Chapter 2 - II

Utilizing and protecting health data on a medical DPF

Kyoichi Iida*

1 What is a medical DPF?

Recently, a variety of digital platforms (hereinafter referred to as "DPF(s)") have emerged in numerous fields. Particularly influential among these are Google and the other GAFAM companies that have developed DPF businesses in the form of platforms that link users and merchants while providing advertising.

In the past few years, several DPFs have appeared in the medical field as well. There is a high probability that the influence of such medical DPFs will continue to expand with the advancement of digital transformation (DX), making people's lives better through the permeation of telecommunications technology.

Yet there is no clear definition of what a DPF is. The term "medical DPF" has been defined as both a platform that provides "methods for medical diagnosis and treatment over the Internet, including making reservations, providing medical histories, receiving examinations and prescriptions, and paying for services via video and text chats on smartphone and PC"[1] and "lead to optimal medical solutions[2] as a foundational element involving diverse players with diverse goals. However, there is no definitive agreement.

In this series, the nation is often likened to the Leviathan, while the DPF is compared to the Behemoth[3]. But as we will see in this article, which investigates some of the challenges and solutions regarding the protection, usage, and application of medical data (personal information related to one's health), medical DPFs are generally seen as "things that enable the distribution of medical data."

Medical DPFs can be categorized as public or private. Some examples of the former are listed in Table 1, while examples of the latter are listed in Table 2.

In addition, large DPFs continue to enter[4] the medical markets overseas and expand their business.

* **Kyoichi IIDA:** Guest Researcher in Keio University Global Research Institute, Attorney at law, kyoichi.iida27@gmail.com

1 Naoko Takato & Akira Mukai. "Power Struggle Among Healthcare Platforms In 2030 — Business Providing Infrastructure That Connects Vendors And Users." *Knowledge Creation and Integration, March 2022 Edition* (Nomura Research Institute, 2022), p.17.

2 Tatsuro Yamamoto. "Investigating The Formation Of Digital Platforms In The Pharmaceutical And Medical-Device Industries." *Ikiren Journal No. 113* (Japan Federation of Medical Devices Associations, 2021), p.57.

3 Tatsuhiko Yamamoto. "Digital Platforms In Modern Sovereign Nations — Leviathan And Behemoth." Edited by Hajime Yamamoto. *Basic Constitutional Theory* (Shinzansha Publisher, 2022), pp.147-181.

4 Allana Akhtar. "Here's where tech giants like Microsoft and Amazon stand in their race to revolutionize healthcare" *Business Insider*, April 20, 2021 (https://www.businessinsider.jp/post-233028, last accessed on January 8, 2024).

Table 1

National Database of Health Insurance Claims and Specific Health Checkups of Japan (NDB)	Stores data related to health-insurance claim receipts (which are provided monthly to insured individuals by medical facilities), specific health instructions, etc.
Nursing Insurance Database	Collects electronic data related to nursing-insurance claim receipts then anonymizes and stores it
Japanese National Cancer Database	Collects, analyzes, and manages data on every individual in Japan who has been diagnosed with cancer
Designated Intractable Disease Database	Consolidates the clinic notes and opinions of physicians etc.
Designated Chronic Children's Diseases Database	Consolidates the clinic notes and opinions of physicians etc.
Nationwide Healthcare Information Platform	Aims to provide superior healthcare by expanding the network of systems such as online qualification-verification services (using My Number as insurance cards) and consolidating all the medical data for a patient (including health-insurance claim receipts etc.) into a single DPF where it can be stored and managed; this idea was proposed in May 2022 by Medical DX Reiwa Vision 2030* as the backbone of future medical DX projects

* Ministry of Health, Labour, and Welfare Website. "About DX In Medical Treatment." (https://www.mhlw.go.jp/content/10808000/000992373.pdf).

