in this regard, the privacy policy of the application developed by the National Health Service (NHS): https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice
88   Interview conducted by videoconference on November 16, 2020.

PART 2
FOR A SHARED CULTURE OF HEALTH DATA

Making data one of the levers of health democracy represents a massive acculturation challenge. The lack of digital literacy among the population, as well as the inherent complexity of the health data ecosystem, limits the understanding of this data. If it is already difficult to understand what data or an algorithm is, how can we expect everyone to easily understand the issues underlying the sharing and use of health data? As revealed by the interviews carried out for the writing of this report, the various healthcare sector stakeholders are well aware of this, and some of them (in particular the private complementary healthcare insurances, the Red Cross, the Health Data Hub, the French Public Healthcare Insurance System, the ANS and the ARS) are launching initiatives to make citizens familiar with the concept of health data. Moreover, the assimilation efforts that need to be made do not only concern the familiarisation of the stakeholders in the healthcare world (citizens, patients, healthcare professionals and establishments, private complementary healthcare insurances, French Public Healthcare Insurance System, industry players, regional and national agencies, etc.) with the digitalisation of this sector. It is also necessary to develop the expertise of the "new entrants" from the digital world who are investing in the health field, and who are not always aware of the issues within this environment.

ACCULTURATE STAKEHOLDERS OF THE HEALTHCARE SECTOR TO DIGITAL DATA

There are ongoing government initiatives to digitalise the healthcare sector, which have gained significant momentum in the last two years. Despite this, citizens still have a relatively low level of awareness of these initiatives, and healthcare professionals and institutions still have a mixed usage of them. However, various studies carried out by the think tank, as well as meetings organised for the purpose of this report, show that this lack of acculturation doesn't only concern health data, but rather data (and digital data) in general. It is therefore a whole data culture that needs to be created.

> *"The lack of digital literacy is a real problem. People are not aware of their digital rights and do not fully understand that their data is very valuable",*
>
> **Jelena Malinina,**
> **DIGITAL HEALTH POLICY OFFICER, BEUC**

Within this acculturation to data effort, the specific nature of health data should not be ignored. While citizens are progressively building their knowledge of the value of some of their data, for example their banking data, this development seems to exclude health data for the time being. Citizens are generally unaware of both the definition and the value of their health data.

DIGITAL HEALTH DATA, AN ASSET THAT IS STILL POORLY UNDERSTOOD

For the non-experts (and sometimes even for the experts), qualifying the benefit of data is not straightforward. Compared to the benefit that can be derived from the analysis of health data, the benefit of a medication, for example, is relatively simple to understand. If we simplify things to the extreme: you get sick, you take medication, you get better. The benefit is easy to understand because it is being experienced. Conversely, understanding that sharing and processing data can improve health is complex. It requires understanding that at the heart of the process, there is a whole ecosystem, which includes researchers, project leaders, who enable innovations, and so on. This is what's at stake in the development of data literacy, which is defined as the ability to produce, understand, and use digital data[89]. In this respect, 54% of the respondents of an OpinionWay survey carried out for the Ministry of Solidarity and Health in November 2020, mentioned the exclusion of users who are not familiar with digital technology as the main risk factor posed by the creation of an *Espace numérique de santé*. The results of the 2020 European Digital Economy and Society Index (DESI) show, on the other hand, that only 57% of the French population have basic digital skills, a figure that has not changed since 2018[90]. Those with more advanced digital skills represent only 31% of the population[91].

But this difficulty in understanding data is not just a literacy issue. It is also a question of equipment. As revealed in the latest digital barometer, carried out by France's Electronic Communications, Postal, and Print media distribution Regulatory Authority (ARCEP), the General Economic Council (CGE) and the *Mission Société Numérique* (programme supporting the digital transition of territories in terms of usage, access rights, and services), 12% of the French population aged 12 and over is still not connected to the Internet[92]. Moreover, a recent study by the Terra Nova think tank showed that, although it is diminishing, the digital gap continues to exist between territories, with rural and peripheral areas remaining under-equipped compared to large conurbations[93]. Involving all citizens in the digital transformation of healthcare is undoubtedly one of the greatest challenges facing the sector in the years to come. To ignore this reality would be to run the risk of setting up tools at a national level (e.g. *Mon Espace Santé*) that would only be used by a certain part of the population, while others would be left behind. In view of this, the need to maintain non-digital alternatives is evident.

Putting citizens in a position to "seize" their personal health data is all the more crucial, as this command is a key component of their ability to get involved in the debates surrounding its use, from which they are often excluded.

The interviews conducted by the think tank as part of this study also revealed great disparities in the preparedness of healthcare professionals, patient associations, and public and political decision-makers with regard to health data. For example, unlike some entities, large teaching hospitals generally have a medical information department (or equivalent), within which data specialists work closely with information systems managers. These human resources give them particularly advanced skills and maturity in the area of health data. Conversely,

89   Renaissance Numérique and Syntec Numérique (2019), « Tous acteurs des données. Appréhender les données pour mieux les valoriser » ("*We're all data stakeholders. Understanding data to make better use of it*"), p. 81: https://www.renaissancenumerique.org/publications/tous-acteurs-des-donnees-apprehender-les-donnees-pour-mieux-les-valoriser

90   Digital Economy and Society Index (DESI) 2020 - France, p. 9: https://digital-strategy.ec.europa.eu/en/policies/desi-france

91   *Ibid.*

92   ARCEP, CGE, Mission Société Numérique (2019), « Baromètre du numérique 2019. Enquête sur la diffusion des technologies de l'information et de la communication dans la société française en 2019 » ("*Digital Barometer 2019. Survey on the dissemination of information and communication technologies in French society in 2019*"), p. 9: https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/numerique/le-barometre-du-numerique.html

93   Terra Nova, « Baromètre des résultats de l'action publique : la France de la fibre optique » ("*Public action results barometer: The optical fibre France*"), April 16, 2021: https://tnova.fr/notes/barometre-des-resultats-de-l-action-publique-la-france-de-la-fibre-optique

other stakeholders, such as certain ARS, have relatively limited capacities in this area. These ARS found themselves in a difficult position during the Covid-19 crisis, when they had to set up the tracking of contact cases and then the vaccination, without being allocated any additional resources. From one ARS to another, data processing skills may also vary greatly, depending in particular on the resources allocated to the statistical departments.

Even within the central administration, particularly in the various government departments, awareness of these issues among staff remains relatively limited for the time being. The plan for the transformation of public action, presented by Minister Amélie de Montchalin in March 2021[94], and supported by the work of the "Bothorel mission" (the mission for a public data policy conducted by MP Éric Bothorel), aims to address this shortfall. Indeed, it is expected that, by September 2021, each government department will complete a roadmap specifying the outlines of its data governance, as well as the policies for opening up and using the data that they will have put in place. This request is also supported by an official order signed by the Prime Minister, Jean Castex, and addressed to the members of the government and regional officials, to whom he reminds: *"It's also your responsibility to set up the most appropriate organisation to promote synergies between the departments in charge of digital data in your ministry, particularly the statistical departments. To this effect, by 15 May, you will appoint a ministerial data administrator, in charge of developing your government department's strategy in this area, coordinating the stakeholders, and being the point of contact for data users and digital applications within your scope."*[95] A contact person has thus been appointed in each ministry[96]. For the Ministry of Solidarity and Health, this is Fabrice Lenglart, Director of DREES. The plan to modernise the civil service also includes a section aimed at opening up more data, in order to steer public policies more effectively and allow greater transparency in public action. This ambition reflects an awareness of the importance of addressing the data issue at the highest level of government. The challenge is now to effectively disseminate this data culture in the various branches of the healthcare administration.

---

94   French Ministry of Public Transformation and Civil Service, « 400 jours pour accélérer la transformation numérique de l'État » ("*400 days to accelerate the government's digital transformation*", Press kit, March 4, 2021: https://www.transformation.gouv.fr/files/presse/Dossier-de-presse-400-jours-accelerer-transformation-numerique-etat-04.03.2021.pdf
95   Prime Minister, Circular n°6264/SG of 27 April 2021 relating to the public policy on data, algorithms and source codes: https://www.legifrance.gouv.fr/download/pdf/circ?id=45162
96   See the full list here: https://www.data.gouv.fr/fr/datasets/liste-des-administrateurs-ministeriels-des-donnees/

PROMOTE A UNIVERSAL ACCULTURATION TO HEALTH DATA

BUILD GENERAL AWARENESS OF HEALTH DATA, CONTINUOUSLY

For a shared command of health data, it is useful to think of an education continuum, which doesn't only refer to a data culture education. This must be based around three axes: education in digital citizenship in the broad sense, healthcare education, and therapeutic education.

ACT ON THREE AXES OF ACCULTURATION FOR CITIZENS TO FAMILIARISE WITH HEALTH DATA

Renaissance Numérique has identified three priority education areas to establish a "health data culture" among citizens:

- Education in digital citizenship in the broadest sense: teach what health data is, what it is used for, and what it could be used for. Make citizens familiar with tools based on health data, which have been developed by public (SMR, ENS) and private services, and guide them in their use if necessary. Enable them to recognise the good and bad practices relating to their health data.

- Healthcare education: explain the importance of having health data prioritised and processed appropriately. This approach can be found in particular through the TousAntiCovid application, which includes an information service on the epidemiological situation and news related to the fight against the epidemic (e.g. measures implemented by the national and local authorities).

- Therapeutic education: support patients that have a particular need for using solutions such as connected medical devices, on how to use them. A noteworthy example is the care of patients with chronic pathologies who are equipped with connected medical devices. These patients must quickly get to grips with reading and interpreting their health data. This acculturation is made possible in particular by the therapeutic assistance provided by healthcare professionals as part of the healthcare pathway.

In order to ensure equal access to healthcare, however, it is crucial that education efforts take into account the different levels of literacy within the population. For example, consulting one's health data on an online platform such as *Mon Espace Santé* or (for the moment) the Shared Medical Record (SMR), already requires a certain level of digital literacy, beyond the actual question of data: internet navigation, password management. Some citizens do not have this level of knowledge. Conversely, diabetic patients, for example, who are used to managing their condition on a daily basis using a device connected to an application, will no doubt find it easier to access and use online healthcare services. According to the above-mentioned OpinionWay survey, "*the use of digital health tools is more widespread among populations used to the digital world, but also among certain populations with more fragile health (people with disabilities, long-term illness beneficiaries[97], patients that frequently visit the doctor, etc.) or those located in medical deserts.*"[98] As illustrated by the example of booking appointments on online platforms for the Covid-19 vaccination, these inequalities in digital acculturation can lead to unequal access to healthcare.

