European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 267-272
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 21

*The Cybersecurity of Health Data Hosted by Public Administrations**

Marcel Moritz
(Senior public-law lecturer at University of Lille, France CERAPS UMR8026)

ABSTRACT As cyber-attacks on health data increase, securing health data is a growing challenge. But this security is not only a mere technical issue aimed at preventing malicious third parties. It is also necessary to ensure the legal security of the chosen hosting solutions, in the context of the opening up of health data, which itself raises many questions. These are the challenges that need to be resolved in order to give full effect to the perspectives offered by the massive processing of these data.

1. *Introduction*

Health data[1] are considered sensitive data within the meaning of the General Data Protection Regulation (GDPR),[2] and as such must benefit from special protection. Indeed, the information likely to be revealed by these data generates particularly serious risks. In wrong hands, these data could, for example, limit access to certain services, or make it difficult to obtain a loan or a job. It is therefore not surprising that health data are one of the most widely traded data on the Darknet.[3] Their value is often far greater than that of bank-card data. The processing of such data therefore requires trust in the controller, especially when the latter is a public administration, such as a hospital, processing large amounts of data. Legally, the GDPR provides several general privacy guarantees for the processing of health data. For example, most processing of such data requires a privacy-impact assessment to be carried out beforehand, as well as the appointment of a data-protection officer. These safeguards are further increased in the context of processing by public administrations, since the latter are always subject to the obligation to appoint a data-protection officer, even if the processing of health data does not take place on a large scale.

The question is whether these guarantees are sufficient, given the legitimate citizens' expectations regarding public bodies processing their health data. From our point of view, this is not a mere matter of personal-data security, but an essential condition for maintaining the public's trust in the State and its public services. To put it another way, in view of the risks and the legitimate trust that citizens are supposed to have in the public administration, the latter's processing of health data should be perfectly irreproachable in terms of technical, organisational, and legal security. However, many recent examples show that this information-security management is not fully satisfying. To give just one example that has received considerable media coverage in France and beyond, we can mention the theft from Paris hospitals, in the summer of 2021, of the personal data of around 1.4 million people tested for Covid-19. This data breach was widely publicised, as required by the GDPR, which imposes communication to data subjects in such cases.[4] Thus, cybercrime has become a major issue for health data, which we will highlight in the first part. But there is also another important issue, that of the sovereignty of data storage and the legal risks induced by some cloud solutions. This will be developed in the second part. Finally, we would like to emphasise the risks induced by the future implementation of the data-governance act, in that it promotes open data, particularly personal and sometimes health data, which could well give rise to new legal

* Article submitted to double-blind peer review.

[1] Art. 4 §15 GDPR provides that: *"'data concerning health' means 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"*.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[3] www.keepersecurity.com/fr_FR/how-much-is-my-information-worth-to-hacker-dark-web.html.

[4] Indeed, according to art. 34 GDPR "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay".

risks. These aspects will be studied in the third part.

2. *Threats related to cybercrime and legal responses*

Unsurprisingly, cybercriminal groups are interested in health data because of their high value. Indeed, they can potentially be used for a variety of malicious purposes: phishing, ransomware,[5] advertising fake medicines, restricting access to bank credit or to certain services such as health insurance, training of artificial intelligence, etc. In the US, it was found that the annual number of ransomware attacks on health-care delivery organizations more than doubled from 2016 to 2021, exposing personal-health information of nearly 42 million patients.[6] In France, according to a May-2021 report,[7] in 2020, no fewer than 27 attacks affected French hospitals, and the health sector has suffered one cyberattack per week since the beginning of 2021. Even more worrying is the fact that these figures appear, according to the public authorities themselves, to be lower than reality: "Symptomatic of this disparity in the perception of the issues, the number of serious incidents reported by health establishments is still low and lower than the estimated reality".[8]