Table 2

"CLINICS" (Medley, Inc.)	Online treatment and medication guidance app service
"LINE DOCTOR" (LINE Healthcare Corporation)	Online treatment service
"RIMOLEA" (Cancer Philosophical Outpatient Clinic)	Online treatment service
"KEN COMPASU"(Medical Compass, Inc.)	Online treatment service and self-care app

The purpose of healthcare is considered to be "providing medical treatment to patients and maintaining or improving the health of all people (including the prevention of illness)."[5] Since medical DPFs will distribute the sensitive medical information of individuals and continue to exert more influence within our societies, they may become so large that they begin to infringe upon people's rights. But they may also be responsible for saving people. In that case, it will be essential to not only prevent medical DPFs from violating the rights of people, but also to use regulations to control the expansion of the scope within which medical data is utilized and applied.

This article therefore aims to address two of the current issues related to the protection and usage of medical data: (1) the problems that arise due to the nature of a medical DPF itself, and (2) the fact that medical DPFs will allow medical data to be utilized under the primary purpose of use. First, in section 2, we will consider the issues with a medical DPF handling medical data. Section 3 then examines the current situation

5 Japan Medical Association. "Notes On Medical Ethics — The Purpose Of Medicine." (https://www.med.or.jp/nichinews/n120320u.html).

with the Act on the Protection of Personal Information, which governs the protection, usage, and application of medical data by a DPF, as well as the Next-Generation Medical Infrastructure Act. Finally, section 4 discusses some of the remaining challenges and their potential solutions.

2 Challenges of a medical DPF

(1) Protecting medical data

The medical data generated when we are diagnosed and treated at clinics and other medical facilities (including online consultations) is extremely sensitive and private information that could identify our illnesses and thus lead to prejudice or discrimination. Considering the frequent occurrence of massive leaks of personal data in recent years, many of us have probably worried about whether our diagnosis and treatment data is being used outside its purpose of use or provided to a third party without permission. It is therefore necessary to establish regulations that prescribe certain protections and restrictions regarding the use of medical data outside the scope of its purpose of use or providing it to a third party without the owner's consent.

(2) Utilizing and applying medical data

Meanwhile, as information technology and artificial intelligence have advanced, many companies have begun offering services that allow for the better utilization and application of data. In the world of healthcare, the use of data via medical databases, medical DPFs such as the Japanese National Cancer Registry Database, is expected to result in a number of new possibilities, including higher-quality medical treatment, the discovery of unknown side effects, the development of new drugs and other advances in medical science, the generation of new industries, and the formation of a society that enjoys a long healthy life expectancy. Moreover, the nation's birth rate is declining, and its population is getting older—plus, there is an urgent need to rapidly construct systems before the next biological danger such as the unprecedented global pandemic we just experienced. And in a country like Japan that suffers from frequent natural disasters such as earthquakes and tsunamis, the usage and application of medical data should be permitted over a wide range to achieve the goal of healthcare, as long as that data is afforded a certain level of protection and restriction. In concrete terms, we need regulations supporting application and usage that allows the data's owner to directly benefit and is also beneficial to the overall future of humanity (such as through medical research).

(3) Specific challenges

Let's look at some specific problems with medical DPFs from the viewpoint of protecting and utilizing medical data.

(A) Problems with the nature of medical DPFs (protectio)

In 2024, there was an incident at a university hospital in Osaka in which the names, patient IDs, ages, diagnoses, and treatment information of 2,003 patients participating in a research project were removed from the facility without permission by one of the doctors. In the same year, the names, patient IDs, pregnancy

progress, ultrasound images, and fetal vitals (height and weight) for eight individuals who signed up for an ultrasound video service were leaked due to the machine being operated incorrectly[6]. In 2023, a former employee at a clinic in Nagano Prefecture illegally removed the names, addresses, birth dates, treatment information, and other data of 3,137 dialysis patients and their family members (dialysis is a procedure in which waste products and excess water are artificially removed from the blood to clean it, replacing the function of the kidneys)[7]. While these incidents were limited to individual medical facilities, they clearly suggest that centralizing medical data within a DPF will create the risk for widespread damage if that data is stolen or leaked. Thus, protecting the medical data they contain is the primary challenge faced by medical DPFs. A study conducted by the European Union Agency for Cybersecurity regarding cyber-incidents that occurred between January 2021 and March 2023 found that 53% of the incidents during that period involved medical providers, and 43% involved the theft or loss of data[8].