It is also essential to set up specific support for the most isolated people, for example through the *France Services centres*[99], which are relays in the regions and complement the national "*Ma Santé 2022*" strategy. In this respect, during the presentation of her plan, the Minister for Transformation and the Civil Service insisted on the need for the administration to take advantage of its digitalisation to offer simpler, more user-friendly, and faster procedures, stressing however that "*it's not about doing 100% digital, but doing 100% quality digital, and a ways offering an alternative*"[100]. Nor should certain persistent technical obstacles be minimised, such as the lack of interoperability between information systems and business software. If, since 2011, only just over 9 million shared medical records (SMRs) have been made available (with a target of 40 million

by 2022), this is also due to the lack of interoperability between healthcare information systems[101].

Disseminating a health data culture in society inevitably requires raising awareness continuously. First of all, it must be embodied at the highest level of government. Without strong political support, there is a risk that we will be left with discussions led by ultra-specialists. It is therefore essential, on subjects as crucial as digital health, that public decision-makers adopt clear and understandable messages. The issue of health data and its use is not limited to technological issues or issues related to potential misuse. The misuse has largely dominated recent debates, whether on the StopCovid application (questions about Bluetooth technology, controversy about the possibility of using the application developed by Apple and Google, fear of widespread surveillance and restricted use) or the Health Data Hub (data hosting by Microsoft Azure). In addition to these elements, which from a citizen's point of view deserve to be explained and understood, the acculturation to digital health must be tackled from a healthcare perspective. This involves, for example, identifying simple and concrete use cases, success stories that people can identify with (e.g. the *ViteMaDose* (QuickMyDose) platform, which makes it possible to find Covid-19 vaccination slots), in order to familiarise citizens with health data and its uses. Given the importance of the issues at stake, these efforts must be widespread and involve public campaigns, as was done in the fight against Covid-19. The challenge is also to reach the public who are furthest away from these issues, particularly young people in good health, who don't feel it is relevant to them. To do this, the communication put in place must be designed according to the different target audiences. Social networks are, for example, an important channel for communicating with young people.

Whether in the professional world or at school, medical check-ups, which are part of preventive measures, are also opportunities to raise general awareness of digital health. In this regard, data education deserves to be reinforced at school, from the earliest age. In this respect, the Health Data Hub is cooperating with the French Ministry of Education to ensure that the question of data is integrat-

97   The long-term illness allowance concerns any person suffering from a chronic disease. This means that the French Public Healthcare Insurance System covers 100% of the healthcare costs related to that chronic disease.
98   French Ministry of Solidarity and Health, Citizen Workshops on Digital Health, « Rapport Phase 2 : Les français et le virage numérique en santé » ("*Phase 2 report: The French and the digital shift in health*"), 2020, p. 27: https://esante.gouv.fr/sites/default/files/media_entity/documents/ateliers-citoyens-rapport-phase02-vdef-2020-11-17-web.pdf
99   See: https://www.cohesion-territoires.gouv.fr/france-services In its information report on shared medical records and health data, Cyrille Isaac-Sibille, Member of the French Parliament, suggested using *France Services centres* to ensure that people who are not digitally literate have access to their SMRs.
100 French Ministry of Public Transformation and Civil Service, *Ibid*.: https://www.transformation.gouv.fr/files/presse/Dossier-de-presse-400-jours-accelerer-transformation-numerique-etat-04.03.2021.pdf

101 Cyrille Isaac-Sibille (July 2020), « Rapport d'information déposé en application de l'article 145 du Règlement, par la Commission des Affaires sociales, en conclusion des travaux de la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale sur le dossier médical partagé et les données de santé » ("*Information report submitted pursuant to Article 145 of the Rules of Procedure, by the Social Affairs Committee, concluding the work done on the evaluation and monitoring of social security financing laws on shared medical records and health data*"), 124 pp. : https://www.vie-publique.fr/rapport/275971-rapport-sur-le-dossier-medical-partage-et-les-donnees-de-sante

ed into the notion of digital education in moral and civic education classes, and is also working on providing teachers with data-related tools. This is an approach that deserves to be deployed on a large scale, by broadening the base of stakeholders involved (as it is not the Health Data Hub's role to drive the data education policy in France).

STAKEHOLDERS FROM THE HEALTHCARE SYSTEM MUST STEP UP WITH REGARDS TO THESE ISSUES

Some key stakeholders in the healthcare system also need to step up to the challenge of acculturation and be empowered in this respect. From this point of view, not everything has to be reinvented. Patient associations and communities could, for example, be a high-potential acculturation agent. However, the interviews carried out as part of this report revealed that these associations were, on the whole, very poorly structured in this area. Patient organisations must therefore be encouraged to tackle the issues related to health data, be trained, and be prompted to get in touch with each other in a mutual learning process. Those who are more familiar with digital health could take part in the sharing of best practices in terms of data appropriation, which could then be passed on by each association to its members. This empowerment of patient organisations should also give new impetus to health democracy, by strengthening their role in decisions relating to digital health policy.

Moreover, a certain number of professions, such as doctors, nurses, pharmacists, or even stakeholders in the medico-social and paramedical sector (e.g. nursing assistants), are de facto already healthcare mediators. In the future, their role will include supporting citizens in their use of digital health. In this respect, pharmacists and nurses could, for example, have a specific role related to certain diseases, certain connected devices, or certain types of remote monitoring. This is not a question of creating new professions, but of developing existing ones. For the deployment of the ENS, for example, the Ministerial Delegation for Digital Health (DNS) recommends "*drawing on general practitioners, specialists, and dispensing pharmacists who are highly trusted and are already familiar with the shared tools system*"[102].

" Healthcare professionals are our first point of contact: it's up to them to guarantee the transparency and the framework surrounding the use of this data (possibility of opt-out, etc.). There is an anxiety-provoking environment regarding the use of data (StopCovid, news headlines). We need to put healthcare professionals back at the heart of all this, by giving them the necessary means and training"

Nesrine Benyahia,
CO-PRESIDENT OF THE DIGITAL BOARD, FRENCH DIGITAL HEALTH SOCIETY

Digital health will have a de facto impact on the professions in the sector, which will see their field of expertise widen or narrow. Each profession must seize this challenge in order to reinvent itself, and be assisted by some form of change management support. The recent creation of a medical assistant status for private practitioners, for example, is part of this approach.[103]

Some professions, such as doctors (both general practitioners and specialists), nurses, pharmacists and other stakeholders in the medico-social and paramedical sector, must not only be given more support in the performance of their duties, but also be empowered if necessary, if these duties expand and/or change in terms of their responsibilities. Faced with the rapid development of digital solutions applied to healthcare, the multiplicity of offers available in terms of business software, recent changes in the legal framework, or the requirements to be met in terms of interoperability and security standards, some healthcare professionals may feel helpless. This applies to both hospitals and outpatient clinics. Although this injunction has been systematically mentioned for several years, it is worth recalling the need to integrate concepts relating to the use of digital technology and data in the healthcare field into healthcare training curricula, whether within initial training level or continuing training (which is, moreover, almost non-existent in this field). On 22 February, the Minister of Solidarity and Health, Olivier Véran, and the Secretary of State for Digital Transition and Electronic Communications, Cédric O, announced that "*awareness of cybersecurity will be integrated into all training courses for*

---

102 French Ministry of Solidarity and Health, Citizen Workshops on Digital Health, *Ibid.*, p. 27: https://esante.gouv.fr/sites/default/files/media_entity/documents/ateliers-citoyens-rapport-phase02-vdef-2020-11-17-web.pdf

103 « Création des assistants médicaux : les textes sont parus ! » ("*The introduction of medical assistants: the texts have been published!*"), *Infirmiers.com*, August 21, 2019: https://www.infirmiers.com/actualites/revue-de-presse/creation-assistants-medicaux-textes-parus.html

healthcare professionals, in order to reinforce 'digital hygiene' practices"[104]. While this is a step in the right direction, cybersecurity is far from being the only aspect healthcare stakeholders need to be made aware of. To fill these gaps in training, the National Association of Pharmacy Students in France (ANEPF) has drawn up an e-health teaching model that could be incorporated into all healthcare students' initial training. Some of the proposals listed in the document include incorporating a common introductory module on digital health into healthcare students' initial training, creating a set of continuing education courses on digital health that are specific to each healthcare profession, diversifying the range of hospital and industrial internships in order to make students aware of the new digital professions, and encouraging the creation of an e-health master's degree or university diploma[105]. Healthcare professionals must also be given practical support for using certain applications such as business software (security and interoperability guidelines to respect).

In addition to this stepping up of the stakeholders in the healthcare system, and the development of certain professions, there is a more general need for guidance in raising awareness on digital health challenges, and all the more so of health data, among the population as a whole (including the less connected). In this respect, the National Agency for Territorial Cohesion (ANCT)'s initiative to train 3,000 "digital advisors" by June 2022[106] should be highlighted. Once trained, these advisors will be deployed as a priority in *France Services* offices throughout the country. At a time when entire areas of public policy are being digitalised, particularly in the healthcare sector, this digital mediation policy deserves to be massively expanded in order to meet these new challenges.

---

104 French Ministry of Solidarity and Health, « Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie » ("*Security of IT networks in healthcare institutions: the Government is strengthening its strategy*"), Press release, February 22, 2021": https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante

105 French National Association of Pharmacy Students (2021), « Enseignement Supérieur et Numérique. Contribution Innovations Pédagogiques et Évolution des Études de Pharmacie » ("*Higher and Digital Education. Contribution to Pedagogical Innovations and Development of Pharmacy Studies*"), 26 pp.: https://drive.google.com/file/d/117Hnu-IL_cKIdAXEJiTxJiqgCRmN3h27/view

106 « L'Afpa et Simplon.co vont former près de 3000 conseillers numériques d'ici juin 2022, sur tout le territoire », ("*Afpa and Simplon.co will train nearly 3,000 digital advisors by June 2022, throughout the country*"), *Labo Société Numérique*, April 20, 2021: https://labo.societenumerique.gouv.fr/2021/04/20/lafpa-et-simplon-co-vont-former-pres-de-3000-conseillers-numeriques-dici-juin-2022-sur-tout-le-territoire/

A CULTURE THAT WILL ALSO COME WITH PRACTICE

This acculturation also needs to be achieved through usage. As an example, we can cite the StopCovid application, which, because it was initially designed and promoted primarily as a contact tracing tool, failed to be adopted at first. It was only in its second version, TousAntiCovid (the application now includes information on the epidemic, personalised advice, a map of the nearest testing laboratories and vaccination centres, access to travel certificates, information on the eligibility for vaccines, test and vaccination certificates, etc.), that a larger part of the population adopted it. The benefits, in terms of usage, are undoubtedly significant in this adoption. In the same vein, the Estonian "patient portal"[107], equivalent to the future ENS, allows citizens to view their consultation history, their medical analysis results (including Covid tests), their consultation and hospitalisation reports, their vaccination records, the list of treatments prescribed by the healthcare professionals they have consulted, and also to make medical appointments, obtain the medical certificates required to renew their driving licence, and indicate their preferences with regard to their health status (e.g. "In the event of an accident, would you agree to receive a blood transfusion? In case of death, do you wish to donate your organs?" etc.). In France, the ENS, which will be accessible to all citizens from 1 January 2022, is currently under construction. Questions were raised regarding what strategy to adopt. Is it wiser to aim for a gradual approach, initially offering a limited number of services, or on the contrary, focus on massive developments, encompassing many services that concern the entire population, in order to catch up? The Ministerial Delegation for Digital Health (DNS) seems to have chosen the second option. The ENS will be open to all, from birth, on an opt-out basis, and will consist of a general base intended for all. Another option would have been to offer services by pathology, in order to guarantee a certain level of adherence by large communities of patients, before considering extending the services available to the entire population. If the DNS has chosen to create a general base, including many services for all citizens from the start, it will be necessary to ensure that ENS's "massive" approach takes into account the different "types" of citizens. Although the approach is global, support must be progressive and adapted to each individual.