The general principles of the GDPR regarding data security impose de facto an enhanced protection for health data. Indeed, by advocating a risk-based approach, Article 32 imposes appropriate technical and organisational measures adapted to the risks[9], including for example "(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing". This involves a risk-assessment carried out under the responsibility of the controller. The latter must also inform the competent data-protection authority in the case of personal-data breaches[10] and, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons",[11] "communicate the personal data breach to the data subject without undue delay".[12] This is the reason why in the above-mentioned case of the theft of Covid-test data, a specific communication was set up after notification to the French Commission Nationale de l'Informatique et des Libertés (CNIL).[13]

In the case of health data, specific sectoral guidelines may apply, in particular the security guidelines resulting from the Politique Générale de Sécurité des Systèmes d'Information de Santé (General Policy on the Security of Health Information Systems) known as the PGSSI-S,[14] referred to in Articles L. 1470-5 and L. 1470-6 of the French Public Health Code (Code de la santé publique, CSP), as well as the Health data hosts (Hébergeur de données de santé, HDS) accreditation and certification guidelines, referred to in Article L. 1111-8 of the same Code. CNIL declaration or authorisation requirements may also apply,[15] for example the declaration of compliance with the reference methodology MR-003 applicable to health research without consent.[16]

But the most important security factor is probably that many health data are processed by stakeholders who are operators of essential

[5] In October 2020, at least 2,000 Finnish patients received an email threatening to publish the details of their psychological treatment on the web if they did not pay several hundred euros, after the data of a network of psychotherapy centres was hacked (www.slate.fr/story/215763/bonnes-feuilles-ma-sante-mes-donnees-coralie-lemke-premier-parallele-securite-gafam-secret-medical-informations).

[6] Vv. Aa., *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021*, in www.jamanetwork.com/journals/jama-health-forum/fullarticle/2799961.

[7] Ministère des solidarités et de la santé, *Cybersécurité dans le secteur de la santé et du médico-social : une priorité nationale pour réussir la transformation numérique*, dossier d'information, 05/2021, 28.

[8] *Ibid.*, 7.

[9] "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (...)".

[10] GDPR, art. 33.

[11] GDPR, art. 34.

[12] *Ibid.*

[13] www.cnil.fr/fr/fuite-de-donnees-de-sante-ap-hp-que-pouvez-vous-faire-si-vous-etes-concerne.

[14] www.esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire.

[15] www.cnil.fr/fr/declarer-un-fichier.

[16] www.cnil.fr/fr/declaration/mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consentement

services' and/or - under French law - operators of vital importance[17] - and are thus covered by the network and information system (NIS) Directive[18] and/or article 22 of the French law of 18 December 2013.[19] As a result of these texts, the entities concerned have an active obligation to implement certain cybersecurity measures under threat of sanctions and may be required to undergo control audits, carried out in France by the "Agence nationale de la sécurité des systèmes d'information" (ANSSI)[20] or by entities approved by this agency. These cybersecurity requirements apply to an increasing number of entities. For instance, on 22 February 2021, the Ministry of Solidarity and Health presented, via a press release, its ambitions in terms of IT security for hospitals and announced that 135 territorial hospital groupments[21] will be included in the list of operators of essential services. At the same time, it was announced that a budget of 350 million euros will be earmarked for strengthening the IT security of French health institutions. Aware of the limits of a repressive policy towards cyber criminals, public authorities have therefore focused in recent years on the development of cyber-security measures and the allocation of resources in this respect. However, this security can still be improved in many respects. The news has given us several mediatised examples, such as the cyber-attack by ransomware which targeted the Corbeil-Essonnes hospital in August 2022 and which led to the disclosure of data by the hackers. According to the institution, the data that was disseminated potentially include "certain administrative data", including the national insurance number, and "certain health data such as examination reports and in particular external anatomocytopathology, radiology, analysis laboratories and doctors' files".[22]

Moreover, it is not only a question of technical security, in the context of risks of criminal cyber-attacks, but also of guaranteeing the legal security of data hosted in the cloud. In many respects, this issue is at least as challenging.