In 2010, there was a court case concerning the unauthorized provision of a patient's medical data to a third party by their family doctor[9]. The court ruled that explaining MRI scan results and communicating the opinion that the patient's spinal disc herniation was age-related to the employer of the patient without the patient's consent was a breach of medical confidentiality. The court therefore ordered the doctor to pay ¥1 million in damages. In its ruling, the court noted that physicians "must be careful to once again verify with the patient the scope of their consent" when asked to disclose their medical information to a third party[10]. If the idea is that medical data will be shared among multiple medical DPFs (databases etc.), then the challenge is to clearly explain to them that the data will be shared when asking for their consent to acquire said data.

This court case involved the unauthorized provision of medical data to a third party. But in reality, the patient's consent is currently regarded as highly important in clinical settings. In practice, data is almost never used without the owner's consent. We can only speculate about the reasons for this, but perhaps it is due to the current societal trend that places absolute importance on consent, or maybe the concept of informed consent (fully explaining the details of the illness, testing, treatment, prescriptions, etc. to the patient so that they understand them well enough to provide their voluntary consent prior to starting treatment) has been established among medical practitioners, creating a deep-seated reluctance to use data without the consent of the patient or their family. People generally recognize the need to get the patient's consent during treatment, and that the proxy consent or implied consent of a family member is often used in place of that consent in order to use the patient's data[11]. However, some have noted that equivocating actual consent and implied

6 https://www.med.kindai.ac.jp/notice/2024_0513_6086.html Last accessed on June 11, 2024.

7 Takunori Yasuda. "Personal Data Of 3,137 Patients Leaked — Did A Former Employee Remove It From The Hospital?" *Asashi Shimbun Digital*, March 30, 2023. (https://digital.asahi.com/articles/ASR3Y7FQLR3YUOOB001.html, last accessed on June 11, 2024).

8 ENISA THREAT LANDSCAPE: HEALTH SECTOR, Masahito Yamaga. "ENISA Releases Report On Ransomware, Data Theft, And Other Serious Cyberthreats Within EU Healthcare." *Internet Watch*, August 3, 2023. (https://internet.watch.impress.co.jp/docs/column/security/1520495.html, last accessed on January 27, 2024).

9 Decision by the Saitama District Court, Kawagoe Branch on March 4, 2010 (Judicial Case Report 2083, p.112).

10 Satoru Makita. "Disclosing Medical Data To An Employer Without The Patient's Consent Is Illegal." *Nikkei Medical*, March 22, 2017. (https://medical.nikkeibp.co.jp/leaf/mem/pub/series/dispute/201703/549457.html, last accessed on June 11, 2024).

11 Shigeto Yonemura. "Problems With Medical Data Within the Legal System." *Journal Of Medical Law, No. 34* (2019), p.121.

consent in this way reduces the idea of consent to a mere formality.

(B) Challenges with the fact that medical DPFs allow medical data to be utilized under the primary purpose of use (utilization and application)

Imagine a scenario in which a patient that is currently receiving treatment travels far from home on a business trip. Suddenly, their condition worsens and they require emergency medical care. But the medical facilities in that area might not be able to obtain detailed medical information about this individual. If the patient is in possession of all their own medical data, then they could receive care at a local hospital or clinic, which would clearly be beneficial.

The usage and application of medical data is categorized as either (A)"primary usage," in which the usage is for the purpose of directly administering treatment to the owner of the data; or (B) "secondary usage," which involves usage that is not for the patient's immediate benefit, such as case studies (disclosing clinical progress to one's staff members to verify in detail whether the appropriate treatment strategy has been selected), statistical analyses of treatment, research, innovation, or policy-making. The challenge is to establish regulations not for frameworks involving the currently popular secondary usage of medical data (which has been identified as being potentially useful for healthcare and other purposes)[12] but rather those involving the primary usage of health data via a medical DPF for treatment that directly benefits the data's owner.