---

107 See: https://www.digilugu.ee/login?locale=en

"MON ESPACE SANTÉ": A TOOL MADE AVAILABLE TO CITIZENS TO ACCESS AND PROVIDE ACCESS TO THEIR HEALTH DATA

The Law of 24 July 2019 on the organisation and transformation of the health-care system provides for the automatic creation of an *Espace numérique de santé* (ENS) for all users of the healthcare system, unless the user or their legal representative objects, by January 2022 at the latest.

Named "*Mon Espace Santé*", this ENS will contribute to the development of France's digital health ecosystem by publishing a catalogue of digital health services developed by public and private stakeholders and referenced by the public authorities (i.e. hospital patient portals, digital services for users developed by software and application publishers and start-ups, applications and connected medical devices developed by manufacturers, etc.).

Through their ENS, users will be able to access:

· their shared medical record (SMR), a secure storage space for health data (medical records, health measurements, vaccination records, medical reports, medical biology test reports, prescriptions, reimbursed treatments, radiology images, etc.);

· a secure messaging system for exchanging information and documents (prescriptions, photos, etc.) with the professionals involved in the patient's healthcare;

· a "health diary" to consolidate various healthcare related appointments: medical appointments, hospitalisations, reminders, etc. These slots can be booked by the appointment booking system, the institutions' portals, and the users themselves;

· a catalogue of services referenced by the public authorities (the ENS "store"): users will be able to choose to give access to data, including health data, from their ENS to applications of their choice and, conversely, to record data from these applications onto their ENS.

Source : sesam-vitale.fr/espace-numerique-de-sante

RAISE THE DIGITAL SECTOR'S AWARENESS OF ISSUES THAT ARE SPECIFIC TO HEALTH DATA

Developing "digital health" (or e-health) solutions is not simply a matter of adopting digital tools or reasoning and applying them to the healthcare sector. It requires a deeper understanding of the healthcare ecosystem and the challenges it faces, which digital technology could potentially address.

"We need to change the perspective from a "digital" angle to a "healthcare" angle. The best way to access the market, before imagining any digital innovation applied to healthcare, is to respond to doctors' and patients' needs"

Yann-Maël Le Douarin,
TELEHEALTH MEDICAL ADVISOR, DGOS (GENERAL DIRECTORATE OF HEALTHCARE PROVISION),
MINISTRY OF SOLIDARITY AND HEALTH

In e-health, the starting point should not be technology, but health. The identification of a specific issue in the healthcare chain should prompt a response based on digital solutions, and not the other way around. This requires efforts to acculturate the digital sector to health-related issues.

As in many other sectors, professions from the "pure" digital world, such as data scientists, are gradually entering the health sphere. However, handling data related to individuals' health requires extremely detailed professional knowledge. It is not only a question of knowing how to interpret the data, but also of understanding the business processes that surround it: Who generates it? Who uses it? For what purposes? For example, in the fight against the Covid-19 epidemic, defining the right metric to certify whether or not the vaccination is going well, requires skills that go beyond data science alone. Should the metric be the number of doses given? The number of second doses? Answering these kinds of questions requires not only sta-

tistical, logistical or data skills, but also healthcare skills (e.g. epidemiology, infectious diseases, etc.).

Furthermore, we shouldn't forget that health data was not initially designed for analysis or research purposes. The data contained in the SNDS, for example, can be particularly difficult to grasp at first glance. Analysing it requires a learning process that can take several months. This dimension is all the more important to emphasise, as the ability to understand this data often plays a major role in obtaining processing authorisations. Thus, requests for access to SNDS data, submitted by individuals who are familiar with the data format and what it can be used for, can be validated within two months. In this respect, health data professionals, who know how to understand this data, could play a role in the acculturation of digital stakeholders to the health sector. This requires building bridges between these two worlds, which work on the same subjects without necessarily meeting each other.

Ultimately, these health data acculturation efforts throughout the healthcare chain should clarify the roles of the various stakeholders involved in digital health. However, while taking control of health data is a major challenge in terms of acculturation, it is also a governance challenge. For the time being, certain technical and legal aspects on which arbitrations must be carried out, make this governance complex.

PART 3
REDEFINE DATA GOVERNANCE FOR A MORE EFFICIENT AND DEMOCRATIC HEALTHCARE SYSTEM
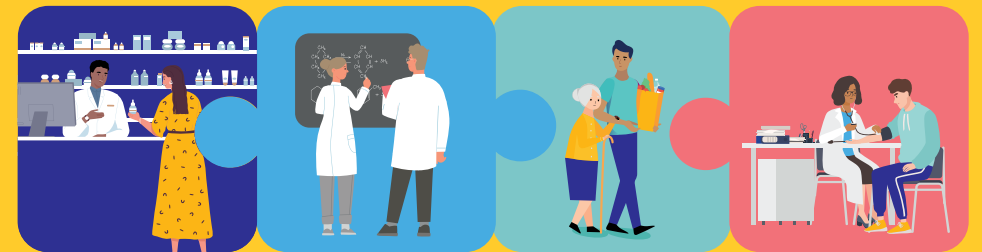
In conjunction with the necessary step-up of all the stakeholders in the healthcare chain on the subject of health data, taking control of this data requires having a greater clarity regarding its governance. Redefining the governance of health data means, on the one hand, clarifying the role of the various stakeholders involved in its production, collection, sharing and use, and, on the other hand, clarifying the methods (technical and legal) of producing, collecting, sharing and using this data.

CLARIFY THE STEERING OF PUBLIC POLICY ON HEALTH DATA

STRENGTHEN THE COLLABORATION OF STAKEHOLDERS INVOLVED IN HEALTH DATA GOVERNANCE

Redefining the governance of health data requires, first of all, clarification of public policy in this area. To be effective, the governance of health data must involve all the stakeholders in the healthcare chain, right down to the citizens, and take into account the interest that this data may have for the various links in the chain. Teaching hospitals, ARS, ministries (and even different entities within the same ministry), healthcare professionals, private complementary healthcare insurances, citizens, patients, patient associations, and industry players do not all have the same relationship with data and do not all have the same uses for it. These different interests must therefore be taken into account, as well as certain specific territorial characteristics.

In the short term, it is important to ensure that dialogue flows between the various stakeholders, and this is partly a management matter. Not all deadlocks are caused by political decisions. Deadlocks also occur because dialogue takes place at sub-optimal hierarchical levels. In order to get the word out between the various stakeholders in the system, a cross-functional task force dedicated to issues related to the processing of health data could be set up, whose role would be to assist stakeholders such as the ARS and the HAS, providing them with specific knowledge to support their step up. This

task force would be a sort of PEReN (digital regulation expertise centre)[108] for health data, but its prerogatives would not be limited to regulatory issues. It could be inspired by the infusion rationale that is emerging in the field of digital regulation, by encouraging emulation between the various stakeholders' different areas of expertise, such as ANSSI, CNIL and health statisticians.

For this multi-stakeholder governance to work, there needs to be more communication between the different stakeholders in the system, and a clear definition of their roles. However, according to the interviews conducted for this study, this is not always the case. While encouraging these stakeholders to cooperate more may be a short-term solution, in the long term, their roles will need to be defined more clearly, which cannot be done by decree, and requires collective arbitration.

ENCOURAGE STAKEHOLDERS IN THE HEALTHCARE CHAIN TO SHARE THEIR DATA MORE EXTENSIVELY

Steering the public policy on health data also means thinking about and setting up mechanisms to encourage the sharing of this data. In particular, this requires the introduction of trusted intermediaries between the stakeholders who are likely to make their health data available, and those who wish to reuse it. Among the forms that these intermediaries can take, there are data trusts[109] (the precise contours of which have yet to be defined). Through a data trust, the data generated by individuals or an entity is entrusted to a third party, the data trustee, who manages it entirely on their behalf, respecting their wishes (with whom to share, for what purpose, etc.). The Health Data Hub is, to some extent, part of this approach, through which the State plays the role of trusted third party for the stakeholders who agree to make their data available via the platform (and therefore, indirectly, for citizens). But despite the efforts made within the "*Ma Santé 2022*" strategy, many health institutions are still reluctant to make their data available through the national platform. At the same time, health data platforms are being created at regional or even inter-regional level

108 PEReN is the "digital regulation expertise centre", a unit with national scope, attached to the Ministries of Culture and Economy, and the Secretary of State for Digital Affairs. Its purpose is to pool expertise in a shared service centre, as the regulation of digital platforms is a cross-cutting issue for many administrations and independent administrative authorities.
109 Open Data Institute, "What is a data trust?", July 10, 2018: https://theodi.org/article/what-is-a-data-trust/

(see Figure 2). These two approaches are not necessarily mutually exclusive and may even complement each other. The development of regional and inter-regional hubs enables health data to be used on a smaller scale than the Health Data Hub. But they can also ensure that the timeframes required to obtain authorisation to process data for research purposes is shorter than if all requests were centralised at national level. Ultimately, what's important is that the initiatives taken on both sides can be brought together. A minimum level of cooperation is therefore necessary between the various health data hubs that are emerging. This can also be a good way of avoiding duplication of initiatives.

> *"We already have a number of large structures that are grouping together in the Grand-Est or Grand-Ouest regions in order to set up regional or interregional data repositories. There must be complementarity between these and the Health Data Hub. The Health Data Hub must rely on the skills and repositories already in place"*
>
> **Cécile Chevance,**
> **DIRECTOR OF THE FINANCE/FHF DATA DIVISION AT THE FÉDÉRATION HOSPITALIÈRE DE FRANCE**
> **(FRENCH HOSPITAL FEDERATION)**

In order to promote a greater flow of public and private data in the European Union, the European Data Governance Act, proposed by the European Commission in November 2020[110] aims to professionalise "data altruism", which the European executive believes is not sufficiently leveraged, and to encourage its widespread use. The text offers the possibility for trusted third parties, acting as intermediaries, to register as "altruistic data organisations recognised in the EU", in order to strengthen trust in their activities. This model is all the more interesting when it comes to exchanging highly sensitive data such as health data. To go further, this proactive approach could be supplemented by providing the third parties in question with a European Commis-

sion certification. Although this possibility has not been included in the text, the Commission doesn't rule it out.