3. *Threats related to data storage and legal responses*

The idea of keeping health data for study purposes, particularly statistical ones, is not new. As early as the 1980s, the Programme de médicalisation des systèmes d'information (PMSI) was created in France to provide a synthetic and standardised description of the medical activity of health establishments. Since then, many databases have been developed, in particular the hospital health-data warehouses (entrepôts de données de santé hospitaliers, EDSH)[23] to collect large amounts of data. The implementation of EDHSs in France dates back to the end of the 2000s and was reinforced at the end of the 2010s. There are about twenty warehouses, some of which have teams of several dozen full-time equivalent employees, while others are much more modest in terms of resources. The nature of the data processed also varies widely depending on the ESDH.[24] In addition to these warehouses, the law of 26 January 2016[25] gave birth to the National Health Data System (SNDS), to create one of the largest health databases in the world.

Managed by the National Health Insurance Fund (Caisse nationale de l'Assurance Maladie, CNAM), the SNDS contains (i) health insurance data, (ii) hospital data, (iii) databases on medical causes of death and (iv) data on disability. The 2019 law on the organisation and transformation of the healthcare system extended the scope of the SNDS to data for healthcare professionals and organisations, data on loss of autonomy, and surveys in the field of health, school medicine, maternal and child protection and labour medicine. The SNDS thus makes it possible to provide a complete vision of the care pathways of the entire French population, over

[17] "Opérateur d'importance vitale".
[18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[19] Law no. 2013-1168 of 18 December 2013 on military programming for the years 2014 to 2019 and on various provisions relating to defence and national security.
[20] www.ssi.gouv.fr.
[21] www.usine-digitale.fr/article/voici-la-strategie-gouvernementale-pour-lutter-contre-les-cyberattaques-contreles-hopitaux.N1063569
[22] www.lemonde.fr/pixels/article/2022/09/25/cybercriminalite-l-hopital-de-corbeil-essonnes-refuse-de-payer-la-rancon-les-hackeurs-ont-commence-a-diffuser-des-donnees_6143112_4408996.html.
[23] For a recent report regarding these warehouses: www.has-sante.fr/upload/docs/application/pdf/2022-11/rapport_entrepots_donnes_sante_hospitaliers.pdf.
[24] www.has-sante.fr/jcms/p_3386123/fr/entrepots-de-donnees-de-sante-hospitaliers-en-france.
[25] Law no. 2016-41 du 26 janv. 2016 for the modernisation of French healthcare system.

a maximum historical depth of 20 years[26], to improve health policies, healthcare provision, social protection, medic-social care and research, but also to enhance France's international competitiveness through the release of these data[27].

Since 2019, a Health Data Hub[28] (HDH) has been added to this set. This platform is intended to facilitate the sharing of health data from a wide variety of sources in order to promote research, especially in the field of artificial intelligence[29]. Shortly after its creation, a decision motivated by the pandemic broadened the scope of the data that can be processed[30].

If the HDH has caused such a stir in France, it is not so much because of the extent of the data likely to be shared, but because of the choice of its technical operator: Microsoft Azure. Indeed, as an American company, this corporation is subject to a legislation that may, in certain situations, require it to transmit data to the American authorities. For the record, the Court of Justice of the European Union (CJEU), in its judgment of 16 July 2020, known as "Schrems II", ruled that the surveillance carried out by the American intelligence services on the personal data of European citizens was excessive, insufficiently regulated and without any real possibility of appeal. It concluded that transfers of personal data from the European Union to the United States are contrary to the GDPR and the Charter of Fundamental Rights of the European Union, unless additional measures are put in place or the transfers are justified under Article 49 of the GDPR[31]. In the case of the HDH, the situation is somewhat different since the data are not transferred to the United States, but to an American company while remaining hosted in Europe, a point on which the Court did not rule directly in the Schrems II case. It is this state of affairs that led the French Conseil d'Etat to validate - at least in the current context - the contract between the French State and Microsoft Azure, while acknowledging that there is a risk that Microsoft could be forced to provide data to the US authorities[32]. In another judgment, it was judged that the fact that Microsoft is governed by US law and may have to transfer data to the United States for the administration of the technical solution it offers, "in accordance with the Commission's decision of 12 July 2016", cannot be considered, at the date of this order and in the state of the investigation, a seriously and manifestly unlawful interference with the fundamental freedoms that the GDPR is intended to protect[33].