3 Medical DPF regulations

The Act on the Protection of Personal Information (hereinafter referred to as "APPI") and the Next-Generation Medical Infrastructure Act[13] (hereinafter referred to as "NMIA") are two laws that establish regulations related to the protection, use, and application of health data by a medical DPF. Let's look at how these laws restrict medical DPFs with regard to the aforementioned challenges.

(1) APPI

While the development of our digital society has expanded the application of personal data in a useful way, it has also created the need to preemptively prevent the infringement of various human rights due to the improper handling of that data. Therefore, this law aims to protect people's rights and interests while considering the usefulness of their personal data. APPI applies to "businesses handling personal information" who use databases or their equivalent to systematically organize personal data so that specific individuals can be searched for using a computer. Most medical DPFs, including hospitals and other medical institutions, online healthcare providers, and database vendors, are businesses that handle personal information and therefore are subject to the jurisdiction of the APPI. Businesses that handle personal information are obligated to

12 George Shishido. "Privacy And The Act on the Protection of Personal Information." *Journal Of Medical Law, No. 34* (2019), p.95.

13 The "duty of confidentiality" that is required of physicians as well as the "ethical guidelines for medical and life-science research conducted on humans" are also regulations that cover the protection, use, and application of medical data; however, their discussion was omitted here due to space constraints.

establish safety-control measures for data.

Information such as medical records that include the notes of physicians; diagnostic information that healthcare professionals learn about the patient's physical status, pathology, treatment, etc. during the course of their medical care and prescription medication; the results of medical examinations; instructions regarding healthy living; and similar records are considered "sensitive personal information" that require special care. Acquiring sensitive personal information requires the owner's consent, defined as "the owner's declaration that they agree to their personal information being handled in accordance with the methods stated by the handling business."[14] The business is also required to specify the data's purpose of use prior to obtaining the owner's consent, notifying of or disclosing to that individual the specified purpose of use, unless otherwise announced in advance. This disclosure must be in a form that allows the owner to logically anticipate or imagine how their personal data will be used.

For medical institutions, the data's purpose of use is often published on their website that lists things like security guidelines and purpose of use information[15]. In the case of online healthcare services and other private-sector medical DPFs, it is referenced in their privacy policies (rules that govern how personal information as well as privacy in general are handled)[16]. As for public medical DPFs like the NDB mentioned earlier, separate policies that protect personal information may be established[17] with government guidelines. The owner's consent must also be separately obtained for any usage that exceeds the specified purpose of use, or when providing their data to a third party[18]. Violating these regulations makes the handling business subject to spot inspections by the Personal Information Protection Commission, which may order the business to make some changes. Non-compliance may result in up to one year of imprisonment or a fine of up to ¥1 million (corporations are subject to fines of up to ¥100 million).

There are a few different systems that facilitate the usage and application of personal information or data. (A) Anonymized systems can provide data to third parties without the owner's official consent because they process the data in a way that makes the owner unidentifiable (such as by deleting their name, address, and other personal information). For example, claim receipt data held by a society-managed health insurance organization could be anonymized then provided to a medical database provider (a medical DPF), who could then use it to provide data, consulting, and other services to such organizations as well as to research

14 For example, individuals can consent by providing oral confirmation, submitting a document (including electronic formats), submitting an email, checking a confirmation box, clicking a button on a website, inputting their voice, tapping a touchscreen, activating a button or switch, etc.

15 Keio University Hospital(https://www.hosp.keio.ac.jp/about/privacy/policy.html)
Kyorin University Hospital(https://www.kyorin-u.ac.jp/hospital/introduction/privacy_policy/)

16 LINE Healthcare Corporation, for example, has established privacy policies for its overall services, patients, and physicians.
・Overall Services (https://terms2.line.me/LINE_Healthcare_common_Privacy?lang=ja)
・Patients (https://terms2.line.me/Telemedicine_LHC_Privacy?lang=ja)
・Physicians (https://terms2.line.me/TelemedicineCMS_LHC_Privacy?lang=ja)

17 Prior to publishing research that used the NDB, the Ministry of Health, Labour, and Welfare that there are no cases involving rare diseases or other facts that could be used to identify specific individuals. This is done in accordance with its "Guidelines for Using Databases with Anonymized Health-Insurance Data etc." (https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryouhoken/reseputo/index.html).