In addition to data trusts, a relationship of trust can also be achieved through contractual solutions. Certain guarantees, notably concerning the nature of the data shared, the intention behind its re-use, possible limits to this re-use, or obligations relating to the transparency of the processing or the responsibilities incumbent on the person in charge, can be included in specific clauses in data sharing contracts. Such practices provide greater protection for both parties, a clearer and more secure communication, and ultimately a greater incentive to share data. For example, one can imagine this kind of clause in a contract between a healthcare professional and their digital solution provider. However, the stakeholders involved don't necessarily have the required expertise to draft such clauses. Moreover, these clauses are not always very clear. In order to overcome these difficulties, the European Commission's Support Centre for Data Sharing offers, for example, legal assistance to stakeholders wishing to set up data sharing. In particular, the organisation has developed a "contractualisation wizard" which, depending on the information provided by the two parties (the purchaser and the data provider), automatically generates a personalised licence agreement for the data sharing in question. A similar system could very well be envisaged at national level, in an inter-ministerial effort, bringing together the various relevant ministries, namely the Ministry of Solidarity and Health (and in particular the Delegation for Digital Health), the Ministry of Higher Education and Research, and the Ministry of the Economy, Finance, and Recovery. The G_NIUS platform (which aims to drive digital innovation in healthcare by accelerating the marketing of new devices), set up by the Ministry of Solidarity and Health, in partnership with the French National Agency for the Safety of Medicines and Health Products (ANSM), the French Public Healthcare Insurance System, Bpifrance, the CNIL, and the HAS[111], could host standard contracts as well as a contractualisation wizard such as that devised by the European Support Centre for Data Sharing.

Developing mechanisms to encourage the sharing of health data also means tackling the data hoarding practices adopted by certain stakeholders in the healthcare chain. In this respect, it is worth recalling the distinction between

110   European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), COM/2020/767 final, November 25, 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

111   The G_NIUS platform aims to stimulate digital health innovations. It offers tools to help entrepreneurs interpret eHealth regulations, identify the ecosystem's stakeholders and their roles, and find out more about accessible sources of funding.

two key concepts: "sharing" data and "giving access" to data. While in the first case users have a physical copy of the data on their server, in the second case, they can only use it through secure access to the producer's server, without keeping a physical copy. In this respect, the "mission for a public data policy" report (known as the "Bothorel mission"), condemns the fact that many stakeholders *"don't even consider the possibility of sharing some of their data in a limited and secure manner"*[112]. This observation once again underlines the importance of educating all those involved in the production and processing of health data. The problem is not specific to healthcare, and concerns all ecosystems based on data sharing between stakeholders. However, the health sector remains one in which the idea of data valorisation is not well regarded. There are also technical solutions that allow data from multiple sources to be used without the user having direct access to it. This is the case, for example, with multi-party machine learning. This technology allows several entities that wish to collaborate to train an artificial intelligence model, to produce a model by pooling their data, but without each stakeholder having access to its partners' data. The use of techniques known as "confidential computing" can also be of interest. Confidential computing is based on the capabilities of the latest generation of processors and, thanks to an encryption process, allows data to be shared without giving access to it. Such solutions should be encouraged by the public authorities in order to remove the reluctance of certain stakeholders to share their data.

MAKE SURE THE NATIONAL PUBLIC POLICY TAKES INTO ACCOUNT THE EUROPEAN STRATEGY ON HEALTH DATA

The French public policy on health data must also take into account the European strategy in this regard, which will be widely developed in the coming years.

In April 2018, the European Commission issued a communication on the digital transformation of health and healthcare services in the digital single market[113]. It has three objectives: secure access to health data for citizens and sharing of health data with other Member States, improve data quality to drive research forward, for disease prevention, and personalised healthcare, and promote digital tools for citizen empowerment and person-centred care. In line with this statement, the EU executive adopted a recommendation on the European format for the exchange of electronic health records[114]. The idea is to promote the exchange of electronic health records between Member States by encouraging the development of a common exchange format. While 22 Member States are expected to be able to exchange these types of documents by the end of 2021 through the dedicated eHealth Digital Service Infrastructure (eHDSI), only Finland and Estonia have achieved this so far. It is therefore essential that the development of national platforms, such as the future French ENS, which will enable all citizens to access their medical records, take into account European requirements in terms of format interoperability. Under the European National Contact Point eHealth (NCPeH) project, it is also expected that by the end of 2021, any healthcare professional in the European area will be able to access the medical records of patients who are citizens of another country. In France, the Digital Health Agency (ANS) has been designated as the national contact point for e-health. As such, it is connected to the European Commission's coordination services, and will act as an intermediary between requests from NCPeHs in other countries, and national infrastructures such as the ENS.

In addition to documents (e-prescriptions, reports), the requirement for interoperability also applies to the format of health data in general, some of which should be able to be integrated into the future common European health data space. In this respect, it should be noted that, through the Health Data Hub, France is taking part in the European Health Data Space joint action (or TEHDaS) launched on 1 February 2021, which brings together the European Commission and 26 Member States. The purpose of this initiative is, through the sharing of knowledge between the various stakeholders involved, to produce recommendations for the implementation of the future platform for sharing health data at a European level. Finally, the

112 Bothorel mission, « Pour un politique publique de la donnée » ("*For a public policy on data*"), December 2020, p. 9: https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf

113 European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM (2018) 233 final, April 25, 2018, 14 pp.: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0233&from=EN

114 European Commission, Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format, February 6, 2019, 10 pp.: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0243&from=EN

governance of health data at national level will have to take into account the Data Governance Act, which aims to improve the conditions for data sharing in the internal market by creating a harmonised framework for data exchange.

Although French public policy on health data is already well embedded in the European strategy, the stakeholders who remain reluctant to use international interoperability standards have yet to understand this need.

MAKE ESSENTIAL TECHNICAL AND LEGAL CHOICES

STRENGTHEN THE ADOPTION OF TECHNICAL INTEROPERABILITY AND SAFETY STANDARDS

As mentioned in the first section of this report, the heterogeneity of health data is one of its main characteristics. It constitutes a heritage scattered within a multitude of different databases, which often operate in silos in relation to each other, and are managed by a wide variety of stakeholders. Each stakeholder has thus adopted, over time, its own information systems and its own software and procedures for collecting and processing data. The data is therefore not always standardised, which greatly limits its use.

"Today, digital health data exists mostly in an "unstructured" format, which is detrimental to the exploitation of high added-value business data. Health information systems are evolving towards data production and exchange, particularly in the context of the "Health Data Hub", which means that governance and practical tools must be put in place to structure digital health data and code it semantically."

French National Strategic Roadmap for Digital Health

From the point of view of the technical arbitrations that need to be made, the challenge is therefore, first of all, to facilitate the matching of this data from different databases, without overlooking the security and confidentiality precautions that this sensitive data requires (see the section of this report entitled "A strict legal framework, which acts as a guardian"). For the stakeholders taking part in the collection of health data (healthcare professionals and establishments, software publishers, healthcare industry players, French Public Healthcare Insurance System, etc.), this means complying with basic standards in terms of security, interoperability and ethics (see Figure 3). In France, responsibility for developing these standards lies mainly with the Digital Health Agency (ANS).

The use and widespread implementation of a National Health Identity (INS) is one of the key measures of the government's "*Ma Santé 2022*" strategy. The INS is an identifying number (each individual has an INS), which allows any patient to be recognised in all IT systems in a unique way, thus ensuring healthcare continuity. Its use has been compulsory since 1 January 2021 and the INS is now the key for matching people: all health data must be referenced with an INS number. Despite this compulsory requirement, it would seem that this reference system is struggling to be adopted. The meetings organised in the context of this report revealed that, almost six months after the requirement came into effect, its use was not systematic. For example, it is not used for all internal activities within the French Public Healthcare Insurance System. Because of the technical difficulties involved in switching from one reference system to another, there is a general reluctance on the part of some healthcare institutions and professionals to adopt this new reference system. While its creation has mobilised many stakeholders in the healthcare system for several years, the challenge is now to move towards mass adoption of the INS. The Digital Health Agency (ANS) is working on this, and recently launched a communication campaign on this subject, notably via social networks[115]. Regional action plans are also being coordinated by the Regional Health Agencies (ARS), the Regional Support Groups for the Development of e-Health (GRADeS) and the Risk Management Coordinating Directors (DCGDR), with the aim of ensuring that the INS is used in at least 80% of communications between healthcare professionals by the end of 2022.

115 For example, via LinkedIn: https://www.linkedin.com/posts/agence-du-numerique-en-sante_lidentifiant-national-de-sant%C3%A9-devient-l-activity-6785933231482126336-kuoo/

In addition to the INS, which serves as a security reference, the Digital Health Agency (ANS) has also developed a framework for the interoperability of health information systems (CI-SIS)[116], which aims to encourage "*the dematerialisation and homogenisation of information exchanged and shared, while respecting the autonomy of health information systems*"[117]. The CI-SIS is a reference document, which proposes technical and semantic rules for publishers and digital health project developers, in order to promote the sharing and exchange of health data. In other words, the aim is to ensure that the various stakeholders speak the same language, which, in the end, should greatly facilitate data matching. In this respect, the Digital Health Agency asks industry players to fill in the Convergence tool[118] to assess their compliance with this framework.

FIGURE 5 - THE BASIC STANDARDS APPLICABLE TO HEALTH DATA IN FRANCE

Source : esante.gouv.fr

*Online solution that offers universal access to all e-Government platforms
**National authentication service for healthcare professionals
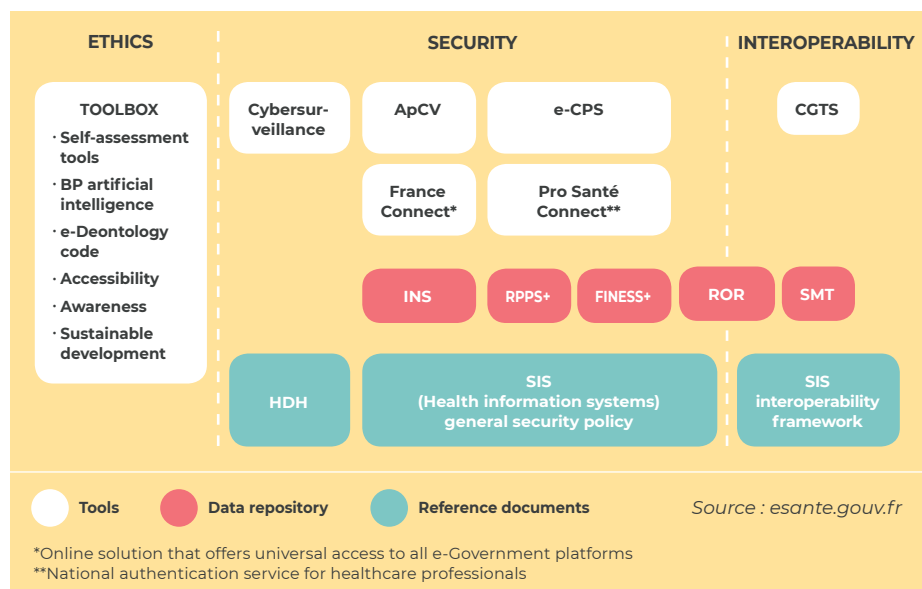
Although the coming into effect of these standards is already an achievement, a sustained level of incentive must be maintained to ensure that they are adopted on a massive scale. Levers have been designed precisely for this purpose. With regard to the digital infrastructures of healthcare institutions, the incentive can be provided in particular by requiring them to comply with the interoperability standards in their calls for tenders. The interoperability obligation also applies to manufacturers of software and connected medical devices. The HAS and the French Healthcare Products Pricing Committee (CEPS), which negotiates the prices of these tools, are very attentive to compliance with these provisions and tend to make it an evaluation criterion. Lastly, we should not forget primary healthcare professionals, who are also affected by incentives to comply, particularly with regard to their business software. In order to help them modernise and computerise their practices, the French Public Healthcare Insurance System has introduced the 'structure package', a two-part financial incentive that can amount to a maximum of €6,195 per year[119]. The indicators used for the payment of this incentive include having a business software with prescription assistance tools (LAP) certified by the HAS and compatible with the use of shared medical records (SMRs). If this criterion is not met, the healthcare professional cannot receive the first part of the incentive (which requires five cumulative indicators to be met), which for 2020 amounted to €1,960€[120]. In addition to equipment, this "structure package" takes into account the use of various "digital health" tools, like for example the percentage of medical claim forms or sick leaves processed electronically.