The HDH has thus been at least temporarily saved. But the legal risks remain real, as the CNIL has consistently stated,[34] and will probably not be completely removed by the presidential decree signed by President Biden, directing the steps that the United States will take to implement U.S. commitments under the European Union-U.S. Data Privacy Framework[35].

The above-mentioned disputes are therefore probably not the last. They have had the essential merit of putting the need for a sovereign cloud back at the heart of the debate, particularly regarding health data. Thus, on 19 November 2020, the Minister of Health, Olivier Véran, sent a letter to the President of the CNIL, in which the Minister undertook to terminate the contract with Microsoft and transfer the hosting of the Health Data Hub to a French or European player within two years.[36] Almost three years

[26] www.assurance-maladie.ameli.fr/etudes-et-donnees/en-savoir-plus-snds/presentation-systeme-national-donnees-sante-snds.

[27] L. Cluzel-Métayer, *Les données de santé, ou le défi d'un partage sous haute protection*, in *Revue de droit sanitaire et social* (RDSS), 2022, 149.

[28] To note that the French State has been ordered to stop using the expression "Health Data Hub" and its acronym "HDH", since there are translations approved by the commission for the enrichment of the French language, Tribunal administratif de Paris, 20 October 2022, *Revue Lamy Droit de l'Immatériel* (RLDI), 197, 1 November 2022.

[29] For more details, see article L. 1462-1 Code de la santé publique.

[30] Judgment 21 April 2020.

[31] For a global analysis of the HDH with regard to GDPR, see www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub.

[32] Conseil d'État, ordonnance de référés, 13 October 2020, no. 444937: *La semaine juridique édition générale* (JCP G), 2020. 1358, comm. B. Bertrand ; *Revue Lamy droit de l'immatériel,* 2020, 176, 5974, comm. P. Navarro and F. Zannotti.

[33] Conseil d'État, ordonnance de référés, 19 June 2020, n° 440916, pt. 28 : *Revue Lamy droit de l'immatériel* (RLDI) 2020/172, n° 5904, obs. L. Costes.

[34] P. Navarro, *Souveraineté et surveillance, les enseignements tirés de l'affaire du Health Data Hub*, in *Revue Lamy droit de l'immatériel*, 2020/176.

[35] www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework.

[36] www.mediapart.fr/journal/france/221120/health-data-

later, and despite political reactions during the 2022 presidential elections,[37] the situation seems to be frozen. The problem is that very few cloud service-providers could meet the requirements of the Health Data Hub in terms of security and privacy from a technical point of view. There may not be many alternatives to undertake a project of this size with all the necessary privacy considerations and guarantees.[38]

The most relevant response should come from the European Union itself, in order to achieve a fully sovereign storage of these data. What remains is to develop a solution that can compete from a technical point of view with that of digital giants such as Microsoft. This is the ambitious objective of the European Health Data Space, a specific health ecosystem comprised of rules, common standards and practices, infrastructures and a governance framework.[39] The aim is to provide a trustworthy setting for secure access to and processing of a wide range of health data, including the opening of health data.

4. *Threats related to the opening of data and legal responses*

Health data are unique in that they need to be not only protected, but also opened, particularly for research purposes. In France, this principle of open access was established by the law of 26 January 2016[40] and reinforced by the law of 24 July 2019.[41] In European-Union law, this principle of open access is now also advocated by the Data Governance Act[42] (DGA), which allows protected data (for example data that is protected as personal data) to be made available.