18 And in cases where the government provides data to a third party within the scope of its purpose of use, consent is not required by APPI.

institutions, pharmaceutical companies, etc. Also, (B) if the business handling the personal information is an academic research institution such as a university, some regulations allow it to use the personal data of individuals outside the stated scope or to provide it to a third party without the owner's consent in certain situations—when it is needed for scholarly research, for instance, or when the third party is an institution for scholarly research that needs the data for an academic study. APPI also (C) recognizes the right of patients to request disclosure of their retained medical data.

(2) NMIA

It has been pointed out that is not realistic to expect many medical facilities and other organizations to use an anonymizing system due to the fact that the anonymization process remains as the responsibility of the facility itself, and in the case of outsourcing, it is difficult to determine whether the contractors have sufficient anonymization capabilities. This led to the creation of the NMIA on April 28, 2017.

This act aims to further contribute to the formation of a healthy and long-lived society through cutting-edge research and development as well as the creation of new industries related to health and medicine. It does this by establishing regulations for the handling of medical data and anonymized medical data. NMIA ensures the quality of anonymized data by allowing only companies that have been certified as possessing strong processing capabilities and data-security standards (safety-control measures) to create anonymized data. It also gives data owners or their surviving family members the right to request that their medical data[19] not be provided to certified companies by medical facilities if that data can be used to identify them. Employees, etc. of certified business operators, etc that illegally provide medical data through a database face up to two years of imprisonment or a fine of up to ¥1 million (or a fine of ¥100 million in the case of a corporation).

Anonymized medical data can now be widely utilized in Japan by drug companies, research institutions like universities, local governments, or anyone else as long as the data contributes to research and development within the field of medicine. A 2023 revision to NMIA also enables certified companies to connect to certain public medical DPFs like the NDB discussed earlier so that their anonymized medical data can be used. This made it possible to track data about a patient's death in some cases, which was difficult to do previously.

4 Current issues and possible solutions

(1) Problems with the nature of medical DPFs (protection)

(A) Issues

Regarding the issue of protecting medical data, both APPI and NMIA aim to control the unauthorized disclosure of such data by obligating companies to establish safety-control measures and stipulate sentencing

19 For example, the Center Hospital of the National Center for Global Health and Medicine has a disclosure on its website stating that it provides medical data in accordance with NMIA (https://www.hosp.ncgm.go.jp/aboutus/zisedai/index.html).

guidelines for imprisonment and fines. Due to the sensitivity of medical information and the potential for the expansion of medical DPFs, the development of further regulations remains an outstanding issue.

Although APPI requires that the purpose of use of medical data be disclosed to its owner, it is relatively flexible regarding how the owner's consent is obtained. As a result, the law in its current form does not sufficiently ensure that the owner understands precisely what they are consenting to. The development of further regulations remains an issue. Another problem with these current laws is that they do not satisfactorily solve the issue of placing too much importance on consent itself, and they turn the concept of consent into a mere formality. If these outcomes are to be avoided by removing the need for consent and establishing a framework for protecting the rights of the owners, further legislation for such a framework is still required.

(B) Possible solutions

On the topic of regulations that curtail the unauthorized disclosure of medical data, the extremely sensitive nature of this sort of data means that repairing the damage may be impossible if it is accidentally leaked to a third party. One potential solution is therefore to enact legislation that creates certain technical requirements such as managing the data in a format that cannot be easily restored, which could prevent the spread of damage if it is leaked. And since the ethics of healthcare professionals etc. ultimately have a substantial effect on how medical data is handled, another solution could be to establish regulations for a system that increases awareness among such individuals that handle data in connection with a medical DPF.