Finally, in accordance with Article L-1111-8 of the Public Health Code, and in order to guarantee the security of health data as much as possible, "*any person who hosts personal health data, collected during preventive, diagnostic, treatment, or social and medico-social monitoring activities, on behalf of the natural or legal persons responsible for producing or collecting this data or on behalf of the patient himself*" must be approved or certified for this purpose. More specifically, these intermediary stakeholders, who may for example subcontract the hosting of health data on behalf of a hospital, are

---

116 See: https://esante.gouv.fr/interoperabilite/ci-sis

117 ANS, « Interopérabilité, pierre angulaire de la croissance en e-Santé » ("*Interoperability, the cornerstone of growth in eHealth*"): https://esante.gouv.fr/interoperabilite

118 See: https://convergence.esante.gouv.fr/

119 See: https://www.ameli.fr/paris/medecin/exercice-liberal/vie-cabinet/aides-financieres/modernisation-cabinet

120 CNAM, Methodological Guide, Structure package 2020, Medical agreement of August 25, 2016, 28 pp.: https://www.ameli.fr/sites/default/files/Documents/489483/document/note-metodo-forfait-structure-2020.pdf

required to host the data on "health data host" (HDH)[121] certified (new procedure) or accredited (old procedure) servers. The 2020 progress report of the strategic roadmap for digital health mentions 125 HDH hosts that have been approved by the ANS. Although some healthcare institutions are themselves HDH certified or approved (e.g. AP-HP, Marseille Teaching Hospitals (AP-HM), Thuir Hospital, Nantes Teaching Hospital, Nîmes Teaching Hospital), this is not the norm. Healthcare establishments, territorial hospital groupings (GHT), medical laboratories, and other organisations likely to produce or collect healthcare data are not subject to this obligation if they host this data on their own behalf. In view of the increasing number of cyberattacks on healthcare institutions' information systems (IS) in recent months, this lack of obligation may raise questions. Of course, there is no such thing as zero risk, and cybersecurity in the area of health data, as in any other sector, is not just a matter of technological devices. Flaws are often found "between the chair and the screen", and the security of healthcare information systems is monitored on a daily basis. An HDH certification, in addition to compliance with the general policy on the security of healthcare information systems (PGSSI-S)[122], contributes to a significant increase in the security level of healthcare information systems. Although the public authorities are gradually becoming aware of this, the scope of their efforts is limited for the time being. Among the measures in the plan aimed at strengthening the security of healthcare institutions' IT networks, we can highlight the fact that "*no project can henceforth be supported by the State if 5 to 10% of its IT budget is not dedicated to cybersecurity*"[123]. However, beyond the budget thresholds allocated to cybersecurity, it is important to think about how the adoption of HDH status can be encouraged and supported. During their speech, the two ministers emphasised that the Regional Health Agencies (ARS) will be responsible for helping establishments to comply with the new cybersecuri-

ty obligations[124]. Renaissance Numérique recommends going further, by imposing on health establishments and GHTs the obligation to be HDH certified or to use HDH certified hosts. The need to align cybersecurity certification with the HDH standard is all the more critical, given the authorities' desire to develop interoperability. This interoperability will only be able to develop if the same security level is guaranteed between the services that have to exchange health data with each other. For example, let's suppose that a doctor uses tool "A" (HDH certified) and decides to extract a report and upload it to another tool, tool "B" (which is not HDH certified). This would compromise the efforts made by the service "A" since, in the end, the data would end up in a non-HDH certified space. It is thus urgent that all stakeholders, including healthcare institutions, comply with HDH certification.

Gradually, the various standards developed by ANS should thus be massively adopted. But it is not a question of simply "letting time take its course". Complying with these existing standards must not simply be a "best practice". While all these guidelines are intended to be legally enforceable, some are only recommendations (when an official order has not made them enforceable). In such cases, compliance incentives for the various stakeholders concerned should be maintained, or even intensified.

MOVE TOWARDS A FRAMEWORK THAT IS BOTH MORE PROTECTIVE OF AND CONDUCIVE TO HEALTH INNOVATION

IMPLEMENT A MORE AGILE REGULATION

Due to its sensitivity, health data is subject to a particularly strict legal regime. In France, certain national provisions have been added to the European framework (GDPR) and lead to greater legal security. Thus, while the GDPR allows for reduced formalities prior to authorising data processing (by making data controllers responsible for proving that their use of the data complies with the regulation), this possibility is limited by the Data Protection Act. According to Article 66 of the text, the simplified procedure cannot be applied to data processing for research purposes (one of the exceptions men-

---

121 See: https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante
122 Since 2012, the general policy on the security of healthcare information systems (PGSSI-S) has been setting the security requirements for digital services in the healthcare sector. Developed by the Delegation for Health Information Systems Strategy (DSSIS) with the support of the Digital Health Agency (ANS), it brings together requirements standards and best practice guidelines, and proposes a common framework for the IS security level in the healthcare sector.
123 French Ministry of Solidarity and Health, « Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie » ("*Security of IT networks in healthcare institutions: the Government is strengthening its strategy*"), Press release, February 22, 2021: https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante

124 With regard to the compliance of stakeholders in the medico-social sector, the modalities were being developed by the French Ministry of Solidarity and Health at the time this report was written.

tioned in Article 9 of the GDPR). Nor does it apply to processing operations for a public interest purpose. However, where the legal basis for the processing is consent, for example, the simplified authorisation procedure may apply. In order for the processing to be lawful, data controllers must nevertheless set up a register of processing operations, carry out impact assessments, ensure that data subjects are informed, formalise their roles and responsibilities, appoint a data protection officer (in cases where this is compulsory) and provide information on the measures taken to guarantee data security[125].

Despite CNIL's publication of several practical factsheets (on processing registers, impact assessments, informing individuals, use of subcontractors, etc.), it emerged from the series of interviews conducted for this report that the legal framework for health data processing remains difficult to interpret. In particular, its multiple levels of interpretation sometimes lead to some project leaders not applying it strictly, which may ultimately lead some of them to abandon their projects or postpone them. This non-compliance with the legal framework may also have harmful consequences on citizens' data protection. There are requests for more clarity on the interpretation of the GDPR, and what does and doesn't fall within the set of exceptions it proposes. On 16 March 2021, the European Parliament's Civil Liberties Committee (Libe) adopted its resolution on the two years of GDPR application[126]. In the resolution, MEPs call on European data protection authorities and the European Data Protection Board (EDPB) to produce clear guidance on the proper implementation of the GDPR in public health policies. The group also asks that the application of the Regulation by SMEs be simplified. In order to reconcile the protection of individuals and innovation, clarity on the interpretation of the legal framework surrounding the processing of health data is necessary.

In particular, some project leaders feel that, as it is interpreted at the moment, this legal framework requires them to know in advance what they will be looking for and what they will find. If we take the example of the processing of health data for research purposes, for each request it receives, the CNIL analyses the "*necessity to use personal data*" and "*the relevance of the processing in relation to its declared purpose*". These are two aspects that

can be difficult to anticipate. Similarly, it is particularly complex to identify all the risks that may arise during the course of the research. Some risks also appear along the way, without it being possible to anticipate them. In order to encourage innovation while maintaining a very high level of protection for individuals and their data, Renaissance Numérique encourages the implementation of regulatory sandboxes for research projects requiring the processing of personal data related to health. This procedure could allow project leaders to carry out their research through auditable mechanisms, under the constant scrutiny of regulators. In order to ensure maximum protection of the data processed, and compliance of the project with the GDPR, this process would require the regulators involved to be able to monitor, on a regular basis, how the research is carried out, which implies full transparency of the process.

While they are used in some European countries such as Germany and the UK, regulatory sandboxes have never been the subject of a real public debate in France. On 15 February 2021, the CNIL announced the creation of a "GDPR sandbox to support innovative projects in the field of digital health"[127]. Intended to facilitate innovation in the health sector, this initiative aims to "*select applications that highlight or establish good sectoral practices (resolution of a new or important legal issue or definition of technical choices, thus clarifying the CNIL's doctrine)*"[128]. However, the aim should be to give project leaders the necessary leeway to conduct their research (including by waiving certain obligations, within the framework of the sandbox), while complying with the rules on personal data protection. The benefits of setting up a regulatory sandbox will remain limited if it doesn't allow this degree of flexibility.

OVERCOME CULTURAL BARRIERS IN ORDER TO LEVERAGE REAL-WORLD DATA

In connection with innovation in the healthcare sector, a specific kind of data could be used to a greater extent, especially in France, where it is not used enough: "real-world" data. This category includes data that is not collected in an experimental context, but which is generated in day-to-day clinical

125 CNIL, « Quelles formalités pour les traitements de données de santé à caractère personnel ? » ("*What are the required formalities for the processing of personal health data?*"): https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel
126 "Civil Liberties Committee calls for further improvements to the GDPR implementation and strengthened enforcement", European Parliament News, Press release, March 16, 2021 : https://www.europarl.europa.eu/news/fr/press-room/20210311IPR99708/civil-liberties-committee-on-the-gdpr-implementation-and-enforcement

127 CNIL, « Un « bac à sable » RGPD pour accompagner des projets innovants dans le domaine de la santé numérique » ("*A GDPR "sandbox" to support innovative projects in the digital health*"), February 15, 2021: https://www.cnil.fr/fr/un-bac-sable-rgpd-pour-accompagner-des-projets-innovants-dans-le-domaine-de-la-sante-numerique
128 *Ibid.*

practice, particularly during routine healthcare treatments, but also outside of treatments. This data is usually collected by medical devices (MDs) or by connected objects and digital applications. In a report published in May 2017, commissioned by the Minister of Health, Marisol Touraine, Bernard Bégaud, Dominique Polton and Franck von Lennep already highlighted the fact that real-world data represented "*major stakes in terms of quality of healthcare, system efficiency, and intelligent regulation*", but that France was not "*measuring up to the challenge*"[129].