However, one may wonder about the risks generated by such openness. Indeed, even if the regulation imposes security measures prior to the opening of these data, it has been shown that the risks of re-identification are exponential depending on the volume of data available. Latanya Sweeney's studies are particularly interesting on this subject, especially regarding health data.[43] The risk is that many data sets, when correlated, can allow re-identification of individuals. In the case of health data, the risks could be extremely high for the persons concerned. One solution to this problem would be to invest massively in the quality of anonymisation, which has a significant cost. However, the fees that the Regulation provides for public-sector bodies to authorise the re-use of such data are likely to be limited in practice.[44] Indeed, only the costs of processing requests will be taken into account in the calculation of the fee and not the real value of accessing and using such databases. Moreover, it is foreseeable that some States, such as France, will not charge for access to such data at all. Thus, notice n°6264/SG of 27 April 2021 on public policy on data, algorithms and source codes[45] states: "This renewed ambition implies, in addition, (...) the extinction, by 2023, of fees charged for the re-use of data, in particular on the basis of Article L. 324-1 of the Code of relations between the public and the administration". Although this notice predates the adoption of the regulation, it does not seem that the principle of free access therein advocated is likely to be called into question.[46]

This situation seems problematic, at a time when large sums of money must be invested to set up data warehouses and the European Health Data Space, as we have seen, but also and above all to carry out the crucial work of anonymising these data. Beyond the economic

hub-veran-s-engage-retirer-l-hebergement-microsoft-d-ici-deux-ans.

[37] www.lemonde.fr/pixels/article/2022/01/11/sante-coup-d-arret-pour-le-controverse-health-data-hub_6109065_4408996.html.

[38] P. Navarro, *Souveraineté et surveillance, les enseignements tirés de l'affaire du Health Data Hub.*

[39] www.health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

[40] Law of 26 January 2016 for the modernisation of French healthcare system.

[41] 24 July 2019 on the organisation and transformation of the healthcare system.

[42] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).

[43] See for instance J. Su Yoo, A. Thaler, L. Sweeney and J. Zang, *Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data*, in www.techscience.org/a/2018100901.

[44] Art. 6 (5): "Fees shall be derived from the costs related to the processing of requests for re-use of the categories of data referred to in Article 3 (1). The methodology for calculating fees shall be published in advance".

[45] www.legifrance.gouv.fr/download/pdf/circ?id=

[46] In France, the report of the Bothorel Mission can be cited in the same vein: *Rapport Bothorel, Pour une politique publique de la donnée*, December 2020, 57. www.gouvernement.fr/rapport/11979-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources.

question[47] - should valuable data be made available to private companies for profit with taxpayers' money? - free access could well limit investments in the effective anonymisation of data and therefore in the legal security of their opening. This would seem to us highly questionable and provides an interesting opportunity to rethink our models of data opening and sharing. At a deeper level, a major challenge lies ahead: how can the European Union be both a model for personal-data protection and a champion of AI? Indeed, developing these AIs requires large amounts of learning data and can therefore generate legal risks. This is not an issue specific to health. Smart CCTV or predictive justice solutions raise for instance the same questions. But because of their sensitive nature, health data involve particular risks that must be taken into account.

In conclusion, the question of material, human and financial resources appears to be central: resources devoted to the technical and organisational security of information systems, to the sovereign storage of data, and to the safe opening of data. In a statement on 18 February 2021, President Macron stated: "Health structures will be invited to systematically devote 5 to 10% of their budget to cybersecurity, in particular to maintaining the security of information systems over time".[48] The political ambition on this point is therefore clear, but in the face of a public hospital in crisis, is cybersecurity really a priority? As for the European cloud, the example of Gaia-X[49] demonstrates the implementation difficulties encountered in the face of well-established giants such as Microsoft and AWS. In this context, it is easy to understand the fears inspired by the massive desire to open up data advocated by the DGA. Preserving our personal data has a price. Making the European Union an AI giant has a price too. The price of sovereignty.

[47] www.dsih.fr/article/4631/le-data-governance-act-ou-la-reutilisation-des-donnees-sans-veritable-valorisation.html.

[48] www.vie-publique.fr/discours/278659-emmanuel-macron-18022021-cybersecurite.

[49] www.lemondeinformatique.fr/actualites/lire-le-projet-europeen-gaia-x-est-bloque-au-stade-du-concept-86551.html.