As for the problems of trivializing consent and ensuring that the owners of data can fully understand what they are actually consenting to, further study and exploration are needed to determine the exact techniques and methods for obtaining proper consent. One possibility is to construct frameworks and accompanying regulations that categorize the different types of consent and repeatedly seek confirmation from the owner depending on the level of consent needed, as well as those that include personalized AI tools etc. within medical DPFs to help owners make their own decisions regarding their consent[20]. The Council for Promotion of Regulatory Reform, [21] on June 1, 2023, suggested allowing medical data to be used for the benefit of the public (secondary usage) without the owner's consent. These discussions were partly triggered by the fact that consent has been reduced to a formality as well as the adoption by the European Health Data Space[22] (EHDS; a framework for sharing health data within Europe) of mechanisms that work in lieu of consent to strengthen data governance and thus prevent the infringement of individual rights. However, there is the need to clarify the logic behind allowing the creation of a system that does not require consent within a field like medicine, which has high potential for public benefit[23]. Careful consideration must be given to any system that works independently of consent, due to its potential impact on the right to self-determination. Creating specific models and regulations for a framework that prevents rights infringement appropriately without the

20 Koiti Hasida. "Personal AI and Value Creation." *Japio Yearbook 2022* (Japan Patent Information Organization, 2023), pp.16-19.

21 The Council for Promotion of Regulatory Reform. "Developing Systems etc. for Using Medical Data (Draft)." (https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/committee/230601/230601general_03.pdf).

22 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

23 Masako Wakae. "Using Patient Data—Consent No Longer Required." *Yomiuri Shimbun*, morning edition dated July 26, 2023 (remarks by Tatsuhiko Yamamoto).

use of consent in a manner similar to the EHDS could be the first step in constructing such a framework. (Within the EHDS, for exampl, "health data access bodies" are created to determine whether research institutions and other entities who wish to use medical data should be allowed to do so. This framework not only anonymizes data before giving it to users, but also supervises their usage of the data to ensure compliance with laws and regulations.)

(2) Challenges with the fact that medical DPFs allow medical data to be utilized under the primary purpose of use (utilization and application)

(A) Issues

NMIA established the notion that the best treatment can be provided to patients in general by facilitating research and development within the field of medicine through the use of anonymized medical data. In other words, anonymizing a person's health data will benefit that individual by providing them with more advanced treatments developed by research institutions through the use of the health data. So, unlike NMIA which focuses on secondary purpose of use, APPI assumes that usage could be under the primary or the secondary purpose of use. The request for disclosure created by APPI does allow individuals to acquire and use their own medical data, but it does not go as far as establishing regulations for a framework that helps people take the initiative in managing that data themselves, since corresponding with every single data owner would be impractical.

(B) Possible solutions

As mentioned, APPI assumes that usage could be under either the primary or the secondary purpose of use. In that case, we must consider whether a framework could be constructed and regulated under the law to go beyond requests for disclosure and enable patients to proactively use their own medical data for primary purposes. The General Data Protection Regulation (GDPR) establishes data portability as a basic right of European citizens. The data portability definition being considered for the EHDS is even more stringent than that of the GDPR, allowing users of one service to take the usage history and other data accumulated on that service and bring it to another service for use there. Since APPI does not mandate data portability, adding regulations to it that introduce a similar system and provide a regulatory framework that facilitates the emergence[24] of medical DPFs which enable the medical data of individuals to be collected and used by a variety of healthcare facilities (or at the very least, that lets individuals retain their health data in a decentralized manner and use it at their own discretion) could be one solution for expanding the scope of usage under the primary purpose of use.

24 Koiti Hasida. "Expanded Data Portability and AI Governance." *Japio Yearbook 2023* (Japan Patent Information Organization, 2023), pp.278-281.

5 Conclusion

This section discussed two of the remaining challenges related to the protection and usage of medical data by medical DPFs (the challenges that arise due to the nature of a medical DPF itself, and the fact that medical DPFs allow medical data to be utilized under the primary purpose of use) and presented a potential solution for them. Regulations that control medical DPFs are essential for protecting and utilizing medical data in a way that allows us to achieve the goal of treatment in the modern age, which is "providing treatment to patients and maintaining or improving the health of people (including the prevention of illness)."

There is a global trend of utilizing and applying medical and other personal data more liberally than before, and medical DPFs will play a big role in that. This article has only scratched the surface of the remaining challenges and their solutions, so more discussion related to the usage and application of medical data by DPFs is needed.