However, greater use of real-world data would enable more efficient funding and reimbursement of medical treatments and devices. For example, the reimbursement of medication by the French public healthcare system currently depends on its "therapeutic value" (TV), as defined by the French National Authority for Health (HAS) during the evaluation of each medication[130]. The TV may be classified as "major or important" (in which case the medication is reimbursed at 65% by the French Public Healthcare Insurance System), "moderate or low" (in which case the medication is reimbursed at 30% by the French Public Healthcare Insurance System) or "insufficient" (in which case the medication is not reimbursed). Medications considered irreplaceable and particularly expensive (e.g. those used in the treatment of long-term illnesses, AIDS/HIV or cancer) have a 100% coverage by the French Public Healthcare Insurance System[131]. In the absence of available data from randomised[132] clinical trials[133], instead of issuing an unfavourable decision on reimbursement, the HAS could, for example, make more frequent use of real-world data to determine the conditions for one-off and derogatory reimbursements, on

condition that the manufacturer provides real-world data demonstrating the clinical interest and efficacy of the medication or device. This would make the reimbursement of treatments and medical devices conditional on their effectiveness, as observed in "real life". The latest "expenditure and income" report by the French Public Healthcare Insurance System particularly recommends following this path for connected medical devices, stressing that "*the uncertainty generated by these devices suggests the need for a more flexible approach, that takes into account the effectiveness of the device throughout its life cycle*"[134]. While the HAS sometimes gives conditional assessments with post registration studies (EPI) as part of the renewal of device reimbursement after three to five years, this is currently seldom the case for first-time registrations. However, recent announcements by the HAS National Commission for the Assessment of Medical Devices and Health Technologies (CNEDiMTS) suggest that the authority is gradually moving towards greater use of real-world data in its assessments.

Furthermore, the analysis of healthcare effectiveness is currently based mainly on measurements taken outside the context (in a hospital or medical practice), and on measurements based on patients' self-reporting over the past months. However, when the doctor asks the patient about the past months, the patient is often not able to give a detailed summary that is relevant, which is to be expected. Similarly, a cardiologist, for example, doesn't need one heart rate measurement at a given time, but several measurements under "normal" conditions (i.e. in everyday life, outside the hospital where the measurements may be biased by the stress of exercise). If, in addition to the measurements made in hospitals or medical practices at a given time, it was possible to rely on regular measurements (e.g. once a week instead of once a year), the analysis of healthcare effectiveness would take on a new dimension.

This data could also be very useful for prevention purposes, for example, by identifying early signals that would enable the medical professionals to act before the acute phase of an illness. For the time being, it would seem that a more extensive use of real-world data in healthcare pathways is facing an acceptability issue, both for healthcare professionals (who are not all aware

129 Bégaud, B., Polton, D., von Lennep, F., « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé. L'exemple du medicament » ("*Real-world data, a major issue for the quality of healthcare and the regulation of the healthcare system. The example of medication*"), May 2017: https://solidarites-sante.gouv.fr/IMG/pdf/rapport_donnees_de_vie_reelle_medicaments_mai_2017vf.pdf

130 French National Authority for Health, « Le service médical rendu (SMR) et l'amélioration du service médical rendu (ASMR) », ("*Therapeutic value (TV) and improvement of the therapeutic value (ITV)*"), April 16, 2013: https://www.has-sante.fr/jcms/r_1506267/fr/le-service-medical-rendu-smr-et-l-amelioration-du-service-medical-rendu-asmr

131 French Public Healthcare Insurance System, « Tableaux récapitulatifs des taux de remboursement », ("*Reimbursement rates summary tables*"), January 6, 2021: https://www.ameli.fr/paris/assure/remboursements/rembourse/tableau-recapitulatif-taux-remboursement/tableau-recapitulatif-taux-remboursement

132 See: Wikipedia, "Randomized controlled trial": https://en.wikipedia.org/wiki/Randomized_controlled_trial

133 A clinical trial, or clinical study, or therapeutic trial, is a scientific study conducted in human medical therapeutics to evaluate the efficacy and safety of a diagnostic method or treatment. Depending on the type of study, and the stage of drug development, investigators enrol healthy volunteers or patients.

134 French Public Healthcare Insurance System, « Améliorer la qualité du système de santé et maîtriser les dépenses - Propositions de l'*Assurance Maladie* pour 2021 » ("*Improving the quality of the healthcare system and controlling expenditure - French Public Healthcare System's proposals for 2021*"), Report to the Social Security Minister and Parliament on the evolution of the French Public Healthcare Insurance System's expenditure and income for 2021 (Act of 13 August 2004), July 2020, p. 211: https://assurance-maladie.ameli.fr/sites/default/files/2020-07_rapport-propositions-pour-2021_assurance-maladie_1.pdf

of these issues) and for patients (for whom the procedures are not always sufficiently transparent).

The question of using real-world data also arises in the evaluation of medical treatments and devices when they are launched on the market. As mentioned earlier (see section "An ecosystem that is difficult to grasp in its entirety"), the marketing of medical devices (MDs) is subject to strict rules. The same is also applicable to medications. In France, the French National Authority for Health (HAS) is in charge of assessing medications and medical devices that may be reimbursed on an individual basis. As mentioned above, in order to obtain a favourable opinion, the manufacturers of potential innovative healthcare products must provide data from randomised clinical trials to prove the effectiveness of their solution. Although they involve relatively small cohorts of patients (usually a few hundred), but also over a short period of time (3-6 months), randomised clinical trials remain the norm. Real-world data, on the other hand, collected through connected medical devices or dedicated applications, is sometimes related to several hundred thousand people, or even millions. However, it emerged from the interviews conducted as part of this study that manufacturers who include real-world data in their assessment applications for the HAS sometimes feel that this data is not regarded as being of the same quality as data from randomised studies.

While the question is not whether real-world data can replace data from clinical studies, it is worth considering whether they are complementary. Rather than opposing them, and reserving each one for separate uses, we should consider that each of them has its limits and its virtues. Where do the barriers and reluctance to use of real-world data more systematically in the evaluation of medications and medical devices come from? Are there legal barriers to their use? Technical barriers?

It would seem that the answer is a mixture of technical and cultural barriers, with the limitations not in fact being related to legal issues. Some barriers still exist from a technical point of view, particularly in terms of data interoperability. Furthermore, some stakeholders question the quality and reliability of real-world data, while others question the capacity of randomised clinical trials to answer these questions. Another reason that often came up during the interviews conducted for this report was the persistence of cultural obstacles, which are said to stem in part from the French regulator's doctrine. Some European countries, such as Belgium, Spain, and the United Kingdom, place greater emphasis on these issues. As mentioned

in the latest communications from the CNEDiMTS[135], the HAS is nevertheless working on a methodological guide on the studies that are considered in the assessment of medical devices and health technologies. This guide, which is intended to be shared with the concerned industry actors, aims to clarify the commission's assessment principles. This initiative should make it possible to reaffirm the CNEDiMTS doctrine concerning the consideration of real-world data, and thus clarify this issue for certain stakeholders in the chain, in particular manufacturers of medical devices. However, medical devices and health technologies only represent a part of the healthcare offer that is assessed by the HAS. What about, for example, the use of real-world data in the assessment of medications? In order to overcome the current relative vagueness, Renaissance Numérique calls on the stakeholders concerned to place the issue of real-world data use at the heart of the public debate. With regard to their use for the evaluation of medications and medical devices, it would also be useful for the HAS to formalise its doctrine on the matter. Regarding the first point, it should be noted that the General Economic Council, in its public consultation "Structuring the e-health sector", introduced a section entitled "Controlled circulation of data, AI, and research", in which it proposes to "allow a wider use of real-world data in compliance with the GDPR"[136].

It seems essential that the above-mentioned elements be taken into account in the proposal to create a Health Innovation Agency, recently announced by the French Ministry of Solidarity and Health.

PUT CITIZENS AT THE HEART OF HEALTH DATA GOVERNANCE

Redefining the governance of health data should be an opportunity to put citizens at the heart of the process. The growing use of health data in healthcare and research affects the entire population, young and old, people with diseases and those in good health. However, patients' associations are very often recognised as the only entities representing the population with sufficient legitimacy to be

---

135 See in particular the agenda for the meeting of the HAS deliberative board of 10 June 2021: https://www.has-sante.fr/upload/docs/application/pdf/2021-06/2021_06_04_odj_cd_2021_06_10_vd_signe.pdf

136 General Economic Council, Online survey dedicated to the structuration of the eHealth sector: https://forms.office.com/Pages/ResponsePage.aspx?id=00mEUDLWm0KXzvitIrOn55_p8Ud_bjF-Pu7kQtfHA8h1UQTlOTVI2TVdCSUNSUk9XN0Y0OTRDQTNFOC4u

heard by health authorities. Beyond patients and patient organisations, citizens as a whole should be given a greater role in the development and implementation of public health policy.

TOWARDS GREATER TRANSPARENCY AND A BETTER CONSIDERATION OF CITIZENS' EXPECTATIONS WITH REGARD TO PUBLIC HEALTH

As mentioned in the "Bothorel mission" report published in December 2020, "*data is a means of correctly assessing our public policies. On the one hand, using data is only ever going to make the good old management control system more reliable and allow it to be used in real time; on the other hand, it's also a way of monitoring the implementation of public spending.*"[137] In order to encourage a shift in the way things are done in this respect, the plan to transform public action, which is in line with the above-mentioned mission, invites all ministries to tackle the question of their data. Among the three priority areas identified for the 2021/2022 period, the first is that of the management and governance of public data. More specifically, the aim is to open up the public data held by the various ministries, with a view to improving the management of policies and enabling greater transparency in public action. The plan also envisages that new public policies will be included in the barometer of public action results launched by the government in January 2021[138]. Thus, for a set of thirty-six policies deemed to be priorities, each citizen will be able to find out, on the government's website, the actions' status and the objectives to be achieved by the end of the presidential term, whether at a national level or in each county. This approach should, in the end, enable the existing gap in feedback on the various health reforms undertaken at national level to be partly filled. For the time being, it is extremely difficult to accurately qualify and quantify the benefits brought by these reforms to citizens and to the healthcare system as a whole, both at a national level and in local territories.

It is also urgent to ensure that citizens can take part in the debates that shape and set public health policy objectives. As previously mentioned, our healthcare system's digital transformation raises ethical, economic, technical, and legal is-

sues that are a matter of collective choice. Citizens must be invited to give their opinion on these issues, especially since, as was the case in the fight against the Covid-19 pandemic, certain public health priorities can clash with individual freedoms such as freedom of movement. Although public health policy is largely developed within the National Assembly, it is mainly based on the guidelines set by the French Public Healthcare Insurance Funds (CNAM) in its "Report on expenditure and income", which is submitted annually to the government and parliament. These consist of an analysis and concrete proposals aimed at improving the quality of the healthcare system and controlling its expenditure[139]. These reports are the basis for the annual Social Security Financing Bills (PLFSS), which focus on the French Public Healthcare Insurance System's budget. Citizens are not consulted on what they expect from the healthcare system, and there is no real debate on the overall direction of public health in France. Recent work by the High Council for the Future of the French Public Healthcare Insurance System (HCAAM), however, suggests the possibility of moving towards more democratic health strategies, with PLFSS being the annual variations of public health guidance plans voted at the start of each five-year term[140]. As the "*Ma Santé 2022*" reform draws to a close, the time has come to think about the strategy to be adopted over the next four to five years. The opportunity must then be taken to involve citizens more widely in this process than has been done in the past. In this respect, in addition to patients' associations, consumers' and users' associations must develop their skills in these matters, in order to give citizens a greater voice in these debates.

Greater transparency in the choices made, and in the priorities set, by certain bodies such as the French Public Healthcare Insurance System or the Health Data Hub could also help to place citizens' concerns at the heart of health data-related issues and, ultimately, strengthen health democracy. Citizens could, for example, be invited to contribute to the priority setting of the French Public Healthcare Insurance System or the research priorities of structures like the Health Data Hub. However, this requires that these stakeholders communicate regularly and in an easy-to-understand way on the objectives they are pursuing, the research programmes that are in progress, what pathologies are being targeted, and the concrete results of their actions. It also requires a certain amount of proactivity on citizens' behalf, in particular, efforts to access this information. In order to complement these initiatives, it would be a useful exercise to set up

137 Bothorel mission, *Ibid*., p. 7: https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf
138 French Government, « Lancement du baromètre des résultats de l'action publique » ("*Launch of the public action results' barometer*"), January 13, 2021: https://www.gouvernement.fr/lance-ment-du-barometre-des-resultats-de-l-action-publique

139 For more information, see: https://assurance-maladie.ameli.fr/qui-sommes-nous/publica-tions-reference/assurance-maladie/rapports-charges-et-produits/rapport-charges-produits
140 See, in particular, the HCAAM's (High Council for the Future of the French Public Healthcare Insurance System).

consultation mechanisms based on representation, so that the citizens' voices can be heard on specific matters (for example, the deployment of new digital health services by the public authorities, etc.). For such initiatives to be truly successful, however, particular attention must be paid to the decision-making processes that result from them, in order to ensure that the expectations formulated by citizens are respected, and to avoid any disappointment.

STRENGTHEN CITIZEN REPRESENTATION IN HEALTH DATA GOVERNANCE BODIES

It is also important that citizens be more involved and better represented in certain health data governance bodies. Of the fifty-six founding members of the Health Data Hub, only one, the National Union of Approved Associations of Healthcare System Users (France Assos Santé)[141], represents citizens. With a few rare exceptions, such as UFC Que Choisir (French consumer organisation), the National Council of Secular Family Associations, and of the Consumption Housing Living Conditions Association, France Assos Santé is made up almost exclusively of patient associations. It is therefore essentially citizens suffering from pathologies who are represented in the Health Data Hub's bodies, and through a single "voice". What about healthy citizens? The agreement between the hub's founding members doesn't exclude new memberships[142]. In order to ensure that citizens' voices are heard in this organisation, it would be beneficial, in the near future, to broaden this representation and to include civil society associations, particularly right defenders.

THE POSSIBILITY FOR CITIZENS' DIRECT INVOLVEMENT IN IMPROVING THE HEALTH-CARE SYSTEM THROUGH DATA REPORTING

Beyond this macro level, it is important to involve citizens in the health data issues that are most closely linked to their daily lives. This means, in particular, providing more information and raising awareness within the framework of healthcare pathways. Although the benefits of collecting and using health

data are generally accepted by professionals in the sector, they are not yet widely known by the general public. Each stage of the healthcare pathway should therefore be an opportunity for the various stakeholders involved to inform the public about how their data can be used to improve the healthcare system as a whole, about their rights, and about the guarantees (in terms of security, confidentiality) that surround the sharing of this data. Whenever possible, and if they so wish to, citizens should be able to share their data, for example in order to contribute to medical research programmes of their choice, or to the evaluation of medical procedures, in a contributory approach. As already mentioned, it is indeed through practice that citizens will gradually become familiar with the issues underlying health data and their use.

This reporting from the field would also enable a better understanding of the impact of public health policies on the entire territory. This would contribute to the regulation of the healthcare system "through data" and would allow citizens to actively take part in its governance, in a bottom-up approach. In this respect, Renaissance Numérique encourages a "platformisation" of the healthcare system regulation. This could, for example, be achieved by setting up alerts, or sending out forms via *Mon Espace Santé*. Simple universal indicators (treatment times, number of inpatient hospital stays, presence or absence of a quality proximity service, etc.) could be set up, which citizens would be asked to give their opinion on. By taking part in the assessment of healthcare quality in this way, citizens take ownership of their own healthcare, and contribute to improving the system as a whole. If, thanks to the reporting thus accumulated, we realise that, in a given territory, for a given pathology, it takes two years to obtain an appointment, then we will have identified a problem, and we can provide the necessary resources to solve it. However, this initiative would require that the bodies that contribute to the regulation of digital health, such as the French National Authority for Health (HAS), the Ministry of Solidarity and Health, the French Public Healthcare Insurance System, and the ARS, be equipped with the capacity to process this information and take it into account when defining public health objectives. Data feedback at all levels of the healthcare system should also make it possible to identify regional particularities which could enable the system's local governance bodies (particularly the ARS) to become more effective.

---

141 Gérard Raymond, President of *France Assos Santé*, is also Vice-President of the Health Data Hub.
142 Subject to approval by a qualified majority of two-thirds of the voting rights of the members of the General Assembly.

While the work already done to clarify the governance of health data should be emphasised, the efforts made, in particular by the Digital Health Delegation and the Digital Health Agency (ANS), in terms of education, but also in terms of the development of basic reference systems, must be continued and stepped up. While various initiatives have just been launched or will be launched in the near future, it is not too late to give ourselves the necessary means, and to place the citizen at the heart of the system.

CONCLUSION
CITIZENS AS PILLARS OF THE EUROPEAN DIGITAL HEALTH SPACE

It is impossible to ignore the changes that are currently taking place regarding the use of data in the healthcare system. Driven by the "*Ma Santé 2022*" strategy, the "digital shift" in healthcare, reinforced by the Covid-19 crisis, is gradually gaining ground every day. The 2020-2021 period will have been the turning point in this respect, with an explosion in the number of teleconsultations[143], the launch of the Health Data Hub, and the implementation of the "*Mon Espace Santé*" pilot phase in three French departments (Haute-Garonne, Loire Atlantique, and Somme). But these changes will only be truly beneficial if citizens manage to embrace them. In addition to an improved implementation of existing technical standards (particularly in terms of cybersecurity and interoperability), this still requires serious efforts to educate all the stakeholders in the healthcare chain, including citizens. "Getting to grips" with health data must also involve familiarisation with this data at a micro level, on a daily basis, particularly within the various stages of the healthcare process. Ultimately, these developments should aim not only to make the healthcare system more efficient, but also to place the citizen at the heart of the system.

This commitment to developing tools that are useful and beneficial, above all to citizens, is reflected in the European Commission's recent announcement, regarding its strategy for a European digital identity[144]. The aim of the future European digital identity portfolio, announced at the beginning of June 2021, is to enable all citizens and residents to identify themselves digitally, and to store and manage sensitive data, including health data, and official documents in an electronic format. This initiative is part of the regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) and aims to tackle the disparities between Member States in terms of digital identity.[145] At the same time, the work of the joint action, launched by the European Commission, to define the contours of the future European Health Data Space is ongoing, with a legislative proposal and a pilot project expected by the end of 2021 or the beginning of 2022. Therefore, while the current challenge is to get up to speed at national level, the next step will be to think about where

citizens stand in the European digital health space. This will inevitably require a degree of harmonisation between Member States, if only in terms of definitions. What constitutes a healthcare team is not, for example, perceived in the same way in all countries. It will therefore be necessary to ensure that these disparities don't become obstacles, particularly in the context of the European Health Data Space, which aims to be accessible to all healthcare professionals in the Member States. In ongoing and future developments, it will also be important to bear in mind that health data and its increased dissemination have a primary purpose, which is to benefit citizens and strengthen their rights. Therefore, particular attention must be given to initiatives which, through their use of this data, could weaken fundamental equilibria on the pretext of better health.

---
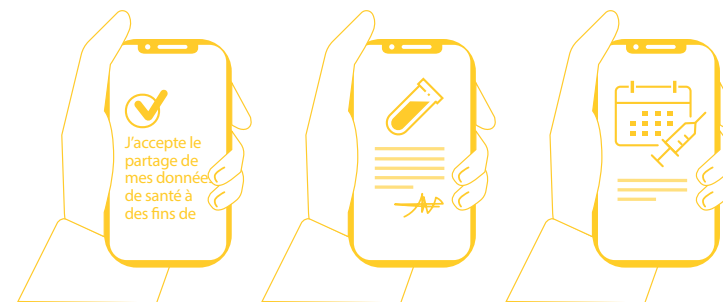
143 The French Public Healthcare Insurance System paid for 12.8 million teleconsultations between January and August 2020, compared to only 138,000 between September 2018 and the end of December 2019.

144 European Commission, " Commission proposes a trusted and secure Digital Identity for all Europeans", Press release, June 3, 2021: https://ec.europa.eu/commission/presscorner/detail/en/ ip_21_2663

145 For the time being, France, for example, has not set up this type of service, although the France Connect system is the first step in this direction.

RENAISSANCE NUMÉRIQUE'S RECOMMENDATIONS

In order to move forward in the use of health data for a better governance and greater efficiency of the healthcare system, Renaissance Numérique has drawn up eleven recommendations, organised around three key objectives:

COMMIT TO SERIOUS ACCULTURATION EFFORTS IN TERMS OF HEALTH DATA, AND MORE GENERALLY IN TERMS OF DIGITAL HEALTH

Recommendation n°1 - Serious acculturation efforts must be directed towards the stakeholders in the healthcare chain (healthcare professionals, patient associations, etc.), right down to the citizens, including new entrants, such as the tech stakeholders who are investing in the field of healthcare, and are not familiar with of all its underlying issues.

Recommendation n°2 - Certain professions, such as pharmacists, nurses, and doctors, have a role to play in disseminating this health data culture by becoming kind of "mediators", trusted third parties acting at the interplay between citizens and the other stakeholders in the chain (State, industry players, etc.). They must be supported and empowered in this respect.

Recommendation n° 3 - Patients', users', and consumers' associations also have an important role to play in this acculturation effort, providing they increase their skills on the health data topic.

Recommendation n°4 - In addition, the digital mediation policy should be massified in order to make all citizens (including the least connected ones) familiar with the issues related to health data, and to support them in their use of digital health.

CLARIFY HEALTH DATA GOVERNANCE

Recommendation n°5 - Clarifying the governance of health data requires clarifying the roles and strengthening the collaboration between the various stakeholders involved in the steering of the public policy on health data.

Recommendation n°6 - The various stakeholders in the healthcare chain should also be encouraged to share their data more widely. Incentive tools and mechanisms (data trusts, contractual solutions, technical tools) exist and should be more widely used.

Recommendation n°7 - Clarifying the governance of health data will also require a more effective implementation of the requirements relating to technical interoperability and security standards: encouraging stakeholders to adopt the standards set by the ANS (SIS interoperability framework, use of the Convergence tool, etc.) and require hospitals and GHTs to be HDH-certified or to use HDH-certified services.

Recommendation n°8 - Lastly, we need to move towards a framework that is both protective and more conducive to innovation in health: introduction of regulatory sandboxes, increased use of real-world data.

PUT CITIZENS AT THE HEART OF HEALTH DATA GOVERNANCE

Recommendation n°9 - Putting citizens at the heart of the healthcare system means that they must be able to play a greater part in the collective decisions that need to be taken on health data, by being consulted on public health policy plans and via establishing a dialogue on specific topics.

Recommendation n°10 - Citizens must also be more strongly represented in health data governance bodies (French Public Healthcare Insurance System, Health Data Hub) through patients', consumers', users', and rights' associations.

Recommendation n°11 - Finally, they must be able to share their data directly, in order to help assess the quality of healthcare and to regulate the healthcare system through data, and thus take an active part in improving the healthcare system.

GLOSSARY
KEY TERMS

Anonymisation: processing of data using a set of techniques that make it practically impossible to identify the individual by any means, in an irreversible way.

Health data: personal data concerning health is data relating to the past, present, or future physical or mental health of a natural person (including the provision of healthcare services) that reveals information about that person's health status.

- Health data by nature: data that is intrinsically and obviously health data.

- Health data by cross-referencing: data which, taken independently, does not constitute health data, but which, when cross-referenced with other data, may give an indication of a person's health status, or on the potential risks for the health of that person.

- Health data by purpose: data that becomes health data because of its use for medical purposes.

Health democracy: the concept of health democracy aims to involve all stakeholders of the healthcare system in the development and implementation of public health policy, in a spirit of dialogue and consultation. It is enshrined in Title III of France's Law of 4 March 2002 on patients' rights and the quality of the healthcare system.

Interoperability: the ability of an IT system to communicate, run programs, or transfer data with other existing or future IT products or systems, without any constraint for its user in terms of access or implementation, and without multiplying development efforts[146].

Matching: the reconciliation of separate data sets, using common information (e.g. grouping patient data from different sources).

---

146 Source: https://www.houdart.org/les-entrepots-hospitaliers-de-donnees-du-mythe-a-la-re-alite/

Medical data: nformation collected and held by healthcare professionals. This is collected from birth (weight, height, medical report) and then throughout life, during visits to healthcare centres and pharmacies.

Mon Espace Santé: *Mon Espace Santé* is a digital health space (ENS), a patient portal that will be accessible to any user of the French healthcare system from 1 January 2022. It aims to provide easy and secure access to a number of services: SMR, secure messaging, a "health diary" allowing the consolidation of various healthcare-related appointments, and the "ENS store", a catalogue of digital health services referenced by the public authorities.

National Health Data System (SNDS): managed by the French Public Healthcare Insurance System, the SNDS constitutes a complete and detailed database on patient pathways and the organisation of the healthcare system in France. It gathers:

- The National Inter-Regime Public Healthcare Insurance Information System (SNIIRAM): an anonymous data repository containing information from reimbursements made by all French public healthcare insurance schemes for healthcare delivered by private practitioners.

- Data from the Program for the Medicalisation of Information Systems (PMSI): data from hospitals and other healthcare establishments.

- The CépiDC: a database managed by *Inserm* which collects data on medical causes of death for the whole population.

Pseudonymisation: (reversible) processing of personal data which makes it impossible to identify the data subject without resorting to additional information, provided that this additional information is kept separate and subject to safeguards.

Real-world data: data that is not collected in an experimental setting, but which is generated in everyday practice, particularly during routine healthcare. This data is usually collected by medical devices (MDs) or by connected objects or digital applications.

Shared medical record (SMR): the SMR is a digital health record that stores and secures health information (treatments, test results, allergies, etc.) relating to the users of the French healthcare system. It allows this information to be shared with healthcare professionals in a totally secure way. From 1 January 2022, it will be accessible via the *Espace Numérique de Santé* (ENS), becoming one of its building blocks.

KEY STAKEHOLDERS

Digital Health Agency (*Agence du Numérique en Santé* or ANS): formerly the Shared Health Information Systems Agency or ASIP-Santé, the ANS is a French government agency in charge of digital health. In particular, it draws up ethical, security, and interoperability guidelines relating to health data.

Directorate for Research, Studies, Evaluation, and Statistics (DREES): attached to the Ministry of Solidarity and Health, DREES is the Ministry's public statistical department. It is part of the public statistical department led by INSEE.

Ministerial Delegation for Digital Health (DNS): the DNS is responsible for steering all digital health transformation projects in France. It reports directly to the Minister for Solidarity and Health and provides closer supervision of the Digital Health Agency (ANS).

National Authority for Health (HAS): the HAS is an independent public authority which contributes to the regulation of the healthcare system in terms of quality. Its role is to assess healthcare products (medication and medical devices), professional best practices, the organisation of healthcare and public health.

National Institute for Health and Medical Research (INSERM): French public scientific and technological institution specialised in medical research.

Public Healthcare Insurance Fund for Employed Persons (CNAMTS): the CNAMTS manages the 128 Primary Public Healthcare Insurance Funds (CPAM) located at a local level, which are responsible for paying out social security healthcare insurance benefits. It manages the National Health Data System (SNDS).

Regional Health Agency (ARS): a public administrative establishment of the French State, responsible for implementing health policy in its region.

ACKNOWLEDGMENTS

Caroline Guillot, Deputy Director of Associations and Citizens Relations, Health Data Hub

Hélène Guimiot-Bréaud, Head of the Health Department, CNIL

Cyrille Isaac-Sibille, Member of Parliament (Rhône), Rapporteur on SMR and health data

Aurora Ursula Joala, Adviser on "e-services development and innovation policy", Estonian Ministry of Social Affairs

Irina Kalderon-Libal, Policy Officer, "e-Health, Well-being and Ageing" Unit, DG CNECT, European Commission

Kalle Killar, Deputy Secretary General for e-Services Development and Innovation Policy, Estonian Ministry of Social Affairs

Jean-Christophe Klein, Co-founder and CEO, Libhéros

Christine Laliberté, President, Quebec's Specialised Nurse Practitioners Association (AIPSQ)

Yann-Mael Le Douarin, Telehealth Medical Advisor, DGOS, Ministry of Solidarity and Health

Franck Lethimonnier, Director of the "Technologies for Health" thematic institute, National Institute for Health and Medical Research (INSERM)

Isabelle Levasseur, Vice-president, Quebec's Specialised Nurse Practitioners Association (AIPSQ)

Jacques Lucas, President, Digital Health Agency (ANS)

Jelena Malinina, Digital Health Policy Officer, European Consumer Organisation (BEUC)

Bernard Ourghanlian, CTO & CSO, Microsoft France

Antoine Piau, Geriatric physician and spokesperson for the telehealth transverse medical unit (UMTT), Toulouse Teaching Hospital

Stéphane Pierrefitte, Director of Innovation and Information Systems, Paris Psychiatry and Neurosciences Teaching Hospital Grouping

Jean-Marc Pinguet, Personalised Healthcare Director, Roche

Dominique Pon, General Director of *Toulouse's Clinique Pasteur*, Strategic Manager for Digital Transformation in Health, Ministry of Solidarity and Health

Noemi Porrello, Real World Evidence Leader, Integrated Access Department, Roche Italy

Didier Quercioli, National Delegate and President of MGEN Technologies, MGEN

Gérard Raymond, President, France Assos Santé and Vice-President, Health Data Hub

Dario Scapola, Integrated Access Management Director, Roche Italy

Valérie Schlosser, Data and Digital Strategy Director, Vyv Group

Chloé Simpson, Impact DATA Project Manager, Red Cross (21)

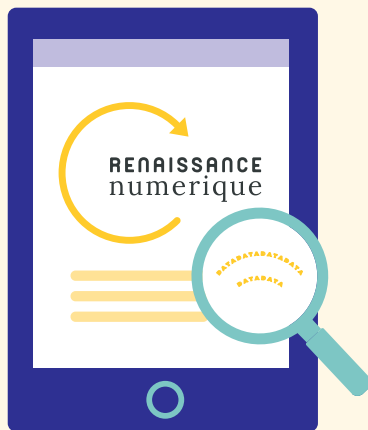**Juliette Valains,** Digital Transformation Manager, Red Cross

Guy Vallancien, Surgeon, Academic, Member of the National Academy of Medicine, Member of the Parliamentary Office for Scientific and Technological Assessment (OPECST)

FURTHER RESOURCES

Renaissance Numérique and Syntec Numérique (May 2019), « Tous acteurs des données. Appréhender les données pour mieux les valoriser » ("*We're all data stakeholders. Understanding data to make better use of it*"), 97 pp.: https://www.renaissancenumerique.org/publications/tous-acteurs-des-donnees-apprehender-les-donnees-pour-mieux-les-valoriser

Renaissance Numérique (March 2017), « 17 Experts / 36 propositions pour une ambition politique en matière de e-santé » ("*17 Experts / 36 proposals for a political ambition in terms of e-health*"), 44 pp.: https://www.renaissancenumerique.org/publications/17-experts-36-propositions-pour-une-ambition-politique-en-matiere-de-e-sante

Renaissance Numérique (September 2014), « D'un modèle de santé curatif à un modèle préventif grâce aux outils numériques » ("*From a curative healthcare model to a preventive one, using digital tools*"), 119 pp.: https://www.renaissancenumerique.org/publications/d-un-systeme-de-sante-curatif-a-un-modele-preventif-grace-aux-outils-numeriques

ABOUT RENAISSANCE NUMÉRIQUE

Renaissance Numérique is France's main independent think tank focusing on the challenges of the digital transformation of society. Bringing together universities, associations, corporations, start-ups and schools, it aims to develop workable proposals to help public stakeholders, citizens and businesses build an inclusive e-society.

Renaissance Numérique
32 rue Alexandre Dumas - 75011 Paris
www.renaissancenumerique.org

June 2021
CC BY-SA 3.0